EU-wide digital Once-Only Principle for citizens and businesses

Policy options and their impacts

FINAL REPORT

A study prepared for the European Commission
DG Communications Networks, Content & Technology
by:

Digital
Single
Market

This study was carried out for the European Commission by Jonathan Cave, Maarten Botterman (GNKS Consult BV), Simona Cavallini, and Margherita Volpe (FORMIT)

Internal identification

Contract number: 30-CE-0743180/00-70

SMART 2015/0062

DISCLAIMER

ISBN 978-92-79-65335-3

doi:10.2759/393169

Abstract

Action 16 of the Digital Single Market strategy calls for improved cooperation among national systems to ensure that "businesses and individuals only have to communicate their data once to public administrations". This report: takes stock of current data re-use in national and cross-border interactions with public administrations; explores gaps and barriers affecting prospects for a EU-wide digital Once-Only Principle (OOP); identifies policy objectives and options; and analyses their impacts on key stakeholders under different possible scenarios (considering the very different circumstances of businesses and of individuals). The study found:

1- Broad support for OOP in general, but wide variation in maturity across Europe;
2- Many initiatives and legislative measures that are likely to simplify implementation of EU-wide OOP;
3- Significant evidence gaps on costs and benefits, especially beyond Member State level.

EU-wide OOP will require a legal basis (Directive at EU level) to support exchange of data for the purposes of the Once-Only Principle (R*ecommendation 1)*. An EU-wide coordinated *"proactive encouragement"* strategy is likely to provide the most effective and beneficial stimulus to balanced and sustainable progress. For this, an EU-wide taskforce is to be set up to advance mutual learning, appropriate convergence and coordination. *(Recommendation 2)*. In order to ensure effective implementation, we propose an approach based on access to an interoperable and clearly-described collection of base registries (*Recommendation 3)*.

Résumé

L'action 16 de la stratégie pour le marché unique numérique appelle à une coopération renforcée entre les systèmes nationaux pour veiller à ce que «les entreprises et les citoyens n'ont à communiquer leurs données qu'une seule fois aux administrations publiques». Le présent rapport: dresse un bilan de la réutilisation actuelle des données nationales et transfrontalières dans les interactions avec les administrations publiques; examine les lacunes et les obstacles qui affectent les perspectives d'un Principe «Une Fois pour Toutes» à l'échelle numérique (PUFT); identifie les objectifs et les options politiques; et analyse leurs impacts sur les principales parties prenantes dans le cadre de différents scénarios possibles (compte tenu des contextes très différents des entreprises et des particuliers). L'étude a constaté:

1- un large soutien au PUFT en général, mais de grandes différences de maturité dans l'ensemble de l'Europe;

2- De nombreuses initiatives et mesures législatives susceptibles de simplifier la mise en œuvre du PUFT à l'échelle de l'Union;

3- des lacunes significatives de preuves sur les coûts et les avantages, en particulier au-delà du niveau d'un État membre.

La mise en œuvre du PUFT à l'échelle de l'Union nécessitera une base juridique (directive au niveau de l'Union européenne) pour soutenir l'échange de données aux fins du principe «une fois pour toutes» (*Recommandation 1*). Une stratégie basée sur un «encouragement proactif» coordonné à l'échelle de l'UE est susceptible d'apporter l'impulsion la plus efficace et profitable à des progrès équilibrés et durables. Pour cela, une task-force à l'échelle européenne doit être établie pour promouvoir un apprentissage mutuel ainsi qu'une convergence et une coordination appropriées. (*Recommandation 2*). Afin de garantir une mise en œuvre efficace, nous proposons une approche basée sur l'accès à un système interopérable et clairement défini de registres de base (R*ecommandation 3*).

Executive Summary

The Once Only Principle (further: OOP) is described in the eGovernment Action Plan 2016-2020 as requiring that members of the public and individuals/businesses should not have to supply the same information more than once to public administrations.

This is in support of Action 16 of the Digital Single Market (DSM) strategy which calls for improved cooperation among national systems to ensure that "businesses and individuals only have to communicate their data once to public administrations" and that in consequence governments will no longer make "multiple requests for the same information when they can use the information they already have" – again assuming that if another Member State's government within the EU has the information, all other Member State governments could/should have access to it.

As a result of our study, we concluded that any progress towards a fair and non-discriminatory EU-wide introduction of OOP requires a sound and consistent legal basis in the form of a Directive that would allow competent authorities to exchange and use (further process) data (including personal data) pertaining to specific natural persons and businesses as an alternative to resubmission of the same or equivalent data by those individuals and businesses while protecting the rights of data subjects, including those enumerated under the GDPR. In our view such a framework at EU level must precede any further steps to implementing EU-wide OOP as it provides clarity on a key element of the Digital Single Market: allowing exchange of data among competent authorities in a harmonised, proportional and non-discriminatory way, in full compliance with data protection and other rules.

In addition, we recommend a strategy of "proactive encouragement of and administrative support for OOP" (Option 2 in the report). This approach will preserve advantageous localisation and specialisation, align progress and improve interoperability across Member States and at EU level while respecting subsidiarity and fundamental rights (especially data protection). The concrete actions involved should be 'business case driven[1]' and 'user centric[2], adopting a Base Registry approach wherever possible. A full move towards using data rather than documents

[1] Concentrated on areas of greatest immediate payoff, in particular business applications.

[2] Aligned to the needs of businesses and individuals rather than those of administrations.

for public administration purposes would further facilitate cost-effective and equitable service provision[3].

In practical terms, we recommend:

1. Preparing and proposing a Directive pertaining to data provided by natural persons or businesses to competent authorities, which would establish grounds for the further processing of those data by the original data controllers or other competent authorities for the benefit of the original natural person or business data subject. Such further processing would specifically entail i) making and ii) responding to requests for transfers or certifications based on the originally submitted data and iii) for the use of those data in place of the same or equivalent data submitted to the successor data controller by the original data subject. Such further processing would only be authorised to the extent (purpose, time and contents) required to replace data that would otherwise have to be submitted and would have fully to conform to the GDPR in respect of personal data;
2. Setting up a task force with Member State representatives to establish a sound and comprehensive framework for facilitating the development of OOP initiatives and their interconnection and access arrangements at European level. It should also provide a continuing capability for collecting and exchanging evidence, analysing impacts and resolving issues arising as OOP and the digitisation of government interactions spread; and
3. Establishing an EU-wide framework for business OOP to interconnect and provide access to base registers and consolidate steps towards portable or mutually-recognised business identities, common ontologies and streamlined procedures, based on requirements of the eIDAS Regulation and standards and interoperability principles in the (revised) EIF.

This will allow government to address framework weaknesses[4] and extend and consolidate progress in a bottom-up and incremental fashion using good practices and proven strategies and components.

Ultimately, we expect all EU Member States to embrace the Once Only Principle in ways that align with domestic requirements, taking advantage of their participation in the joint work in the task force to ensure that EU-wide OOP implementation will also become easier and more effective over time.

In this document, the term 'citizens' is often used to refer to natural persons as distinct from businesses (see further discussion in Section III.A). This is not meant to

[3] A further implication of such a move could be a requirement that certain data 'issued' by public administrations should be automatically available to and used by other public administrations – a sort of 'not even once only principle.'

[4] Including legal, organizational, semantic and technical barriers.

imply that the scope is restricted to citizens of EU Member States; data protection is a fundamental right and independent of citizenship and the bulk of services and information processing covered by OOP is not tied to citizenship status. It is intended to refer to the 'data home' of natural persons, which may be their country of citizenship or where their work visas, asylum application etc. were first registered

Why implementation of OOP

At the present time, there are not enough data to allow precise estimates of the impacts of cross-border OOP implementation on businesses and individuals. While there is some evidence of cost savings to public administrations, there is a shortage of data on required investment costs; levels of engagement and maturity vary greatly across Member States and, where implemented, OOP cannot clearly be separated from the services and other activities to which it applies. Nevertheless, some EU Member States have already embraced OOP for one or more of the following reasons:

1- Reducing the administrative burden on citizens and businesses;
2- More efficient (lower-cost, more effective) government administration;
3- Fraud prevention.

Why EU level action

The EU-wide implementation of OOP foreseen in this study stems directly from a main pillar of the Digital Single Market Strategy[5]: "Maximising the growth potential of the digital economy," which calls for implementation of the Once-Only Principle within a new eGovernment Action Plan as well as a European free flow of data initiative and improvement of the European Interoperability Framework. It also responds to a call in the October 2013 Council Conclusions[1]: "Efforts should be made to apply the principle that information is collected from citizens only once, in due respect of data protection rules."

Without these actions, the coherence and effectiveness of the Single Market may be threatened, impeding or discouraging cross-border mobility. Conversely, progress should accelerate the translation of building blocks and digital services infrastructures into general-purpose architectures that will reduce asymmetries between business and individual arrangements and provide European Public Services to all applicants on a truly location-independent basis. This can remove distortions between the exercise of business and personal mobility, allowing the

[5] Digital Single Market Strategy for Europe - COM(2015) 192 final, published on 06/05/2015.

most productive combination to be used Currently, awareness of specific opportunities to improve mobility and reduce burdens has produced multiple cross-border initiatives among neighbouring Member States; these have (or may soon) produced better local trade conditions for businesses and mobility conditions for individuals than exist with other Member States.

In addition, there are some 'wicked' issues that would benefit from resolution at EU level. These include privacy issues, the establishment of common standards and procedures to reduce fragmentation and, most importantly, a common legal base. This would allow public authorities to request, supply and make use of previously submitted information, and would help in addressing issues of burden (e.g. the cost to countries asked to supply information for use by another country) and liability (e.g. for incorrect decisions resulting from the re-use of incorrect or obsolete information).

Conclusions

The present study: takes stock of current data re-use in national and cross-border interactions with public administrations; explores gaps and barriers to an EU-wide digital Once-Only Principle; identifies policy objectives and options; and analyses their impacts on key stakeholders under different possible scenarios (considering the very different circumstances of businesses and of individuals). We found:

1- Broad (i.e. in most nations) support for OOP, but wide variation in maturity across Europe;
2- Many initiatives and legislative measures that are likely to simplify implementation of EU-wide OOP;
3- Significant evidence gaps on costs and benefits other than isolated one-off estimates at Member State level.

The proposed *"proactive encouragement"* option and the three concrete recommendations including the proposed European Member State taskforce to advance mutual learning, appropriate convergence and coordination, the interconnected[6] base registry approach to ensure effective sharing and a legal base for exchange of administrative data under OOP is likely to provide the most effective stimulus to cross-border European OOP implementation and balanced and

[6] Some documents refer to the creation of a system of base registers that incorporates interconnection, tailored access provisions and common or unambiguously-mapped descriptions of data contents, sources and quality as a 'federated' approach, especially when it specifies a single authoritative source for each specific datum. To avoid confusion with the political sense of the term, 'federated', we avoid using it here.

sustainable progress towards the establishment of OOP throughout the Member States.

Without any action, the opportunities will not be grasped and the situation will become further fragmented, leading to discrimination among individuals and businesses depending on the existence and nature of within- or between-country OOP.

Sommaire exécutif

Le Principe «une fois pour toutes» (ci-après le «PUFT) est décrit dans le plan d'action pour l'administration en ligne 2016-2020 comme requérant que les particuliers et les entreprises ne devraient pas avoir à fournir plus d'une fois les mêmes informations aux administrations publiques.

Cette initiative vise à soutenir la réalisation de l'action 16 de la stratégie pour un marché unique numérique, qui appelle à une coopération renforcée entre les systèmes nationaux pour s'assurer que «les entreprises et les citoyens n'aient à communiquer leurs données qu'une seule fois aux administrations publiques» et, qu'en conséquence, les gouvernements ne feront plus de «demandes multiples pour les mêmes informations lorsqu'ils peuvent utiliser les informations dont ils disposent déjà» — toujours en supposant que si un autre État membre au sein de l'UE possède toutes les informations nécessaires, tous les gouvernements des autres États membres pourraient/devraient y avoir accès.

À la suite de notre étude, nous avons conclu que tout progrès vers une introduction équitable et non discriminatoire du PUFT à l'échelle de l'UE requiert une base juridique solide et cohérente, sous la forme d'une directive, qui permettrait aux autorités compétentes d'échanger et d'utiliser (et de transformer) des données (y compris les données personnelles) se rapportant à des personnes physiques et aux entreprises, constituant une alternative à de nouvelles soumissions des mêmes données ou données équivalentes par les personnes et les entreprises concernés tout en protégeant les droits des personnes concernées, y compris ceux énumérés au titre du règlement général sur la protection des données. De notre point de vue, un tel cadre européen doit précéder tout autre mesure pour la mise en œuvre du PUFT à l'échelle européenne car il apportera des éclaircissements au sujet d'un élément essentiel du marché unique numérique: permettre l'échange de données entre les autorités compétentes, et ce de manière harmonisée, proportionnée et non discriminatoire, dans le respect intégral de la protection des données et d'autres règles.

En outre, nous recommandons une stratégie basée sur un «encouragement proactif» et un appui administratif pour le PUFT» (option 2 dans le présent rapport). Cette approche préservera l'avantage de la localisation et de la spécialisation, alignera les progrès et améliorera l'interopérabilité entre les États membres et au niveau de l'UE, tout en respectant le principe de subsidiarité et les droits fondamentaux (notamment la protection des données). Les actions concrètes

concernées devraient être axées sur des cas d'usage[7] et centrée sur l'utilisateur[8], en adoptant une approche fondée sur les registres de base dans la mesure du possible. Le passage complet à l'utilisation de données plutôt que de documents pour les besoins des administrations publiques contribuerait encore plus à la fourniture de services efficaces sur le plan des coûts et équitables[9].

Concrètement, nous recommandons:

1. Préparer et proposer une directive ayant trait aux données fournis par des personnes physiques ou des entreprises aux autorités compétentes et qui établirait des bases pour le traitement ultérieur de ces données par les contrôleurs de données originales ou par d'autres autorités compétentes au profit de la personne physique ou personne morale concernée. Ce traitement ultérieur pourrait concrètement entraîner i) établir et ii) répondre aux demandes de transfert ou de certifications fondées sur les données présentées initialement et iii) pour l'utilisation de ces données à la place des données identiques ou équivalents soumis au prochain responsable du traitement des données par la personne concernée. Ledit traitement ultérieur ne serait autorisé que dans le contexte nécessaire (objet, date et contenu) pour remplacer les données qui auraient normalement dû être introduites et devrait remplir toutes les conditions pour être conforme au règlement général sur la protection des données en ce qui concerne les données à caractère personnel;

2. La création d'une «task force» avec des représentants des États membres afin de mettre en place un cadre solide et global pour faciliter l'élaboration des initiatives PUFT et leur interconnexion et les accords d'accès à l'échelle européenne. Elle devrait également fournir une capacité permanente pour la collecte et l'échange d'éléments de preuve, d'analyses des impacts et pour résoudre les questions se posant avec la progression du PUFT et de la numérisation des interactions entre administrations publiques; et

3. Établir un cadre à l'échelle de l'UE pour l'application du PUFT aux entreprises afin d'interconnecter et d'assurer l'accès aux registres de base et de renforcer des mesures en faveur d'entreprises mobiles ou avec des identités reconnues mutuellement, d'ontologies communes et de procédures rationnalisées,

---

[7] Concentrés sur des domaines qui donnent le plus d'avantages immédiats, en particulier les demandes des entreprises

[8] Alignés sur les besoins des entreprises et des individus plutôt que sur ceux des administrations

[9] Une autre implication de cette évolution pourrait être une exigence selon laquelle certaines données «délivrés» par les administrations publiques devraient être automatiquement accessibles et utilisées par d'autres administrations publiques — une sorte de «principe même pas une seule fois.»

fondées sur les exigences du règlement eIDAS, des normes et des principes d'interopérabilité du Cadre Européen d'Interopérabilité (révisé).

Cela permettra aux administrations à se pencher sur les faiblesses[10] du cadre et d'étendre et de consolider les progrès d'une manière progressive et ascendante en recourant à de bonnes pratiques, à des stratégies et à des composants éprouvés.

En fin de compte, nous nous attendons à ce que tous les États membres de l'UE s'engagent en faveur du PUFT de manière à s'aligner sur les exigences nationales tout en tirant parti de leur participation aux travaux conjoints dans le cadre de la task-force à l'échelle de l'UE, afin de garantir que la mise en œuvre du PUFT devienne également plus facile et plus efficace au fil du temps.

Dans le présent document, le terme «citoyens» est souvent utilisé pour se référer à des personnes physiques contrairement aux entreprises (voir à ce propos les considérations dans la section III.A). Cela ne signifie pas que le champ d'application est limité aux citoyens des États membres de l'UE; la protection des données est un droit fondamental et indépendant de la citoyenneté et la majeure partie des services et des traitements de l'information couverts par le PUFT ne sont pas liés au statut de citoyenneté. Il est envisagé de faire référence aux «données domicile» d'une personne physique, qui peut être le pays dont elle a la citoyenneté ou dans lequel leur demande d'asile, de visa de travail ont été enregistrés pour la première fois.

Pourquoi la mise en œuvre du PUFT

À l'heure actuelle, il n'existe pas de données suffisantes pour permettre une estimation précise de l'impact lié à la mise en œuvre transfrontalière du PUFT pour les entreprises et les particuliers. Bien que certains éléments indiquent une réduction des coûts pour les administrations publiques, il y a une pénurie de données relatives aux coûts des investissements requis, aux niveaux d'engagement et la maturité varie considérablement selon les États membres et, où il est mis en œuvre, il est difficile de distinguer clairement son impact propre de celui des services et autres activités auxquelles il s'applique. Néanmoins, certains États membres de l'UE ont déjà adopté le PUFT pour une ou plusieurs des raisons suivantes:

1- la réduction de la charge administrative qui pèse sur les citoyens et les entreprises;

[10] Y compris les obstacles juridiques, organisationnels, sémantiques et techniques

2- une administration publique plus efficiente (coûts moindres et plus efficace);

3- la lutte contre la fraude.

Pourquoi une action au niveau de l'UE

La mise en œuvre à l'échelle européenne du PUFT prévue dans la présente étude découle directement de l'un des principaux piliers de la stratégie pour un marché unique numérique[11]: «maximiser le potentiel de croissance de l'économie numérique», qui appelle à la mise en œuvre du principe «une fois pour toutes» dans le cadre d'un nouveau plan d'action pour l'administration en ligne, ainsi qu'une initiative européenne sur la libre circulation des données et l'amélioration du cadre d'interopérabilité européen. Il répond également à un appel lancé dans les conclusions du Conseil d'octobre 2013: «Il conviendrait de déployer des efforts pour appliquer le principe selon lequel des informations ne sont collectées qu'une seule fois auprès des citoyens, dans le plein respect des règles relatives à la protection des données.»

Sans ces actions, la cohérence et l'efficacité du marché unique peut être menacée, entravant ou décourageant la mobilité transfrontalière. À l'inverse, les progrès devraient accélérer l'utilisation des blocs de base et des infrastructures de services numériques dans des architectures d'usage général qui permettront de réduire les asymétries entre les dispositifs pour les entreprises et ceux pour les individus et de fournir des services publics européens à tous les demandeurs sur une base indépendante de leur localisation. Cela peut supprimer les distorsions entre l'exercice de la mobilité professionnelle et personnelle, permettant la combinaison utilisée la plus productive. La prise de conscience des possibilités d'améliorer la mobilité et de réduire les charges administratives a produit plusieurs initiatives transfrontalières entre États membres voisins. Ces derniers ont (ou pourraient très rapidement) créer des conditions commerciales locales meilleures pour les entreprises et de meilleures conditions de mobilité pour les particuliers que celles existant avec d'autres États membres.

En outre, il existe un certain nombre de problèmes irréductibles qui profiteraient de résolution au niveau de l'UE. Il s'agit notamment de questions de respect de la vie privée, l'établissement de normes et procédures communes pour réduire la fragmentation et, surtout, une base juridique commune. Cela permettrait aux autorités publiques de demander, de fournir et de faire usage des informations fournies précédemment, et permettrait de faire face à des questions de charge (par

[11] Stratégie pour un marché unique numérique en Europe - COM(2015) 192 final, publié le 06/05/2015.

exemple le prix réclamé par les pays auxquels il est demandé de fournir des informations en vue de leur utilisation par un autre pays) et de responsabilité (par exemple pour des décisions erronées découlant de la réutilisation des informations inexactes ou obsolètes).

Conclusions

La présente étude: dresse un bilan de la réutilisation actuelle de données dans les interactions nationales et transfrontalières avec les administrations publiques; analyse les lacunes et les obstacles au principe numérique «une fois pour toutes» à l'échelle de l'Union; identifie les objectifs et les options politiques; et analyse leurs impacts sur les principales parties prenantes dans le cadre de différents scénarios possibles (compte tenu des circonstances très différentes des entreprises et des personnes physiques.) Nos constatons:

1- un large soutien (c'est-à-dire, dans la plupart des états membre) au PUFT en général, mais de grandes différences de maturité dans l'ensemble de l'Europe;

2- de nombreuses initiatives et mesures législatives susceptibles de simplifier la mise en œuvre du PUFT à l'échelle de l'Union;

3- des lacunes significatives de preuves sur les coûts et les avantages, en particulier au-delà du niveau d'un État membre.

L'option basée sur un «encouragement proactif» et les trois recommandations concrètes, y compris la proposition d'une task-force d'Etats membres de l'UE pour promouvoir l'apprentissage mutuel et une convergence et une coordination appropriées, l'approche fondée sur l'interconnexion[12] des registres de base pour garantir un partage efficace et une base juridique pour l'échange de données administratives en vertu du PUFT sont susceptible d'apporter l'impulsion européenne transfrontalière la plus efficace à la mise en œuvre du PUFT et à des progrès équilibrés et durables dans la mise en place du PUFT dans tous les États membres.

En l'absence de toute action, les opportunités ne seront pas saisies et la situation deviendra plus fragmentée, ce qui donnerait lieu à des discriminations entre les

[12] Certains documents font référence à la mise en place d'un système de registres de base qui intègre l'interconnexion, des dispositions en matière d'accès et une description sans ambiguïté du contenu des données, des sources et de leur qualité comme une approche fédérée, en particulier lorsqu'il stipule une seule source faisant autorité pour chaque donnée spécifique. Pour éviter toute confusion avec le sens politique du terme «fédéré», nous évitons de l'utiliser dans ce rapport.

individus et entre les entreprises selon l’existence et la nature du PUFT à l'intérieur ou entre Etats membres.

Table of Contents

I. Introduction

Individuals who want to benefit from the opportunities provided by the European Single Market for travelling, working, doing business and living abroad and businesses that want to conduct business across borders are generating significant demands for public services in cross-border situations. Public administrations are expected to deliver services in order to guarantee that - in the framework of the European Single Market - transactions requested by non-national users are not disadvantaged by unnecessary administrative burdens. Public administrations require data in order to be able to provide their services. While recognising that data can be obtained in many different ways[2], implementation of the Once-Only Principle (OOP) leads to a reduction of the administrative burden as information only needs to be provided once to a public administration, and as public administrations have to receive and validate it only once.

When done at European level and in particular in cross-border interactions with public administrations, OOP can provide significant benefits in terms of time and cost savings for those who request services and for public administrations, whose service provision stimulates mobility. In addition, the further processing of these data to provide those services can help ensure that the advantages of OOP are available within Member States as well, by increasing the utilisation of information assets, identifying inaccuracies and fraud, identifying and disseminating good practice, providing necessary framework conditions and enablers and aligning the costs and benefits with broader policy objectives defined and pursued at European level.[3] However, there are potential drawbacks as well: the legal basis for OOP is not yet complete, producing uncertainty regarding such matters as the competence of authorities to retain and further process data for OOP purposes; the incidence of costs and burdens for filling data requests on behalf of other countries and liabilities arising from inaccuracy or inappropriate reuse of data are not fully understood or clearly resolved; and the very different levels of demand experienced in different countries contribute to different speeds and forms of OOP implementation.

Our findings indicate that implementation of the Once-Only Principle throughout European Member States is still evolving and fragmented; experience with cross-border implementation is limited to a few services and cross-border arrangements between individual Member States. Thus it is not yet a principle.

As a consequence there is little quantitative evidence of OOP's costs, benefits and wider advantages, beyond a narrow and non-representative sample. It is clear that the benefits and costs of further implementation throughout Europe will vary greatly depending on the current state of OOP in Member States. It is also

important to recognise that costs for providing OOP data will be higher, and benefits lower, as long as OOP is not ubiquitous, yet.

The present study on "*EU-wide digital Once-Only Principle for citizens and businesses: Policy options and their impacts*" has: taken stock of the current situation regarding data re-use in national and cross-border interactions with public administrations; explored the gaps and barriers to implementing OOP EU-wide; identified possible ways to proceed; and assessed impacts on key stakeholders of various policy options, taking into account different futures. In doing so, we have also taken account of the different circumstances of businesses and of individuals (natural persons).

Due to the broad scope and applicability of the Once-Only Principle, this analysis focuses on a selected set of service contexts (functionalities) to form a more precise impression of data and information re-use initiatives and practices. This approach ensures a valid basis for comparison across countries and makes it possible to map use and re-use of information to their impacts on e.g. administrative burdens.

The analysis and findings are presented in accordance with standard inception impact assessment methods. Chapter II presents the problem and Chapter III explains why action at European level is justified. Chapter IV identifies general and specific policy objectives.

This leads to a range of candidate measures to help OOP implementation and to overall policy options based on them. These are summarised in Chapter V and the measures discussed in detail in Annex X. Their evaluation, taking into account key uncertainties that would have an important influence on how the different measures would work over the years to come and considering impacts on the main affected parties and stakeholders, is presented in Chapter VI.

From this, conclusions are drawn and presented in Chapter VII, together with recommendations for the way forward and candidate actions to support this way forward.

Please note that in this document, the term 'citizens' is often used to refer to natural persons as distinct from businesses (see further discussion in Section III.A). This is not meant to imply that the scope is restricted to citizens of EU Member States; data protection is a fundamental right and independent of citizenship and the bulk of services and information processing covered by OOP is not tied to citizenship status. It is intended to refer to the 'data home' of natural persons, which may be their country of citizenship or where their work visas, asylum application etc. were first registered

As a matter of interpretation, note that the terms ‘processing’ and ‘further processing’ are used throughout to refer to the whole gamut of OOP processes (e.g. collection, storage, computation, transfer, etc.) where no confusion will arise. This is consistent with the way the terms are used in the General Data Protection Regulation (GDPR). We also use the terms data referent, data requestor and data supplier to identify the parties in the OOP process. For more detail on the relation between OOP and GDPR see Annex VII.

A Glossary covering these and other terms is presented as an annex to this report (Annex I). Other annexes provide methodological descriptions, detailed research findings and extended discussions of specific issues.

II. What is the problem?

Costs of resubmitting data to public administrations can be high for businesses and individuals (the most quoted are those concerned with tax related obligations[4]). These costs and other burdens may affect service uptake, quality and consistency across borders and therefore the attainment of common European objectives and in line with the Treaty on the Functioning of the European Union[5], which calls for reduction of any potential distortion of market competition (including administrative burdens).

Action 16 of the Digital Single Market (DSM) strategy calls for improved cooperation among national systems to ensure that "businesses and individuals only have to communicate their data once to public administrations" and that in consequence governments will no longer make "multiple requests for the same information when they can use the information they already have" – again assuming that if another Member State's government within the EU has the information, all other Member State governments could/should have access to it.

In the Public Consultation for the eGovernment Action Plan 2016-2020 (under which the OOP is expected to be enforced), the principle is described as requiring that members of the public and individuals/businesses should not have to supply the same information more than once to public administrations.

To this end "Public administration offices [have to, ed.] take action to internally share this data, respecting data protection rules". Indeed, the implementation of OOP requires definition and application of technical and procedural solutions and strategies to make it possible to transfer and reuse data relating to a single subject (individual or business) for more efficient provision of public sector services. The aim of this initiative is to eliminate or at least reduce unnecessary administrative burdens caused by multiple submissions of the same data and information[6].

A. The problems OOP seeks to resolve

The problems that OOP seeks to resolve are indirect consequences of a range of connected developments in practice and policy and are sometimes deeply rooted in local historical developments, including:

- The growing intensity of information flows between governments on one side and businesses and individuals[7] on the other[8];
- The greatly varying costs, burdens and other potentially adverse impacts on different Administrations that are connected with the need to provide this information in authoritative and consistent ways[9];

- Differences among the rules governing the processing of data that may be regarded as personal, sensitive or standardised: not only in the abstract but specifically in relation to the 1995 Data Protection Directive (DPD)[10] and its successor, the General Data Protection Regulation (GDPR);
- increased information-intensiveness and complexity of individual and business interactions with governments associated with more personalised and effective service provision;
- increasing cross-border personal and business mobility and activity within Europe, which creates a demand for access to public services and government systems; and
- growing reliance on and familiarity with ICT systems in public, private enterprise and civil society spheres, including among Europe's population, which creates enormous potential for further improvements to efficiency and effectiveness.

These problems are linked to a range of legal, organisational, semantic, technical and other issues related to OOP implementation[11]. Although the primary focus of this study is the EU-wide cross-border perspective, EU-wide progress is partly dependent on developments at Member State level.

Recognising that EU-wide implementation of OOP may impose significant costs before its benefits are captured, this study considers what policy options present a realistic way forward, and what costs and benefits should be expected (at EU and Member State level).

B. OOP and other principles

OOP is closely linked to other principles: the move from documents to data; the Whole Government and No Wrong Door principles; the scope and content of European Public Services[12]; fair information processing principles[13]; and security on behalf of subjects (including potential abuse of OOP).

The move from documents to data is a recognition that the functionality and potential of electronically processed information are not only at least as good as those of documents (especially those issued by public authorities) but in many significant regards go well beyond them, e.g. in providing assurance of authenticity, keeping track of when and how processing occurs, controlling security and keeping track of changes.

In this regard, it has been argued that information published by public authorities should be available to and used by other public authorities in place of requesting individuals and businesses to produce such information. This, of course, has limits; there is no reason why documents issued – but not *published* - by one administration should be available to other administrations. In essence, this

concerns access – there is a continuum running from unique paper documents at one extreme (the subject controls access; submission of the original is often required) to open publication (e.g. a public register).

The Whole Government Principle is a form of 'one stop shop' – it typically involves services intended to ensure that all relevant services and offices are informed of necessary information provided by individuals or businesses and have taken appropriate action after they are first notified.

The No Wrong Door principle extends the Whole Government Principle by allowing information to be 'entered' into public administration databases through a wide variety of channels and offices14.

The Fair Information Processing Principles have been expressed in a variety of ways and contexts, including the GDPR. They include principles such as purpose limitation and requirements that data processors will use the minimum data required and hold them for the shortest possible period. These requirements are strongly connected to OOP, as discussed further in Annex VII. They may also be understood as imposing on governments – acting as data controllers – particular responsibilities for ensuring the security of data they hold about and on behalf of individuals (as dealt with by GDPR) and businesses.

C. The problem of EU-wide implementation of OOP

If OOP is adopted as a general principle, there will be losers as well as winners. In principle, it might be argued that existing (European and national) initiatives are expected by those involved to provide net benefits. Those not pursuing such initiatives may be unaware or unconvinced of the potential benefits, or may be deterred by administrative and organisational 'entry barriers.' Some may even have decided that the costs and risks outweigh the benefits. If OOP is adopted or enforced as a general principle, those parties may well incur net costs.

Because the adoption of OOP at Member State and bilateral level remains somewhat patchy, it is likely that the countries and services for which the benefits most obviously exceed the costs are those in the vanguard of current practice, and that filling in the pattern by including more countries, services and types of data, or making the location and re-use of previously-submitted data more 'automatic' from the business or citizen perspective may face considerable obstacles.

It will therefore be important to prioritise steps forward to align expected results with priority policy objectives, urgent societal challenges and situations where investment will be rapidly recouped through tangible economic benefits. Ultimately, each step is to lead to better alignment of costs and benefits, and bringing the costs down and benefits up.

The interpretation of 'Once-only' varies from country to country; this difference in interpretation may be the source of further delay. In some countries, Once-Only is closely linked to formal legal requirements that data submitted to government may be *stored* once only[15] (in a unique and authoritative database) regardless of how many times or in what context they were provided. Other versions of the principle stipulate that the data need only be *submitted* once, but do allow for (or even enforce) multiple records of the same data[16].

More specifically, a 2015 study[17] found that only a few countries have instituted 'hard law' mandates for OOP *as a principle*. 27 of 33 European countries and 24 of the EU28 Member States had begun OOP implementation. In the EU28, 12 countries had both a strategy and implementation initiatives, one (ES) had only a strategy and 7 had initiatives but no overall strategy. 12 countries gave OOP specific formal standing in dedicated statute law, while 6 reported no specific legislation.

Most EU countries that have some form of OOP apply it to citizens' personal data; a slightly smaller proportion use OOP for business identification data ad considerably fewer states use OOP for geographic, fiscal and health data. In most (but not all) cases, this data re-use is backed up by a legal identification of authentic sources.

Implementation costs – and the mixture of benefits to be expected – vary with interpretation, with the extent to which OOP is implemented on a centralised or standardised basis and with the degree of central endorsement and funding. This is particularly marked in cross-border contexts, where multiple interpretations may prevail.

For instance, a once-only storage requirement may prevent a Member State from having a record of data pertaining to cross-border service users; at least, there would be some uncertainty concerning the 'migration' of the single authoritative record from one country to another. If the costs of providing for use of data from another administration or of providing such data to another administration 'belong' to a single office at the service provider (rather than national level) and the benefits accrue more to the citizen or business or to the national or European level, delay or distortion may result from either a failure to net out the costs and benefits in making the business case for OOP or to opt for a low-cost modification of a local system in preference to a more standardised or harmonised system that operates

in a uniform way across the entire national (or European) public administration layer.

At this general level (applying to European citizens and businesses at EU level and below), many of the potential direct beneficial impacts and the indirect, collective and eventual contributions to overall welfare are plausibly limited, distorted, delayed or inequitably divided.

Many of the studies that have been conducted around this issue, and around closely related topics such as eGovernment and Interoperability have traced this problem to a structured set of *barriers*. This is a framing of the problem, rather than a diagnosis; the analyses conducted note that the solutions on which they focus *could* result in more efficient and equitable delivery of European Public Services and in this way to attainment of overarching European economic, societal and other objectives. But it is important to record that these solutions are not necessarily the only way to achieve these benefits, and that they do not develop or operate independently of each other.

D. Gaps and barriers to address

Key for identification of specific action opportunities is a deeper understanding of the gaps and barriers to address. We recognise these gaps and barriers can result from interoperability challenges of legal, organisational, semantic, technical and other causes. We also recognise that, whereas gaps can be resolved over time, some of the measures that are barriers towards easier OOP implementation may continue to be important to maintain, such as restrictions towards handling personal data. Such measures may benefit from revision where possible to facilitate OOP, or may be paired with other specific measures that help overcome such barriers for specific OOP purposes.

Table 1 summarises evidence from the analysis of gaps and barriers including findings from desk research (described in further detail in Annex VI).

Table 1: Gaps and Barriers

Categories	Gaps	Barriers
	Individual and business perspectives	National public administration perspectives

Categories	Gaps Individual and business perspectives	Barriers National public administration perspectives
Legal	• Complexity and heterogeneity of national requirement, procedures and competent authorities	• Heterogeneity of national legal frameworks • Privacy concerns • Data protection concerns
Organisational	• Costs of maintaining the in-presence procedure	• Tendency to cooperate with neighbour countries • Implementation driven by EU compliance • Complexity and costs of deployment and maintenance
Semantic	• Need for certified translation of documents and information	• Different concepts and contents of documents issued in other MS • Heterogeneity of metadata and data types included in base registries
Technical	• Heterogeneity of eID and eTrust services systems implemented at national level (in general lack of interoperability)	• Heterogeneity of technical infrastructures implemented at national level (e.g. Connecting distributed repositories vs. Retrieve of data from base registries) • Heterogeneity of eID and eTrust services systems implemented at national level (in particular eID)
Other	• Lack of political willingness	• Lack of bilateral/multilateral agreement for OOP implementation

III. The case for action at EU level

The OOP applies to data used by national, regional and local governments to provide public services. *Subsidiarity* and *proportionality*[18] restrict EU legislation to competences covered in the Treaty of the Functioning of the European Union (further: TFEU). We are not in a position to provide a formal legal analysis, but it seems likely that EU competence could be asserted if there were strong Single Market (especially for businesses) or fundamental rights (for individuals) implications and evidence that equivalent action or protection would not be consistently and effectively provided by Member States. This may come down to a quantitative question; willingness of a Member State to implement cross-border OOP as data requestor or supplier might depend on expected level of demand (for services or data).

On the other hand, OOP is closely linked to policy objectives within EU competence, which provides a *prima facie* case for EU action to *ensure* uniform and non-discriminatory cross-border access to services (especially 'European Public Services' – see definition on page 60). Also, the (perceived) barriers noted in Chapter II.II.D suggest that national initiatives might not converge to provide uniform OOP implementation within single countries[19], let alone cross-border. Different implementations, even if they offer equivalent levels of service, may fail to offer sufficient interoperability, ease of use and transparency.

EU-wide Cross-border OOP should be viewed as a way to enhance the Single Market through enhancing personal and business mobility and as a stimulus to universal application of OOP throughout the Community. The mobility argument allows the EU to act on its own behalf; the stimulus involves the EU providing leadership and coordination to Member States. In either case, the EU itself rarely requires information in order to provide services to individuals and businesses, so both justifications rely on OOP in the Member States.

The case for OOP would be simpler if the EU and the Member States shared the same priorities. The most commonly-cited reasons for OOP at Member State level are (in roughly this order) fraud reduction, administrative simplification, burden reduction and service improvement. These are not direct EU competences.

OOP can produce trans-European added value, but making a case for intervention on this basis would require evidence that: clarifies the nature of this value; shows that intervention is proportionate in the sense that the benefits justify the costs (taking into account that costs and benefits may not be evenly balanced across countries); and that existing national efforts are unlikely to converge to deliver the

same value. The anticipated benefits are drivers of implementation, but do not compel EU action.

For example, a case for EU action to implement OOP to reduce burdens would have to show that burdens are too high, would be reduced by the proposed action and that other methods are less effective or incompatible, taking into account the costs and burdens of OOP implementation.

Other ways to 'make the case' for EU-level OOP action include:

- The Better Regulation Agenda[20], refers to reducing burdens and improving interactions between public administrations and businesses or individuals and specifically mentions repetitive and complicated information requirements;
- The Malmö Ministerial Declaration on eGovernment[21] (2009): "…public administrations can reduce the frequency with which individuals and businesses have to resubmit information to appropriate authorities";
- The eGovernment Action Plan[22]: "… public administrations should ensure that citizens and businesses supply the same information only once to a public administration. Public administration offices take action if permitted to internally re-use this data, in due respect of data protection rules, so that no additional burden falls on citizens and businesses"; and
- European Council Conclusions[23]: "Efforts should be made to apply the principle that information is collected from individuals only once, in due respect of data protection rules."
-

Case for EU level action in summary

- OOP is clearly not an exclusive competence, but is linked to Single Market;
- MS-level efforts are uneven and not converging
    - More progress at EU level for businesses
    - Further progress would be particularly helpful to SMEs;
    - No progress may lead to increasing "discrimination" as bilateral arrangements are presently underway
- Cross-border OOP ultimately requires Member State uniformity of approach, and will thus lead to convergence of specific data administrations that are to be subject of cross-border OOP; and
- Action at EU level may produce additional benefits.

A. OOP applied to individuals and to businesses

The case for OOP and the constraints on its application differ between natural persons and businesses. This section briefly discusses important distinctions and indicates why approaches and solutions cannot be wholly separated. We note at

the outset that the amount of space devoted to these two types of OOP is not equal; business and individual OOP implementation have very different levels of maturity and homogeneity. For reasons of space, this report does not describe at length things already in progress (mostly on the business side); on the other hand, the report does try to discuss the subtle and hotly-contested personal data issues.

1. OOP for businesses

For businesses, information processing is linked the enterprise as a legally-defined entity. Most of the information used to provide public services to businesses is derived from formal activities (e.g. establishment of a business) and a matter of persistent public record. Many data elements are legally-defined and maintained in base registers. There are some limits to the presumption that data are public and can be further processed for all purposes for which they were originally processed; these include e.g. sensitive or proprietary information.

2. OOP for individuals

For individuals, information processing is bound up with data protection and governed in part by the requirements of the General Data Privacy Regulation (hereafter GDPR). Legal implications relating to the processing of personal data are discussed below. A more detailed discussion is provided in Annex III.

The primary legal obstacle to cross-border OOP, according to the stakeholders consulted, is the lack of suitable legal bases. Legal grounds for processing and the further processing involved in OOP are spelled out by the GDPR. But on its own, this may not give data requestors the right[24] to request information from other public authorities[25]. There may be no equivalence among i) data submitted for a specific purpose; ii) data previously submitted to authorities in the same country[26]; and iii) data or certifications obtained from public authorities in other countries. Conversely, public authorities who are controllers of such data might not have a legal basis for complying with requests for further processing despite the fact that the protection of personal data for natural persons cannot be used as a justification for restricting the free movement of personal data in the EU.

a) Processing of personal data

Article 6(1) GDPR sets out conditions for lawful processing, which include[27]:

- 6(1)(a) – *Consent of the data subject*[28]. Consent is specific to the processing context. OOP implementation involves further processing[29] where the data controller and purpose may be different. Controllers must fully inform[30] individuals *in advance* as to how data will be processed. Consent may be invalid if the processing is required but not necessary for provision of a service.

- 6(1)(b) – Necessity for *performance of a contract* with the data subject or steps preparatory to such a contract.
- 6(1)(c) – Necessity for *compliance with a legal obligation* under Member State or EU law which is binding on the controller, clear, precise and foreseeable[31].
- 6(1)(d) – Necessity to *protect the vital interests* of the data subject[32].
- 6(1)(e) – Necessity for performance of a task carried out in the public interest or exercise of the controller's official authority laid down in Union law or Member State law to which the controller is subject.
- 6(1)(f) – Necessary for the purposes of *legitimate interests*[33]. This cannot be used by public authorities processing personal data in the exercise of their functions. Instead, Member States can introduce specific provisions to provide a basis under Articles 6(1)(c) or 6(1)(e) for other specific situations (e.g. journalism and research). This is likely to produce variation across the EU.

b) Further processing

Most aspects of OOP as applied to personal data involve *further processing* - the processing of previously submitted data in new circumstances. The possibility of further processing may require consideration of whether the purpose of further processing is compatible with the original purposes. Article 6(4) of the GDPR sets out rules governing this assessment. Where processing is not based on consent or Union or Member State law relating to matters specified in Article 23[34] the following factors should be taken into account:

- any link between the original and proposed new purposes;
- the context in which data were collected;
- the nature of the data (particularly whether they are sensitive or criminal data);
- possible consequences of the processing; and
- existence of safeguards including encryption or pseudonymisation.

The limited provision for data transfers is of little relevance to public authorities[35]. Data controllers who process (or control the processing of) data for various purposes need separate consents for each purpose; the GDPR creates a presumption that bundling consents render them invalid.

Also important to OOP is the right of personal data subjects to demand erasure if the processing does not satisfy the requirements of the GDPR or if consent is withdrawn. Public authority data controllers must notify anyone with whom the personal data has been shared unless it would be impossible to do so or require disproportionate effort.

c) Data access and portability

Data subjects have the right to know what data are being held[36] that pertain to them and to gain access within one month. This is shorter than the DPD access period, and may impose significant costs on controllers, including organisational changes.

The GDPR also introduces the concept of *portability*. Subject to various conditions, most notably that the data are processed by automated means, data subjects *may* ask for their data to be provided in a commonly used electronic form. This could require data controllers to be able to handle digital OOP requests.

d) Sensitive data

Narrower conditions[37] apply to processing "sensitive" personal data[38]:

- 9(2)(a) - Explicit consent, unless prohibited by EU or Member State law;
- 9(2)(b) - Necessity for carrying out obligations under employment, social security or social protection law, or a collective agreement;
- 9(2)(c) – Necessity to protect the vital interests of a data subject who is physically or legally incapable of consent;
- 9(2)(e) - Data manifestly made public by the data subject;
- 9(2)(f) – Necessity for the establishment, exercise or defence of legal claims or processing by courts are acting in their judicial capacity;
- 9(2)(g) - Necessity for substantial public interest reasons on the basis of Union or Member State law, provided the processing is proportionate to the aim pursued and contains appropriate safeguarding measures;
- 9(2)(h) – Necessity for preventative or occupational medicine, assessing the working capacity of employees, medical diagnosis, provision of health or social care or treatment or management of health or social care *systems and services* on the basis of Union or Member State law or a contract with a health professional; and
- 9(2)(i) – Necessity for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.

The latter two grounds involve additional confidentiality requirements.

In two special cases potentially within scope of OOP national differences are likely to persist. Under Article 9(4), Member States can maintain existing conditions or impose new ones (including limitations) on the processing of *genetic, biometric or health data*. By contrast, *data on criminal convictions and offences* are not sensitive under GDPR, though they currently are in some Member States (e.g. the UK's Data Protection Act). In this case, Article 10 of GDPR provides that that such data may

only be processed under the control of official authority or where processing is authorised by Union law or Member State law that provides appropriate safeguards.

e) Other affirmative requirements

The GDPR requires public authorities *actively* to comply with all its obligations. Among other things, they must implement: data protection by design; staff training programmes; privacy impact assessments; and an audit of all personal data held. Therefore, for the purposes of OOP for individuals, the GDPR implicitly delivers many of the necessary building blocks.

3. Limits to the separation

Given the separate legal bases for processing data pertaining to businesses and personal data, it is tempting to separate options for "business OOP" and "personal OOP". However, this separation is not absolute. Consider the following examples.

Natural persons may be considered businesses e.g. when registering as self-employed or as single-employee businesses. Rising proportions[39] of the population are taking advantage of this status, including in cross-border contexts. This also applies to members of Europe's 5000 or so regulated professions.

Conversely, much business information involves personal information. Some national registries include personal details of officers; information about employment law and social contributions may include data on employees (natural persons) – though probably not at base register level[40].

4. Coda: European Interoperability Framework (EIF)

Many of the changes necessary to implement OOP at EU and Member State level and many others that facilitate OOP are prescribed in the European Interoperability Framework. This is currently under revision; the new version seems likely to make even more explicit the relation between interoperability in general and the specific forms of data interoperability needed for OOP. Pending release of an official version of the revised EIF, we summarise these in Annex VIII. When finalised, they should incorporated in the baseline option (Option 0 below).

IV. Objectives for EU-wide action

The considerations above lead to a potential general policy objective.

> *The general objective of cross-border OOP is to facilitate the integration and efficient operation of the Single Market and cohesion of the European Union by reducing or removing barriers to cross border business activity and mobility of individuals within the Single Market.*

Specific objectives associated with this include:

- Pan-European implementation: to encourage the implementation of OOP at a European level;
- Burden reduction: to reduce administrative burdens and delays associated with data-intensive service requests;
- Fraud reduction: to minimise the extent and improve the detection of attempts to obtain services by means of inaccurate or contradictory information;
- Non-discrimination[41]: to reduce asymmetries between the treatment of domestic and cross-border individuals and businesses seeking services that require them to submit information to public authorities; and
- Ubiquitous service improvement: to encourage the ubiquitous deployment of further processing of information within Member States in order to reduce the costs and burdens associated with public services while creating incentives for improved services.

V. Candidate Measures and Options

Given the vast array of contexts where OOP is applicable and its status as an architectural principle as opposed to a concrete or separable policy, it is appropriate to consider the possibilities for intervention on two levels; specific measures that might be implemented and general policy options or orientations. In this chapter, we briefly summarise the former, before discussing the latter in more detail. A more extensive discussion of the measures is provided in Annex X.

A. Measures

The specific measures considered in range over legislation, 'soft law' interventions (including standards and guidelines) and indirect support such as R&D and the improvement of framework conditions. While they are for the most part pitched at European level, they also involve a wide range of stakeholders, including the European Commission, Member State governments, industry players and associations and independent regulatory bodies. They are briefly discussed below.

1. EU Regulatory and legislative measures

Legislation offers the advantages of legal compulsion, clarity and unambiguous and consistent interpretation. It also signals political will and commitment, given the time, expense and complexity of changes. Moreover, legislation has invariably been subjected to extensive and transparent scrutiny, involving stakeholder consultation and full impact assessment.

Its potential drawbacks overlap with its advantages; it is difficult to reverse, even in the face of contrary evidence. Beyond that, the legal force of its provisions will censor evidence relating to possible improvements. A further drawback is that laws may not accurately reflect rapidly changing technological or operational realities and thus may not be future-proof or technologically neutral. Finally, legal sanctions focused on objectives such as burden reduction may create incentives that conflict with public service objectives and may be difficult credibly to enforce on public administrations.

Based on the evidence collected, and taking into account further implementation of the new GDPR, a Directive to further clarify the purpose and legal base for exchange of data including personal data in the context of OOP is an important pre-condition, whatever strategy would be chosen to pursue EU-wide implementation of OOP; legal uncertainty surrounding the implications of prior and current privacy laws was cited by many of those interviewed as a significant concern. In particular, to avoid discriminatory outcomes, such a legal base must operate in a symmetric and consistent manner across all Member States. Moreover, clarity and legal

certainty are required to prevent 'precautionary' distortions of data re-use regarding specific country pairs, purposes or data types. In particular, a clarified and harmonised (at EU level) concept of user consent as it applies to OOP may help to overcome remaining data protection issues. Finally, such a Directive should not be limited to the further processing of personal data both because competent authorities currently do not have uniform or harmonised power to request, supply and use shared data for all relevant non-personal data and in view of the complexity of separating personal vs. non-personal data from natural person vs. business data subjects or beneficiaries. Such a Directive could be comparable to the "Police Directive" on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (Directive (EU) 2016/680) – see also the exceptions in Article 23 of the GDPR. Such a legal base could establish a common starting point for managing issues of legal competence to process (request, store, supply and re-use) information and for dealing with liability issues. An example of the sort of structure that might serve is provided by the concept of 'authentic registers' that is discussed further in Annex IX. The Directive could, on this basis, specify in detail how to deal with issues of dispersed liability and responsibility (i.e. as data – including non-personal data - move through multiple controllers and jurisdictions) and make suitable provision for data that do not meet the conditions of reference or base register data (see discussion in Annex IX).Other legislative action could involve Regulation to e.g.

- Mandate *interconnection*[42] of specific types of authoritative data source;
- Compel Member State governments to implement and use (at least permissively) a common European electronic Identity (or interoperable identifiers[43]). The eIDAS Regulation[44] stipulates mutual recognition but does not compel MS to have their own eIdentity, let alone one that is unified across the EU impose conditions for equivalence of documentary and electronic records; or
- Define services and contexts for which Member States are obligated to first consult existing records before requiring individuals or businesses to submit data. Absent specific EU-level provision of services, it does not seem likely that such Regulations could only be applied to cross-border requests, as opposed to being uniformly imposed regardless of country of origin or request. Therefore, they should be seen as enforcing OOP throughout Europe, and not just at cross-border level.

2. Encouragement and coordination measures

These include establishment of working groups and good practice exchanges, frameworks for interoperability, interconnection and access and technical and

operational standards. They also include demand and supply instruments, such as targeted public procurement or subsidies for costly OOP implementation.

3. Exploratory actions

These include new and modified pilots and support projects and data collection and analysis actions to improve the evidence base as to 'what works' and the impacts of different solutions.

4. Data sharing structures

Measures here include EU-wide sharing or interconnection for existing base registers, support for new registers and frameworks or structures for facilitating re-use of non-basic data in compliance with data protection and other legal requirements. In particular, they could entail measures to enhance structures for documenting data availability, locating necessary information and assessing its suitability, keeping track of how and when it has been used and ensuring its authenticity, accuracy and other aspects of quality.

5. Road mapping and sequencing

The implementation of any collection of measures (including at Member State level) will naturally evolve as evidence and experience accumulate and as individuals and businesses learn to take advantage of OOP possibilities. A suitable roadmap can help establish a 'glide path' or implementation trajectory in order to:

- Set targets, learn from experience, and adjust so that costs and benefits are optimised
- Build communities of practice to build awareness and readiness, collect experiences, experiment with alternatives and mobilise support on a peer-to-peer basis
- Allow time and space for developing effective and efficient burden- cost- and responsibility-sharing arrangements
- Adapt to changing circumstances, by moving to or away from coercive, shared, structured interconnection, etc. options as appropriate, knowing that both technological potential and societal need will continue to change;
- Spread disruptions and costs over time (this is essentially a 'real option' approach; if there is learning about OOP implementation, it makes sense to delay part of its implementation and to then expand, adjust, abandon or wait longer depending on how it plays out).

6. 'Blue sky' possibilities

Most of the above measures are already being pursued to some extent, at least in isolated instances. There are other possible interventions or approaches that could

lead to more radical versions of OOP implementation and more profound transformations of the relationships between public administrations and individuals and businesses.

These new possibilities arise when all public administrations eliminate or radically reduce their reliance on documents as opposed to the data and information they contain. Currently, moves in this direction must demonstrate[45] that the digital approach is *as good as* the document-based approach. But these new possibilities exploit the fact that, for many existing and emergent purposes, digital information can be *superior to* analogous documents. Data in digital form are easy to track over uses, space and time, to analyse and to update. The burdens associated with their capture and processing can be reduced to zero or even converted into advantages because the same data can be used for other purposes (reducing the total data collection requirement) and because their timely, costless and verified availability can enable substantial improvements in public services.

Below, we mention three examples. The first two concern automated real-time streaming of information from individuals and from businesses to public administrations, where it can be shaped to the needs of a range of functions (and thus re-used). They help build support for OOP by illustrating the unanticipated benefits of increased data reuse; continuously up-to-date data may make services more cost-effective and automated data collection and sharing can reduce the burdens of repeated and periodic reporting. The third concerns joint control of information suitable for reuse in OOP contexts and could obviate some of the quality and control issues that currently arouse concern.

Improved services based on continuous, real-time monitoring data (active eHealth): The provision of healthcare services is already being transformed by the availability of continuous real-time monitoring data. Initially these data were used asynchronously[46] by experts to detect emerging problems; more recently they have been used to make continuous adjustments in care (e.g. drug pumps that respond to fluctuations in patient conditions). They are also beginning to be used to transfer control and responsibility from providers to patients themselves, especially in the context of patients with chronic conditions[47]. The availability of real-time, interpreted information has been shown to have profound effects on patient behaviour and also to lead to more effective and economical ways of organising clinical care. This development goes hand-on-hand with consumer applications that support people in “staying healthy” by providing real-time feedback on exercise results and physical wellbeing.

Automated compliance verification and improved regulation (Regtech): Much business information requirements concerns the need to demonstrate regulatory

compliance (e.g. for employment, tax payments and financial regulation). The transformative power of real-time digital information in the business context takes the form of 'regtech' –automated streaming of information from organisations' information systems to public authorities, which monitors compliance and enables adjustments to ensure that requirements accurately reflect current conditions. New forms of regulation based on such information could reduce the deadweight loss associated with one-size-fits-all conduct-based rules and the wasted effort and potential for moral hazard (strategic manipulation) associated with periodic reporting – in short, enabling affordable and well-regulated customisation of public services.

Decentralised and shared control of information (Blockchain): Another transformative measure replaces concentrated control of and liability for data repositories and processing with innovative alternatives based on so-called Blockchain models, in which data are maintained as a public resource that anyone can modify but only with the consent of everyone. This provides substantial advantages in terms of accuracy and acceptability; technical means are employed to remove the need for asymmetric and potentially risky trust and authority structures – no more single point of failure. This algorithm-based service is currently attracting a lot of attention and is already disrupting traditional financial service models. It is worthwhile considering in the OOP context, especially in cross-border situations where such 'trustless' structures may be an attractive alternative to complicated legal and organisational arrangements.

B. Options

Below we describe the baseline option (no new initiatives: Option 0) and three alternative options for moving forward towards OOP implementation.

- Option 1 – Legislative approach, in which emphasis is on prescribing implementation;
- Option 2 – Proactive support approach, based on establishment of a Commission supported European Task Force to actively set goals and actions for moving forward;
- Option 3 – Responsive approach, in which Member States are encouraged to progress OOP and EU-wide action will be taken by the Commission as and when asked to do so by Member States.

Please note that each of these options is predicated on the prior implementation of a Directive establishing a legal basis for the further processing of data referring to natural persons and businesses where such processing would operate for the benefit of the data subjects and where such processing is limited to enabling the use of the data in place of equivalent data that would otherwise have to be

provided by the data subject to competent authorities. In particular, the Directive would clarify the protection of natural persons with regards to further processing of personal data by competent authorities. For each of the options we will describe the option as compared to the Baseline Option (Option 0) which is described first. Note also that Options 2 and 3 differ from Option 1 in using non-legislative measures to do the 'heavy lifting' of encouraging adaptive OOP implementation going beyond what the law, with its requirements for uniformity and unambiguous description, can usefully do at this stage of such a dynamic development.

7. Option 0 – no further action

This option continues[48] existing Member State and bilateral initiatives along with current and planned European initiatives such as the ISA^2 programme[49] and the eGovernment Action Plan's large-scale pilot (for businesses) and coordination and support action (for individuals). It follows the planned timeline[50].

The baseline scenario assumes that these activities will continue to develop and spread, generating common understanding and evidence, especially of impacts.

The elements of the actual scenario of EU-wide OOP implementation

Looking at the baseline scenario corresponding to Option 0, the *framework conditions* are part of the landscape in which cross-border OOP takes place, i.e. the status quo. ***Key factors*** are to be taken into account *as* baseline elements which improvements positively affect the framework conditions. Each of them is not sufficient in itself yet will contribute to enabling implementation of EU-wide OOP, but in absence of a specific top-down EU policy they may positively and gradually contribute to re-use of data in Member States.

In the EC (2014) *"Study on eGovernment and the reduction of administrative burdens"*[51] two of the four identified building blocks, *Interoperability and data exchange* and *Base registries*, were considered as significant key factors for the OOP implementation (respectively [KF1] and [KF2]). From the experience of the Connecting Europe Facility (CEF)[52], where building blocks are defined as *"basic capabilities that can be used in any European project to facilitate the delivery of digital public services across borders,* "all the identified building blocks[53] have been brought together in Key Factor 3 e*ID and eTrust services [KF3]*.

In this representation, a second element has to be considered: ***enablers***. Enablers are means/tools that can facilitate the implementation of the OOP. In practice they are realised through measures and initiatives set at local, regional, national, bi-lateral, multilateral and European level to tackle legal, organisational, semantic and

technical gaps and barriers and to create the framework conditions for effective cross-border public services.

Enablers can be classified by key factor[54]:

- For *Data exchange [KF1]:* Data protection, data quality, administrative collaboration and re-use of data, legal requirements, technical architecture, language solutions, semantic solutions
- For Base registries [KF2]: base registries
- For e*ID and eTrust services [KF3]*: electronic identification (eID) systems, trust.

Action of enablers on key factors in the direction of the implementation of an EU-wide OOP is brought together in figure below.

Current significant initiatives and measures on which enablers have been realised are reported in Annex V, while the other policy options presented in the next paragraphs address also the potentialities of specific initiatives for EU-wide OOP (i.e. interconnected base registries).

It also assumes the continuation of existing national and domain differences in the definition, scope and implementation of OOP and the legal, organisational, semantic and technological gaps, barriers, building blocks and drivers[55]. It is expected to generate (unpredictable[56]) changes in organisational culture.

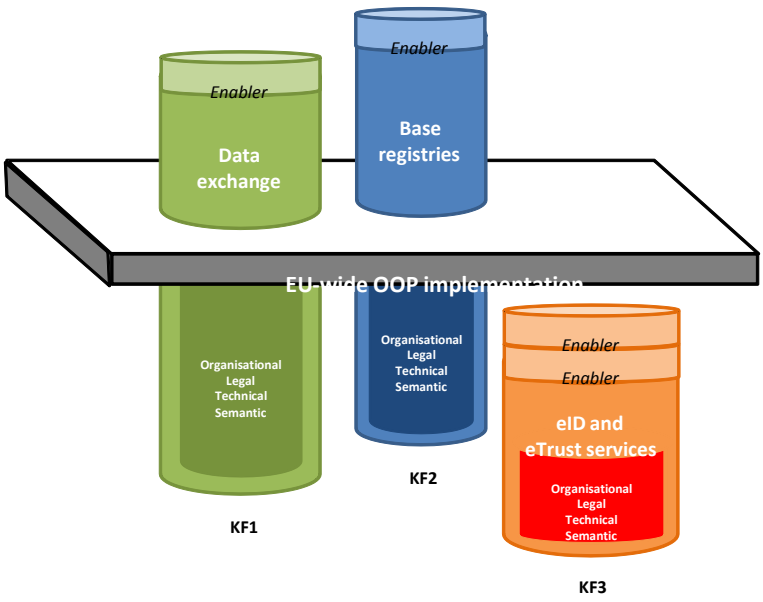


Figure 1: Contribution of the enablers to key factors for the EU-wide OOP implementation

Rationale: the present state of knowledge and mutual understanding may not support more definitive action, and may pre-empt or distort existing initiatives.

Advantages: minimal delay, no additional cost or administrative burden impact, no further complication of regulatory and policy reform measures in specific domains.

Disadvantages: does not fully respond to high-level endorsement, leaves open the possibility that OOP will only be implemented in a non-uniform way and that cross-border applications (where the benefits to individual businesses and individuals are potentially greatest) may be made more difficult by national difference. May not accelerate the complementary 'whole of government' or 'one-stop shop' approach to service delivery[57].

Measures involved: implementing and delegated regulation, especially relating to: the eIDAS Regulation; joint action with ISA[2], eGovernment Action Plan, etc.; planned standard and framework development[58]; and technical data coordination[59] support.

8. Option 1 – Legislative approach

This option would regulate to ensure that specified services (those that are by Treaty available to individuals and businesses from anywhere in the EU) must include an OOP default option – in other words, they should only ask individuals for data that have not been previously submitted to a public administration for equivalent or analogous purposes.

Rationale: some legal barriers require formal remedies. In addition, the legislative approach ensures coherent balancing of OOP with privacy and other issues by legislative scrutiny, analysis and negotiation. Finally, this approach leads to consistent, uniform, proportionate and approximately simultaneous implementation.

Advantages: clarity, compulsion, lack of ambiguity, universality, signal of commitment, extensive scrutiny and consultation, used to 'fix' lags.

Disadvantages: hard and slow to adjust, self-censoring, requires enforcement.

This option may be resisted by Member States, especially those for facing substantial costs of system modification or extension and those more likely to provide than to request information. For this reason, the option may take 7 or more years to negotiate, enact and fully implement. This may change, assuming progress within all Member States on their own data organisation and better use of technologies.

Option 1 entails the following requirements.

- Requirements for the EU:
    - Identify public services and purposes to which OOP must or may apply (e.g. a codified list based on the concept of European Public Services);
    - Establish individual and business rights to opt-out[60] of OOP procedures;
    - Collect and maintain a meta-registry[61] of basic and non-basic data sources;
    - Mandate interconnection e.g. by legislating measures in policy areas related to specific registries to compel Member States to implement and use (at least permissively) effectively unique European electronic identifiers[62]; and
    - Extend and unify existing legal bases[63] for data-sharing, information exchange and interoperability at legal, organisational, semantic and technical levels to all types of data for which OOP is useful. Legal interoperability should establish or qualify cross-border equivalence of master data and define the links, mapping or translation functions used to connect sources and databases holding ostensibly equivalent data in different Member States.
- Requirements for data requestors[64]:
    - check their forms, processes and protocols against the data held in registered databases;
        - use those data when available;
        - review their forms and possibly limit data requests to data generally provided;
    - verify and certify compliance with legal, organisational, semantic and technological interoperability requirements[65];
    - check to see whether legally acceptable data exist for specific service recipients and whether suitable consents are in place;
    - where the data exist and consent has been given, collect the data and use them to satisfy procedural requirements[66];
    - where the data exist but consent has not been given, obtain verifiable consent and collect the data; and
    - give the individual or business concerned the opportunity to review and amend those data.
- Requirements for data suppliers:
    - Supply data catalogues describing the contents, provenance, quality/reliability and permitted/excluded uses of data they hold; and
    - Make specified data available for re-use.

Optionally, the list of services and the scope of required data could be extended to within-sector, cross-sector and cross-MS OOP implementation by incorporating it into existing Directives and Regulations for specific service sectors.

Below EU-wide level, further legal safeguards for OOP and an optional strategy for overcoming legal barriers to implementation can be provided by explicit data sharing contracts or statutory codes[67] covering the following issues:

- What information can or must be shared;
- What information can be required;
- The organisations involved;
- What the parties need to disclose or whom to notify about information sharing;
- Measures to ensure adequate security and safeguards are in place to protect the information;
- What arrangements need to be in place to provide individuals with access to information submitted by/about themselves;
- Agreed common retention periods and trustworthy secure deletion methods.

9. Option 2 –Proactive Encouragement

Proactive encouragement of and administrative support for OOP[68] includes such measures as recommendations, opinions, communications, notices, and guidelines issued by the European Commission[69]. Traditionally, governments find such 'soft law' an attractive alternative to formal legal obligations and the ratification requirements of the legislative approach, especially in international contexts or where competence and subsidiarity do not clearly justify coercive approaches.

Recommendations can help Member States to set up sound and consistent master data policies as a preliminary step towards OOP implementation and more generally to improve and rationalise data management. Given appropriate policies, this makes it easier to establish interconnected networks of Base Registries. Specific recommendations are laid out in the revised EIF draft and other places[70].

Many current EU measures provide proactive encouragement. An example is the eID Building Block under the Connecting Europe Facility. The eIDAS Regulation 910/2014 does not oblige Member States either to implement eID schemes or to 'notify' (open for use by other Member States) any eID schemes they may have, but does make these steps more attractive[71]. The Communication on Online Platforms and the Digital Single Market Opportunities and Challenges for Europe[72] endorses proactive encouragement for trust, transparency and fairness when it says[73] "In order to empower consumers and to safeguard principles of competition, consumer protection and data protection, the Commission will further promote interoperability actions, including through issuing principles and guidance on eID interoperability at the latest by 2017. The aim will be to encourage online platforms to recognise other eID means — in particular those notified under the eIDAS Regulation — that offer the same reassurance as their own."

Option 2 would extend these to encourage:

- incremental progress along the lines of greatest benefit;
- capture and analysis of information on costs, benefits and responses;
- development of common platforms, standards and solutions;
- transition from data sharing practices to the OOP as a principle; and
- convergence at appropriate levels.

This stepwise approach will sustain progress toward OOP; each step makes the next easier. It *will* be slower than option 1, but should ultimately be better and cheaper.

Rationale: Data re-use initiatives come where benefits clearly exceed opportunity cost[74] and reflect the different services sought. Diffusion and ubiquitous adoption are hampered by lack of incentives and resources and (especially cross-border) the difficulty of OOP arrangements among countries or authorities at different levels of development. Benefits can be anticipated from *bottom-up innovation* ('natural experiments') in specific sectoral and regional contexts and *interconnection* (joining-up local initiatives), including better 'fit' to local conditions, horizontally applicable approaches and higher levels of compliance[75]. However, bottom-up diversity might weaken interoperability, efficiency, fundamental rights or compatibility for cross-border extension of successful pilots to other areas. Thus, common principles-based ground rules should be established and used to mitigate risk without restricting innovation.

Advantages: attractive alternative to formal legal process, esp. internationally; allows efficient realignment of responsibility; facilitates sharing of costs, burdens and liabilities[76]; helps align Member State and regional developments; flexibility in the face of future changes; greater and/or less costly acceptance and compliance.

Disadvantages: ambiguity (esp. Guidelines); risk of mission creep[77], capture and loss of effectiveness; fragmentation, need for legal basis and incentives to promote conformity to the recommendations for interoperability in the (revised) EIF.

Option 2 entails the following, in addition to the common recommendation for a legal basis to allow data controllers to make and comply with OOP requests from other countries on the same (or better) footing as information directly supplied by data referents or data controllers in the same country:

- EC participation or leadership in development[78], evaluation and promulgation of standards and codes[79];
- EC informational support[80] for binding codes of conduct;
- Use of codes and standards in EC-level activity[81];

- A catalogue of base registries, giving details on their contents, formats, information quality and means of access; and
- Encouraging[82] public administration stakeholders to
    - comply with applicable codes and standards
    - explain why they are not complying or
    - provide proof of equivalent functionality and interoperability.

10. Option 3 – Responsive Assistance

Option 3 seeks to harness and spread Member State- and sector-specific initiatives in a way that is more responsive than pro-active but retains its shaping influence and power to generate economies of scale and scope. It combines legal adjustments, proactive encouragement and concrete support measures.

Rationale: Proactive encouragement measures in Option 2 encourage or impose common approaches, but are largely limited to 'talk' (recommendations, guidelines and other forms of advice). OOP implementation might be enhanced if it is seen to be adaptable to local conditions[83]; concerns about informational control can be eased by giving stakeholders greater ownership of the process. However, organisational barriers (esp. resources and cultures) can distort this. Local initiatives tend to focus on data re-use (hence service access and mobility) for particular groups of foreign individuals or businesses or cross-border services. There are inevitable trade-offs between reflecting the needs of specific ways of providing services or specific groups of beneficiaries on one side and eliminating barriers to cross-border service eligibility. Therefore, it cannot be concluded that a uniform approach is always best or that all local variation should be catered for. A 'steering' influence in disseminating proven solutions, supporting solutions of general applicability and helping to create common, open support structures and services can limit this risk while capitalising on the enthusiasm and initiative of early adopters and innovators.

Advantages: builds on current progress to refine approaches, to diffuse 'OOP culture' and to extend geographic, service and data reach; low cost and flexible; conforms to strict subsidiarity; draws on widest possible base or approaches and contexts; leads to more accurate and proportionate decisions on key aspects taken by stakeholders closer to the 'coal face.' To the extent that it includes 'Infrastructural services' measures[84] (see Annex X.I), it also enhances: information and policy consistency; rapid critical mass; uniform state of the art implementation (interoperability); and linkage with and reinforcement of the eIDAS Regulation (910/2014/EU).

Disadvantages: slow progress[85]; vulnerability to mission creep[86] and capture; divergence; and violation of financial and behavioural additionality[87]. If this option entails infrastructural services, disadvantages include subsidiarity and legal basis issues and financial, service quality and liability risk.

Option 3 entails the following elements, in addition to the general requirement for a legal basis to allow data controllers to make and comply with OOP requests from other countries on the same (or better) footing as information directly supplied by data referents or data controllers in the same country:

- Analytic, organisational and administrative support to extend existing arrangements to more data, functionalities, services and countries;
- Providing 'comments' and other proactive endorsement;
- Mobilising supplementary or complementary finance for intermediary entities through existing funding and development instruments[88];
- Supporting R&I initiatives to collect, analyse and disseminate data on:
    - direct impacts and knock-on effects on public service efficiency
    - horizontal equity between domestic and foreign claimants and among Member States connected by OOP initiatives and
    - cross-border utilisation and effectiveness of OOP-enabled services to assess impact on cross-border mobility, competition, etc.

VI. Assessing the impacts

A. Affected parties

Various stakeholders are likely to be affected by the options. These stakeholders can be clustered into groups by role in implementing OOP and associated costs and benefits, using the mapping and interoperability implementation scenarios developed for the EIF. Interoperability is an input to OOP, which requires exchange of information between public administrations in different countries. It is also an outcome of OOP implementation, which reduces costs and burdens of information exchange between individuals and businesses and public administrations, creating incentives and capabilities to extend their scope, efficiency and effectiveness. Cross-border OOP strengthens civil society and business linkages among Member States, strengthening framework conditions for interoperability.

The EIF starts from concrete interoperability scenarios that overlap with the use cases (Annex III) and policy options (Chapter IV) and are sketched in Figure 2[89].

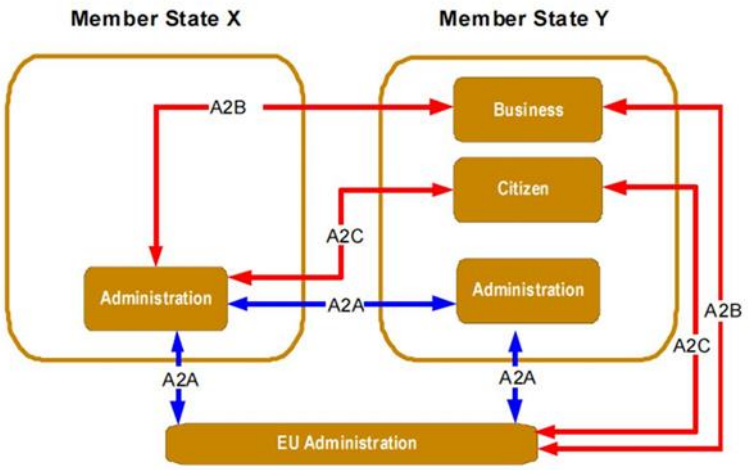


Figure 2: interoperability scenarios

Interoperability Scenario 1 - direct interaction[90] between an individual or business and a foreign government (A2B and A2C above, baseline option 0 below);

Interoperability Scenario 2 - exchange of information[91] among public administrations about an individual or business (A2A). This corresponds to the baseline scenario, options 2 and 3 and most of option 1. Indeed, OOP implementation involves transitions from Scenario 1 towards Scenarios 2 or 3; and

Interoperability Scenario 3 - exchange of information between public administrations and EU institutions. This has been primarily sector-specific, creating administrative networks required to share information according to centralised rules or via a centralised interconnection of databases. It is currently outside the scope of OOP implementation because it rarely involves information referring to particular cross-border service requests rather than statistical data for analysis and dissemination.

We identify broad categories of affected parties (Table 2) and impacts (Table 3).

Table 2: Affected Parties

General	Specific
Public administrations	• European Union • Directorates-General with specific sectoral remits; • Statistical offices and owners and operators of existing[92] databases; • Providers of data brokerage, search and other OOP-related services; • EU Regulators.
	• Member State • Public service providers who collect or request information; • Sectoral ministries who may need to choose required and alternative information and implementation strategies for specific aspects of OOP; • Owners, controllers and operators of base and other registries and databases who may develop and supply data catalogue entries and ingress, access and egress procedures for re-used data; • Providers of data brokerage, search and other OOP-related services; • Regulators[93] who will mediate legal and regulatory barriers and drivers.
Individuals	• Benefit claimants; • Recipients of public services (including information); • Subjects of reporting and information requirements; and • Subjects of legal and regulatory obligations.

General	Specific
Businesses	• Economic operators in national and European sectors and markets[94]; • Applicants for and recipients of subsidies and direct assistance; • Bidders for public contracts; • Recipients of public services (including information); • Subjects of reporting and information requirements; • Subjects of legal and regulatory obligations; and • Participants in industry bodies and co-regulatory arrangements.

Table 3: Types of Impact

Type	Details
Costs	• Economic direct costs – the unavoidable and immediate consequences of the option, in the form of equipment and imputed value of time; and • Economic indirect costs – costs arising from the actions of others, including spill-overs and pass-through from other sectors, and the consequences of reactions designed to minimise, mitigate or transfer costs[95].
Time savings	• Process time – time spent locating, collecting and submitting information, completing administrative procedures and specifying services to the appropriate level of detail (typically on the basis of information provided); and • Elapsed time – time needed to complete procedures from start to finish.
Simplification	• For public administrations, simplification has benefits beyond time and money savings. Note: opportunity costs of OOP processes must be measured relative to alternative uses of time, money and other resources involved and assessed in terms of whole-system costs. • Benefits to individuals and businesses also go beyond time and money; little has been done to capture these service-specific and general consequences of improved trust and other intangibles relating to interactions with government.

Type	Details
Service level and quality	• Specificity – how well services and processes reflect individual circumstances; • Reliability – service speed, effectiveness and consistency; • Complexity – cognitive streamlining of processes and resulting improved service requests, delivery and management ; and • Trust – confidence of users and providers in information and interactions.
Public administration intangible impacts	• Administration-wide simplification of information management; • Increased complexity of office-level operations or intermediary services; • Liability for accuracy and use of information (e.g. as data controller); and • Changes in control over data, budgets and service responsibilities.
Personal intangible impacts	• Service utility – requested services meet actual needs; • Improved mobility – impacts of real or possible cross-border mobility ; • Transparency and accountability – individuals and businesses can easily understand decisions and query inconsistencies ; • Data protection and privacy – informational privacy is respected and individuals retain a right to a private life ; • Security – data and service-related needs are consistently protected; and • Record-keeping and familiarisation – typically treated as time costs in Impact Assessments but OOP implementation adds intangible benefits by removing the need to maintain extensive and authentic records (in a variety of forms) and to become familiar with multiple procedural requirements simply to preserve the option to request services drawing on the same information.

Type	Details
Business intangible benefits	• Suitable versions of above personal intangible benefits; • Market access – reduced barriers and shorter response times for operating in other countries or across the Single Market in the form of lower costs, improved productivity, enhanced competition, faster and better innovation; • Avoiding procedural delays and mistakes ; • Non-economic and unquantifiable benefits of reduced information delay or inaccuracy – flexibility to implement changes, lower legal/reputational risks; and • Changes in organisational behaviours and structure – e.g. reduced need for administrative staff to manage records and navigate administrative procedures.

B. Evaluation scenarios

The term scenario is used in two senses; impacts are derived from the combined effect of policy scenario(s) and environmental (exogenous) scenarios.

In some cases, the environment can be quantified and a baseline forecast determined by trend extrapolation. Variants are obtained by changing key parameters. The baseline against which policy impacts are measured is formed from the 'no further action' policy scenario and the 'most likely' exogenous scenario.

In the present case, significant uncertainties are not quantified and their probabilities cannot be assessed. The baseline is a policy scenario (Option 0) described in terms of OOP adoption and performance independently of environmental influences on demand for cross-border services or impacts outlined in Table 3.

1. Baseline scenario

The current baseline scenario of EU-wide OOP can be described in terms of barriers, gaps, building blocks and enablers.

Table 4: Barriers, Gaps, Building Blocks and Enablers

Barriers
• Heterogeneity of national legal frameworks, esp. for some aspects of data protection[96] and security and property rights[97];
• Lack of effective national OOP in most Member States, heterogeneity;

• Lack of trust among public administrations for cross-border OOP;
• Lack of organisational models for data re-use in most Member States;
• Persistent and significant semantic interoperability issues including the diversity of concepts and documents issued in different Member States[98].
• Persistence of significant technical interoperability issues (e.g. diversity of data management systems[99] and lack of suitable eID system(s);
Gaps[100]
• Complex procedures involving multiple public authorities;
• Lack of common tools for access to non-base repositories[101];
• Lack of a unique and mutually recognised eID system[102] for individuals;
• Demand for certified translations of official documents;
• Difficulties in understanding procedures and regulations of other countries; and
• Costs associated with procedures that require face to face presence.
Building blocks
• Interoperability: legal, semantic, technical rather than organisational issues[103];
• Base registries[104]: will develop and consolidate without further intervention. This may (if evidence is shared) demonstrate OOP impacts even for non-basic data and cross-border settings, but may leave some gaps (Section II.II.D.);
• eID for individuals: national systems are not universal, homogeneous or mutually recognised, which constrains cross-border OOP implementation. eIDAS Regulation will require mutual recognition and ease this, but does not eliminate problems arising if citizens must be physically present to request local identifiers.
Enablers
• Activities to: identify and promote cross-border administrative collaboration (e.g. data re-use[105]); show proof of concept; reduce apparent risks and give access to existing OOP linkages. However, they are limited, do not fully detail practices and lack quantitative performance data. Incentives for improvement focus on low-hanging fruit; Member States may need strategic partnerships to benefit.
• Pilot initiatives for cross-border deployment of technical architectures[106] are more concrete and complete than good practice repositories, but countries must generally adopt them in place of whatever came before. This implies formation of technology-based clusters of Member States, able to interoperate at a high level within but not beyond the cluster[107] and formed around significant flows, hence different for personal or business data exchange.
• Current progress in consolidating data protection suggests that OOP implementation is unlikely to be distorted, though it may be retarded if (especially security) issues relating to data controllers in international contexts cannot be fully clarified[108]. EU data protection provides common high level of data protection; Member States may provide common cybersecurity baseline.

The baseline scenario is defined by these four elements, the need to reduce administrative, time and money burdens on individuals and businesses, behavioural consequences (cross-border opportunities foregone) and sunk costs and irreversible investments already incurred by public administrations[109].

2. Evaluation scenarios

The Baseline must take account of critical uncertainties e.g. current state and trends of Member State OOP, critical framework conditions, requirements for and advantages of specific OOP options and the impact of Member State OOP experiences for other countries and at European level. These, in turn, will influence the demand for cross-border services and the costs involved in moving towards cross-border OOP implementation at EU level and therefore the extent to which top-down vs. bottom up approaches will succeed and the impacts they will produce. To reflect these, we describe a limited number of variants, based on two major uncertainties:

Macroeconomic impacts on supply of and demand for cross-border mobility.

This encompasses three possibilities:

- Favourable: mobility in search of new opportunities, realising comparative advantages110, productivity gains and eventually111 easing public service burden;
- Negative: mobility away from countries experiencing greatest difficulties and towards advanced Member States, increasing demand for support while reducing tax revenues, commercial margins and societal and economic cohesion within and between Member States; and
- [possibly] Structural change: Union cohesion gives way to regional blocs with internal but not interregional mobility.

Interaction between Member State and European OOP-related developments.

National OOP implementation can both hinder and facilitate European OOP. This underlies subsidiarity; whether the EU has competence to mandate or drive OOP. It depends in turn on how successful or disappointing national experiences affect the willingness of Member States to cooperate in different types of OOP: hierarchically interconnected vs. decentralised; general vs. sector- and functionality- specific; and localised vs. standardised in legal, semantic and technical terms. Two polar possibilities are:

- Positive feedback: even different Member State OOP implementations create a common appreciation of benefits that justifies overcoming the resulting legal, organisational, semantic and technical barriers.
- Negative feedback: differentiated forms of OOP create interoperability barriers between countries and among services or public administrations.

Note that removing barriers to European OOP may not always be justified by the resulting form of European OOP or its contributions to Single Market objectives. If European OOP is *ipso facto* good or if its adverse effects can be compensated leaving a net gain, barriers should be removed, minimised or routed around. But a barrier is also a stimulus to further improvement.

For instance, if Member States collect different information for a given purpose, barriers to OOP implementation may lead to a minimal and common alternative that meets the needs of cross-border service provision. Moreover, European OOP may not be the only or the best way to achieve legitimate societal objectives. A 'light-touch' approach allowing small groups of Member States to agree OOP-like data interchange arrangements for the most-requested services may achieve greater cost and burden reduction or service improvement than a global approach[112].

Not all possibilities are relevant or consistent. The policy options will play out in a future that is not certain. Considering the most relevant combinations (scenarios) allows checking the robustness of the options and whether the choice of approach should be delayed until more information is available; it may need to change as the uncertainties are resolved or require complementary actions to hedge against risks.

The possibilities can be recapitulated as follows:

Table 5: Evaluation Scenario Dimensions

Macroeconomic outcomes	Favourable – mobility to positive opportunities; comparative advantage, productivity, eased public service burden.
	Negative – mobility from difficulties to advanced Member States; increased support demand, dwindling tax revenues, commercial margins, social and economic cohesion[113].
	Structural change – formation of regional 'blocs' that share economic and societal flows, but resist cross-bloc interaction.
OOP development at Member State and European level	Positive feedback - different implementations create common appreciation that justifies overcoming LOST barriers.
	Crowding out (negative feedback) - differentiated OOP creates LOST barriers among countries, services, administrations.

The logic behind the selection of these scenarios is as follows. In a favourable macroeconomic climate, either positive feedback leading to broad acceptance of cross-border OOP (scenario I) or crowding-out leading to OOP in some Member States but weaknesses at European level (scenario II) are possible.

Unfavourable macro conditions and austerity pressures may favour a common solution (scenario IIIa) or weakened cohesion (scenario IIIb). For present purposes,

the differences between IIIb and II are minor; we do not further analyse IIIb. Under structural change, positive feedback is unlikely; there will not be enough financial and political resources and generalised austerity postures will themselves undermine convergence.

Table 6: Candidate Scenarios

<table>
<tr><th>Macroeconomic\ MS/EU</th><th>Positive feedback</th><th>Crowding-out</th></tr>
<tr><td>Favourable</td><td>I. Growing together better services, shrinking State burden, user-centred core standardised services</td><td>II. Peaceful co-existence services improve, burdens fall, efficiency and uniformity incentives are too weak for convergence</td></tr>
<tr><td rowspan="2">Unfavourable</td><td colspan="2">Austerity Europe</td></tr>
<tr><td>IIIa. Lifeboat solidarity Economic pressures drive cross-border activity</td><td>Economic pressure is too steep, OOP a limited option in the most necessary areas</td></tr>
<tr><td>Structural change</td><td>Structural change conditions will undermine positive feedback</td><td>IV. Regional OOP Formation of virtual blocs, asymmetric cross-border activity, OOP provided only to the most significant flows, reinforcing separation</td></tr>
</table>

C. Timing and trajectories

1. The OOP-readiness of different countries

The affected stakeholders serve two functions as regards impacts:

- 'Units of account' for measuring (especially micro and meso level) impacts and ensuring that important impacts are not overlooked;
- 'Counterparties' or other actors whose actions will shape the impacts.

For instance, the impacts of Option 0 will depend on the extent to activities like those in the ISA[2] Programme are carried out and the time-frame and nature of the results. At the same time, existing regulations such as eIDAS have not been finalised; their eventual implementation will also affect the transition of OOP from practices to principle and associated costs and benefits.

The *status quo ante* entails the following.

- EU Regulations, Directives and initiatives can[114] facilitate OOP implementation.

- Member State laws and regulations provide elements of an OOP legal basis of varying applicability, OOP-friendliness[115], and sectoral and cross-border[116] focus.
- Databases roughly divided between Base Registries and others; interoperability and other characteristics of the former can be more broadly applied.
- Many Base Registry models; even registries of the same type (e.g. business) differ along almost every important dimension (Annex IX). Structured interconnection is almost inevitable compared to a common approach or central databases.
- 'Non-base' data are more disparate; short-term solutions based on mutual recognition and certification rather than data transfer may be more viable.
- Some Member States have not begun domestic OOP implementation; others have legal foundations and common procedures – most lie in between.
- Few Member States have implemented cross-border data re-use services, let alone legal, organisational, semantic and technological solutions 'open' to data requests from all other Member States; we found none with public services able to request and accept personal and business data directly from all other Member States, let alone to do so without first asking the individual or business involved.
- Where domestic data re-use is not applied as a principle, it is used in the specific contexts, such as Base Registries or particular 'life events' where the need is greatest. Motivations differ: cost and time reduction and simplification for administrations, individuals or businesses; better services; fraud prevention; or benefits for particular cases (e.g. SMEs, reporting deaths) may mean that:
    - Incompatible[117] practices frustrate common approaches;
    - The diffusion of further processing practices follows organisational or functional rather than technical pathways;
    - Practices may not be equally good in all contexts if evaluated using different criteria, or where confirming evidence (e.g. savings) is scant.

For these reasons, option assessment must take differing *OOP maturity*[118] into account. This is not a matter of TRLs or eGovernment maturity alone. As noted in II.B, options to implement OOP are linked to actions intended to give effect to other principles. Assessment of a specific option may need[119] to reflect variations in practice and in principle.

A final remark on maturity is that ongoing option costs should be similar in most countries, but adoption, transition and familiarisation costs may differ. The relationship between OOP-maturity and these one-off costs is likely to be 'U-shaped.'

2. Timing

Impacts will develop over time, allowing flexible and adaptive implementation. Table 7 Table 7 characterises the time frame for different measures and options that use them. 'M' indicates that the type of measure in the row will play a major role in the option indicated in the column, 'l' that the option plays a lesser role.

Table 7: Time Frame for Measures and Options

Measures	Time frame	Option			
		0	1	2	3
Regulation and law	1-3 years for REFIT reviews and Regulations[120]; up to 5 years for Directives	M	M		
Joint action and coordination	Working and coordination groups in place; a new statutory body can take 1-2 years; information and good practice exchange ongoing, but typically need up to 5 years to build a useful community	M	M	M	M
Standards and frameworks	Already being pursued; will continue to develop over the next 5-10 years.	M		M	l
Direct intervention	Short-run measures to extend existing OOP services, 6 months; medium term CAPs and ENOLL projects, 3-4 years; adaptation of procurement regulations, 5-6 years.	M	M		M
Research and innovation	Short-run impact through endorsement in work programmes; general R&I, 3-8 years; empirical studies of impact starting in 5 years (to allow data to accumulate).	M		M	M
Shared/interconnected Base Registries	Ongoing; implementation, 1-2 years.	M	M	l	l
Structures[121] for sharing non-basic data	Initial steps ongoing (revised EIF and ISA[2] actions); substantial progress to parallel BRIS, ECRIS concreteness, 6-10 years.	l		M	M
Dynamic implementation (monitoring and adjustment)	Guidance and recommendations ongoing; retrospective assessment and data analysis, 5 years for preliminary results; major adjustments, 8 years or more.	l	M	M	l

D. Preliminary assessment of impacts and option comparison

Limited national evidence[122] of the monetary value of time savings directly linked to volume suggests that per-capita savings for individuals will remain relatively small

(circa €10-15 per year) for domestic OOP; potentially even smaller for cross-border interactions due to fewer service demands and fewer contacts per case. The remainder of this section gives an overview of impacts and the intermediate outcomes that lead to them. Impact mechanisms are discussed for the Growing Together scenario together with changes per scenario and option. By prior agreement, this does not address any increase in cross-border service demand (which 'scale' OOP impacts) arising as a result of the development of OOP.

Table 8: intermediate impacts

In-country (domestic) OOP	Cross-border
Data/service scope	Data/service scope
Government level(s)	Geographic scope of OOP (bilateral/patchy, uniform/minimal, pan-European).
Domestic citizen burden reduction	Cross-border citizen burden reduction
Domestic business burden reduction	Cross-border business burden reduction
Government simplification, clear responsibility, cost savings	Government simplification, clear responsibility, cost savings

From an overall perspective, playing down scenario differences, the options can be ranked in terms of functional outcomes as shown in Table 9:

Table 9: Overview of Option Ranking by Stakeholder

Criterion	Best ↔			Worst
Extent and speed of convergence EU-wide OOP	Baseline	Responsive Assistance	Proactive encouragement	Legislative approach
Size of common core (cross-border OOP)	Baseline	Responsive Assistance	Legislative approach[123]	Proactive encouragement[124]
Business				
Overall	Legislative approach	Baseline = Proactive encouragement		Responsive Assistance
At home	Baseline = Legislative approach = Proactive encouragement			Responsive Assistance
Abroad	Legislative approach	Baseline = Proactive encouragement = Responsive Assistance		
Individual				
Overall	Legislative approach	Proactive encouragement	Baseline	Responsive Assistance
At home	Legislative approach	Proactive encouragement = Responsive Assistance		Baseline

Criterion	Best	↔	Worst
Abroad	Legislative approach	Baseline = Proactive encouragement	Responsive Assistance
Public administrations			
Data suppliers	Proactive encouragement = Responsive Assistance	Baseline	Legislative approach
Data requestors	Legislative approach = Proactive encouragement	Baseline	Responsive Assistance

Table 10 summarises impacts by option, scenario and affected party. This is discussed in Annex XIII.

Table 10: Summary of Main Impacts

IMPACT OF POLICY vs SCENARIO on Stakeholders		Baseline				Hard Law				Soft law				Responsive assistance			
		B	C	G1	G2	B	C	G1	G2	B	C	G1	G2	B	C	G1	G2
Growing together	Within MS																
	Across border																
	Pan-European																
Peaceful coexistence	Within MS																
	Across border																
	Pan-European																
Lifeboat solidarity	Within MS																
	Across border																
	Pan-European																
Regional OOP	Within MS																
	Across border																
	Pan-European																

High impact	
Moderate impact	
No impact	
Negative impact	

B	Business stakeholders
C	Citizens
G1	Information providing government
G2	information requesting government

From the table it is clear that option 2 "Proactive Encouragement" has overall the most favourable score, when taking into account the high "negative impact" score of option 1 "Legislative approach".

VII. Conclusions and recommendations

Considering the continued spread and development of networked technologies and digitisation in the world (wider context) and the current state of OOP within and between Member States and at Pan-European level (specific context), we are still in the early days of a rapidly evolving area. Evidence shows that continued progress can eventually deliver substantial benefits, but according to Member State representatives interviewed for this study, rapid EU-wide OOP implementation may be costly (e.g. if it duplicates Member State-level initiatives already in place or requires extensive adaptation of existing systems) and resisted by Member States (on the grounds of attachment to existing systems – both national OOP systems and information requirements for access to specific public services – and because filling OOP requests from other countries may impose non-reciprocal and unreimbursed costs on 'home jurisdictions'), unless done very well.

The study found that joint action on EU-wide OOP is necessary to sustain coherent development of the Digital Single Market and to counter possibly-important emergent negative impacts such as fragmentation and (possibly) discrimination in favour of or against individuals or businesses from specific countries. At the same time, full national OOP implementation requires considerable investment and reorganisation, which go beyond the mandate of the European Commission.

Below, we present our conclusions followed by recommendations and open questions.

A. Conclusions

The following findings have emerged from the situation assessment, option development and analysis of their likely impacts.

1. OOP is already happening

OOP is already being implemented at Member State and European level: although not in or between all locations and not for every service, and there is a wide variation in maturity across Europe. There are, however, OOP initiatives at all levels of government:

a) Within Member States, there are some well-developed general OOP rules and structures at regional and national levels, further specific examples and some elements of the required legal basis tied to particular information and services;
b) Between nations, there are examples of OOP services, information exchange processes and common platforms, typically associated with

particularly significant cross-border activities facilitating businesses and individuals from specifically associated nations more than businesses and individuals from other EU member states.

c) At a pan-European level, there are enabling legislative measures, concrete infrastructures and rules for sharing a growing range of information, especially for businesses and certain official data pertaining to citizens, with more in process or planned.

These measures and initiatives are only rarely dedicated to OOP and tend to be linked to other policy domains or principles such as eGovernment services, burden and cost reduction, intergovernmental data exchange and the 'whole government' and 'no wrong door' principles. Some business needs are particularly well served, including registration, public procurement, and tax affairs.

National OOP implementation can be both a barrier to[125] and an enabler of European OOP[126]. This relationship has direct implications for EU competence, subsidiarity and additionality. More generally, successful progress or disappointing experiences at national level may affect Member State willingness to cooperate in OOP implementations that are:

- Hierarchically interconnected vs. decentralised in structure;
- general vs. sector- and functionality-specific in data and services; and
- standardised vs. localised in legal, semantic and technical terms.

From this we identified two polar linkage possibilities between national and European OOP:

- Positive feedback: even different Member State OOP implementations create a common appreciation of benefits that justifies overcoming the resulting legal, organisational, semantic and technical barriers.
- Negative feedback: differentiated forms of OOP create interoperability barriers between countries and among services or public administrations.

2. Many initiatives and legislative measures underway are likely to simplify EU-wide OOP implementation in a changing landscape

Today, concrete *measures*[127] that facilitate OOP are wide-ranging and closely-interlinked. Most are not specific to OOP but derive from other domains (e.g. interoperability). Moreover, many are still evolving. Therefore, they should not be seen as dedicated and independent policy options. Specific regional, Member State and multilateral *initiatives* continue to develop; they can be influenced by EU-level action, but also form the environment for EU-wide OOP development.

Finally, many ongoing EU, Member State and multilateral *actions* make explicit reference to OOP as a motivating factor or objective, but they cannot be considered as OOP *strategies*.

At a practical level, many essential elements have already been developed to reconcile OOP with information sovereignty, taking into account data protection, security and cybersecurity and governments' citizen-facing and data controller responsibilities. These include reference architectures and the recognition that (remote) further processing requires shared data catalogues and semantics.

What is still missing is clarity on the best way to facilitate further processing of (esp. personal) data between authorities across borders. While it is possible to justify exchange of personal data for specific services to specific individuals (at their request or otherwise) on a case-by-case basis, the lack of a common and reliable legal base will retard progress towards effective and sustainable implementation of EU-wide OOP.

3. The impacts of OOP are hard to quantify, yet fundamental

There are significant evidence gaps on costs and benefits, especially beyond Member State level. What can be measured does not cover the most socially important impacts, is not directly attributable to OOP and is not quantitatively significant. Moreover, available measurements do not capture business or citizen impacts. This may be interpreted as a signal of priorities; in any case, care is needed to improve measurements without imposing disproportionate or distorting additional burdens.

As a principle, OOP depends on collective understanding and acceptance of data re-use. Impact measurement can profoundly affect these cultural factors, introducing an element of endogeneity (where measurement changes the impact).

Available data suggest modest direct tangible per-capita savings. Indirect and collective impacts may be higher, as will the impact on fundamental Government-stakeholder relations. This, in turn, will depend on OOP's consequences for trust, security and transition to suitable[128] 'user-centric' services.

One of the most important potential impacts is shifting from data re-use *practices* to the once-only *principle*. This cultural change is hard to measure. Our situation assessment links this to other cultural shifts; from document-focused to information-based government; from power to agency relationships between citizens and businesses and 'their' governments; and eliminating service and government access discrimination on the basis of national origin. In all of these, formal entitlement does not translate into effective equality; costs, delays, risks and

other burdens may leave cross-border applicants at a practical disadvantage. But OOP concerns the essence and not the form of burden reduction and equal treatment.

The situation is particularly complex for services to which domestic and cross-border participants cannot establish entitlement in the same way, e.g. when information used in one country may not be acceptable in another for legal, substantive or ethical reasons. It is also hard to implement 'mutual recognition' based on service equivalence when service architectures (e.g. the bundling together of multiple services or information requirements) differ across borders.

These fundamental asymmetries are compounded by the existence of public services that are not available to domestic and cross-border claimants on the same basis. Sometimes, practical difficulties can be obviated by 'passporting'[129], but the services for which symmetry cannot be assumed show little sign of shrinking[130]. These changes in the scope and effect of Single Market levelling (broadly interpreted) will continue to create difficulties for OOP.

In conclusion: moving towards an EU-wide implementation are expected to lead to many advantages, directon-wise, that are hard to quantify in specific terms today but that are of fundamental nature. Today, it is equally hard to specify costs in specific terms, yet many developments are identified to be underway that are likely to further reduce costs for implementations over time, and that will leverage the advantages.

B. Recommendations

Taking into account current levels of OOP maturity in and across Member States, feedback from Member States during the 2 June Dutch Presidency event workshop on the Once-Only Principle, interviews with Member State officials, and scenario analysis, we recommend:

1. A "Directive to support exchange of data for the purposes of the Once-Only Principle."

This would establish a consistent and reliable legal basis for the exchange and use of data (including personal data) pertaining to and for the benefit of individuals (natural persons) and businesses as an alternative to resubmission of the same or equivalent data by those individuals and businesses.; and

2. *A strategy of "proactive encouragement of and administrative support for OOP" (Option 2 above).*

Policy considerations may lead to "stepping up" to an overtly legislative approach (Option 1) or "stepping back" with a Responsive Assistance approach (Option 3). The legislative approach is more costly as much upfront work is required; it is also less flexible and less encouraging of innovation. The "Responsive Assistance" approach is unlikely to lead to effective OOP implementation across the European Union in the foreseeable future; costs will be low (along with political priority) but the risk of long-term fragmentation remains high and direct individual and business benefits will be minimal.

This approach will preserve advantageous localisation and specialisation, align progress and improve interoperability across Member States and at EU level while respecting subsidiarity and fundamental rights (especially data protection). The concrete actions involved should be 'business case driven[131]' and 'user centric[132]', adopting a Base Registry approach wherever possible A full move towards using data rather than documents for public administration purposes would further facilitate cost-effective and equitable service provision.

In practical terms, we recommend:

- *A consistent legal base at EU level for further data processing in support of the Once-Only Principle* that would allow competent officials to exchange and use data (including personal data) pertaining to specific natural persons and businesses as an alternative to resubmission of the same or equivalent data by those individuals and businesses while protecting the rights of data subjects, including those enumerated under the GDPR. as well as We recommend the use of a Directive to support exchange of data for the purposes of the Once-Only Principle to ensure full consistency with Member State legislation, especially as regards non-personal data, but also in recognition of the scope for Member State variation that exists within the GDPR[133]. This approach will therefore also entail changes to Member State legislation, as the competence for arranging service eligibility and delivery procedures remains largely at Member State level.
- *A Task Force with Member State representatives* to establish a sound and comprehensive framework for OOP initiatives and their interconnection at European level. It should also provide a continuing capability for collecting and exchanging evidence, analysing impacts and resolving issues arising as OOP and the digitisation of government interactions spread. The Task Force could also advise on the extent to which necessary legislative changes should be pursued at EU or Member State level level. Initial Terms of Reference for the Task Force are presented in Annex XI; and
- *A Structured Interconnection of Base Registries approach* to establish an EU-wide framework for business OOP to interconnect base registers and

consolidate steps towards portable or mutually-recognised business identities, common ontologies and streamlined procedures, based on requirements of the eIDAS Regulation and standards of the (revised) EIF. The policy measures presented in more detail below are intended to minimise business burdens, deliver (more modest) burden reduction for individuals, control and balance costs for public administrations and ensure learning by doing while moving forward together.

3. A base registry network to facilitate sharing of data for OOP purposes

While the Directive (Recommendation 1) provides a legal basis that enables public authority data controllers and data processors to make and respond to requests for data re-use and to use such data on (at least) an equivalent basis to directly submitted information, it does not by itself ensure that such data are easily available in the form needed to make this re-use practicable.

A particularly valuable aspect would be creation of a European Catalogue of Base Registers to map: the locations, contents, formats, qualities and applicability of fundamental data about businesses and citizens; means of gaining access (publication of APIs, identity and competence of authorities able to seek access, service-level agreements, etc. This catalogue, in turn, can be most easily and effectively assembled if master data policies are implemented at national and EU level. These policies would also provide other benefits in terms of cost efficiency and data rationalisation.

To minimise the complexities of OOP implementation, it will be important to build on progress already in place and ensure coherence with ISA2 Programme, eIDAS Regulation and the (revised) EIF, and it seems most useful to base the provision of OOP around a system of Base Registries. This is the approach used in some of the most advanced countries, with minor variations.

This approach is further explained in Annex X

Other steps include provision of enhanced conditions intended to increase the acceptability of OOP procedures:

- Where necessary, revise any (existing) Directives and Regulations at EU level that currently limit cross-border data re-use;
- Protect the ability of businesses and individuals to opt-out of further data processing[134]; and
- Where possible, revise national legislation that prohibits the sharing of specific information with other administrations within or across borders in such a way as to support OOP sharing.

Beyond this, it will be important to create a 'landing place' network of Base Registries and other authoritative sources of reusable data (see for more details: Annex IX). There is a clear need for EU leadership – as an alternative to top-down control or a laissez-faire approach – in order to drive progress while respecting national differences and at the same time to balance OOP with other principles (e.g. Whole Government) and policy initiatives (e.g. e-Government).

C. Next steps

For implementation of the above recommendations, to get the best from national and European OOP-related initiatives and optimise long term development, a Task Force should be set up that embraces the principles above and takes responsibility for aligning national and European level activities. It should be formed from relevant national authorities and agencies and consult 'lay representatives' from business and civil society to sustain 'ownership' by Member States and those affected by their activities.

The terms of reference of such a body should call on members to:

- Share experience and learn from practice;
- Coordinate future initiatives:
    - establishment of priorities and a road map for Member State and cross-border OOP implementation;
    - Identify legally reliable objectives for further and wider OOP implementation, which might include:
        - Reducing (cost, time and complexity) burdens on citizens and businesses;
        - Improving the cost-effectiveness of government services;
        - Fraud prevention;
        - Effective government; and
        - Efficient and equitable Single Market functioning (including jobs and growth).
    - Identify and agree a minimal sufficient set of platforms and organisation for interoperability;
    - define and implement a measurement or observatory exercise – in conjunction with Better Regulation – to track the costs, benefits and other impacts of OOP strategy
- Serve as a deliberative body to clarify issues arising.

As a starting point for the work of the task force, we offer the following three tasks.

First task: Set out principles for OOP implementation

It is important to clarify principles at the start, to ensure alignment and credibility. Based on our study findings we suggest embracing the following key principles:

a) Embrace incremental accretion and prioritise business applications

The consensus view of government stakeholders is it may be best to work towards OOP in an incremental fashion, building on current experience and using explicit business case and business case development. This applies to both citizen- and business-facing OOP implementations, but the near-term priority lies with business applications, due to the existence of substantial common (hard and soft) infrastructure, the tangibility of benefits, the greater quantitative significance and lower service diversity of cross-border business-government interactions and the relatively lower hurdles in terms of privacy regulations. The path forward should aim at developing a framework that facilitates effective *cumulative* progress by providing suitable platforms and interoperability at all levels.

b) Ensure user-centrism as the norm

As noted above, building and sustaining momentum requires a shift from administrative to user-centred government and from a reliance on documentation to the information currently (and optionally) contained in those documents. User-centrism extends beyond the specification and delivery of services to include the design of 'user interfaces' that allow a business or individual to employ any single point of contact (the 'No wrong door' principle) to submit information needed for many functions (the 'Whole government' principle).

c) Move to information instead of document processing for administrative services

Most administrations have been moving towards data storing and sharing within their administrations, yet still today there is some legislation or administration rules that require documents rather than the information they contain. This is a major barrier that is mostly a remainder from old times than a necessity.

In addition to the three key principles above the following principles could be considered:

1- Relevant to businesses *and* individuals:

   a. All reusable data should have a data catalogue covering their contents, provenance, legal reliability, quality, validity and attached consents;

b. Administrations providing European Public Services should only ask for information that was not previously submitted, has expired or lacks appropriate consents.

c. Where possible, data should be taken from unique authentic authoritative sources.

d. [Whole government principle] Especially where providing information may be burdensome (e.g. reporting deaths), government should proactively provide 'one-stop-shop' services to ensure that all relevant services and offices are informed and have taken appropriate action after they are first notified.

2- Only to individuals:

e. Must have the right to refuse to give information available from public administration sources, and to exercise all applicable data protection rights (e.g. access and correction) with respect to personal data obtained from government sources.

f. To reinforce data protection rights, further processing (including query-based interrogation of databases and certification) should be recorded and used to ensure that data requestors are made aware of any significant changes.

Second task for the Task Force: Develop a Roadmap for Intervention

This can be approached from the perspective of specific elements of OOP implementation. An approach starting from pre-defined data elements is explicitly foreseen in the eGovernment Action Plan. In step 1 such elements would be collected and shared following the EIF. Step 2 would extend this to all data (again within EIF guidelines). Step 3 would use these data to populate forms or as a direct input into automated processes.

Depending on circumstances, the shared and automated aspect could use a 'light touch' process, supplemented by more detailed data as necessary, along the lines implemented in the Virtual Company Dossier and other 'pre-qualification' evidence, ideally in line with shifting from documents to data and negotiating the 'least common denominator' aspects of such forms.

More generally, implementation should be kept as non-specific and open as possible, to allow room for innovation and experimentation and to avoid ruling anything out or precluding alternatives that might be acceptable and beneficial or yield additional relevant data. Variants already available include pre-populated forms vs. forms where already available or unnecessary elements were greyed out.

We note that if OOP implementation takes the form of populated information forms presented to service beneficiaries for checking, approval and/or correction, the benefits can be enhanced by requiring that any corrections should automatically be used to update 'back-office' (e.g. base register) information. A minor issue is whether the level of assurance needed to provide the service is the same as that needed to correct or change the authentic record. Of course, such checking is itself burdensome; the proportionality of this would need to be assessed on a case-by-case basis, along with the implications of evidence that checking information in pre-populated forms can lead to more errors than filling in blank forms due to 'attention deficit.'.

Third task: develop suitable standards.

A typical part of the specification of interconnected data systems is the requirement for all participants to provide explicit 'data fiche' descriptions of formats, etc. Along with this, such systems may require 'translation' services as an alternative to a single common standard (especially in relation to the recommended Option 2). A single standard would require extensive modification of many countries' data and service delivery systems for the benefit of a small fraction (now and in the foreseeable future) of those using the services (i.e. cross-border users). This may not only be disproportionately costly to administrations, but would impose extensive familiarisation and data management costs on firms who might need to submit information. In addition, there is no obvious way to decide 'which is best' for all purposes. Therefore, a third task for the Task Force would be the determination of what level and type of standardisation is appropriate for different contexts.

D. Open questions

Europe is currently experiencing many political, economic and societal changes. Rapidly developing technologies deeply affect the ways society creates, collects, uses and shares digital data and digitised information. These challenges pose several questions. The answers cannot yet be given, in part due to lack of experience and evidence and in part because they depend on policy discussions that have yet to conclude. They are likely to become more relevant in coming years, so preparing to address them is a useful foresight exercise.

- Should citizens and companies be wholly responsible for the quality and correctness of their information within the governmental data sources, or should government take the initiative (e.g. through periodic verification)?
- Under what conditions would it be acceptable and useful for governments to set up a 'super-database' containing all 'OOP-suitable' information on citizens and enterprises within one data source at Member State or even EU level?

- Once-Only is viewed as a useful step towards recognition of a 5th freedom; free movement of data in EU – should such a freedom be articulated in law?
- Is there any basis for working towards an equivalence of once-only capabilities between public authorities and private businesses?
- Is there an inherent conflict between OOP and personal data protection or personal privacy?
- Should access to (and charges for) different types of business-related data (both registry contents and additional data) be harmonised?

Annex I. Glossary[135]

TERM	Meaning
Administrative Burden	Costs borne by individuals and businesses in order to comply with information obligations resulting from Government regulation or associated with obtaining specific services or exploiting a functionality. Indirectly, this includes the costs to public administrations of dealing with multiple procedures, data and information concerning the same subject, ultimately paid by individuals and businesses.
Authoritative Source	An authoritative source is information that is stored only once and which is believed to be correct, so can serve as a basis for further processing.
Base registry or register (used interchangeably)	A Base Registry is identified as being a trusted and authoritative source of information which can and should be digitally reused by others and in which one organisation is responsible and accountable for the collection, usage, updating and preservation of information. Base registries are reliable sources of basic information on items such as persons, companies, vehicles, licences, buildings, locations and roads. This type of information constitutes the master data for public administration and European Public Service delivery. "Authoritative" in this context means that a Base Registry is considered to be the source of information i.e. which represents the correct status, which is up-to-date and which is of highest possible quality.
Base registry Framework	A Base Registry framework "describes the agreements and infrastructure for operating Base Registries and the relationships with other entities".
Basic Public Services	Basic public services are a type of service that can be reused for creating integrated public services (e.g. issuing a birth certificate).
Business Process	A business process is a sequence of linked activities that creates value by turning inputs into a more valuable output. This can be performed by human participants or ICT systems, or both.

TERM	Meaning
Collaborative Platform	A set of specific services and facilities for the use of a specific community and their interactions, the goal being to facilitate cooperation to achieve shared objectives. Typically, the services are communication-related, and incorporate a repository for exchanged objects, information, materials, etc. A notable example is the Joinup Platform[136].
Consent (of natural person data subjects to personal data processing)[137]	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Core vocabularies[13]	Simplified, re-usable and extensible data models that capture the fundamental characteristics of a data entity in a context-neutral fashion.
Cross-border processing[138]	We state the GDPR definition in order to illustrate its difference from the general meaning of further processing in conjunction with OOP at European level (which typically involves multiple data controllers and data subjects in more than one Member State: (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

[13] A set of commonly agreed Core Vocabularies supported by the EU Member States have been created to provide a concrete starting point for promoting semantic interoperability among European public administrations; see: https://joinup.ec.europa.eu/asset/core_vocabularies/description.

TERM	Meaning
Data controller	From Art. 4(1) of the GDPR: The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. The European Data Protection Supervisor defines it[139] as: The institution or body that (either alone or jointly or in common with other persons) determines the purposes and means of the processing of personal data. In particular, the controller has the duties of ensuring the quality of data and, in the case of the EU institutions and bodies, of notifying the processing operation to the data protection officer (DPO). In addition, the data controller is also responsible for the security measures protecting the data. The controller is also the entity that receives requests from data referents to exercise their rights.
Data Ownership	Under EU law, personal data may not be owned. For other types of data, the following definition[140] may be useful: “The act of having legal rights and complete control over a single piece or set of data elements. It defines and provides information about the rightful owner of data assets and the acquisition, use and distribution policy implemented by the data owner. Data ownership is primarily a data governance process that details an organisation's legal ownership of enterprise-wide data. A specific organisation or the data owner has the ability to create, edit, modify, share and restrict access to the data. Data ownership also defines the data owner’s ability to assign, share or surrender all of these privileges to a third party. This concept is generally implemented in medium to large enterprises with huge repositories of centralised or distributed data elements. The data owner claims the possession and copyrights to such data to ensure their control and ability to take legal action if their ownership is illegitimately breached by an internal or external entity.”

TERM	Meaning
Data model	A data model is a collection of entities, their properties and the relationships among them, which aims at formally representing a domain, a concept or a real-world thing. It includes core vocabularies.
Database ownership	In this document, the term 'owner' shall be used to indicate the entity that controls, governs and/or is liable for the operation of a database. This is a complex area, partially clarified by the Database Directive[141], which distinguishes the rights of database 'makers' and 'users.' For present purposes, however, the intuitive definition suffices.
(Data) processing[142]	Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. In particular, includes: a) organisation, adaptation or alteration of the information or data, b) retrieval, consultation or use of the information or data, c) disclosure of the information or data by transmission, dissemination or otherwise making available, or d) alignment, combination, blocking, erasure or destruction of the information or data.
Data processor[143]	A natural or legal person, public authority, agency or any other body which processes personal data on behalf of (and subject to instruction by) the controller. The processor only acts on behalf of (and subject to instruction by) the data controller.
Data representation	The manner in which data are expressed symbolically by binary digits in a computer.
Data requestor[144]	A public administration data controller that uses data about a data referent to complete an administrative procedure, deliver a service or make a decision. In this document, this refers to the data controller who obtains information under the OOP.
Data subject[145]	The (natural) person whose personal data are collected, held or processed.

TERM	Meaning
Data referent[146]	The natural person or business to whom the data pertains; in this context also the person, citizen or business requesting the service for which data are used.
Data supplier	A public administration or authorised data controller or data processor who holds data about data referents on behalf of a public administration and who makes these data available to data requestors.
Digital Once-Only Principle	applying technical and procedural solutions **based on information and communication technologies** and data to be digitally available, in order to eliminate or at least reduce the extent to which individuals and businesses are required to provide the same information more than once to public administrations, while respecting national and European data privacy and other relevant regulations
Digital Single Market (DSM)	DSM is one in which the free movement of goods, persons, services and capital is ensured and where the individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence[147]
Document	Recorded information or object that can be treated as a unit[148].
eGovernment	eGovernment is about using the tools and systems made possible by information and communication technologies (ICTs) to provide better public services to individuals and businesses.
eID[149]	Electronic identification is one of the tools to ensure secure access to online services and to carry out electronic transactions in a safer way.
eIDAS Regulation[150]	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

TERM	Meaning
Electronic Certification	Electronic certification is the application of an electronic signature, by a specifically authorised person or entity, in a specific context for a specific purpose. It is mostly used to indicate that a certain validation process has been executed and that a given result is being attested by the signer. In the simplest case, it can merely represent the assertion of a given fact by an authorised person.
Electronic Records	As defined by the second version[151] of the Model Requirements for the Management of Electronic Records (MoReq2): a record is "Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business".
Electronic Signature	According to Directive 1999/93/EC, 'electronic signature' means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.
Europe. Interoperability cartography (EICart)	The European Interoperability cartography (EICart) is based on EIRA; it documents European interoperability services and tools and intends to facilitate reuse.
European Interoperability Framework (EIF)	The EIF provides guidance for the provision of European Public Services and a common set of core concepts for the design and update of national interoperability frameworks (NIFs), policies, strategies, guidelines and action plans that promote interoperability.
European Interoperability Reference Architecture (EIRA)	The European Interoperability Reference Architecture (EIRA) is a reference architecture for designing and describing digital public services across borders and sectors. The EIRA is aligned with the European Interoperability Framework (EIF) and complies with the context given in the European Interoperability Strategy (EIS). A common EIRA facilitates interoperability between public administrations and the reuse of solutions when developing European Public Services at the various levels of the administration.

TERM	Meaning
European Interoperability Strategy (EIS)	The European Interoperability Strategy (EIS) is a systematic approach to govern interoperability at EU level, with specific goals set. To this end, the European Interoperability Strategy (EIS) provides a basis for an organisational, financial and operational framework to support cross-border and/or cross-sectoral interoperability. The EIS steers the EIF and all other associated efforts by setting strategic priorities and objectives.
European Public Service	A European Public Service comprises any service supplied by public administrations in the Europe Union, or by other organisations on their behalf, to businesses, individuals or others public administrations.
Formalised Specifications	Formalised specifications are either standards pursuant to Regulation 1025/2012 on European Standardisation or specifications established by ICT industry fora or consortia.
Functionalities	Within this study, a functionality consists of a coherent set of activities or procedures involving provision of data and other information to one public administration office (national, regional or local) by an individual or business in order to obtain or enable a specific public service. For example, "registration as unemployed" is a functionality provided by the local or national office that provides unemployment support. One service may encompass one or more functionalities: this study focusses on 15 selected functionalities (5 concerning individuals' life-events and 10 concerning businesses).
GDPR[152]	The General Data Protection Regulation (Regulation (EU) 2016/679) is a Regulation intended to strengthen and unify personal data protection for individuals within the European Union (EU). It also addresses transfers of personal data outside the EU. The GDPR will be directly applicable on 25 May 2018 and will repeal and replace the data protection Directive 95/46/EC.
Information	Information is semantically enriched data, i.e. collections of data that have been given relevance and purpose.
Information and Communication Technology (ICT)	Technology, e.g. electronic computers, computer software and communications technology, used to convert, store, protect, process, transmit and retrieve information.

TERM	Meaning
Interface	An interface is a conceptual or physical boundary where two (or more) independent legal systems, organisations, processes, communicators, IT systems, or any variation/combination thereof interact.
Interoperability	"Interoperability" means the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems.
Interoperability Agreements	Written interoperability agreements are concrete and binding documents which set out the precise obligations of two parties cooperating across an 'interface to achieve interoperability.
Interoperability Framework	An interoperability framework is a commonly agreed approach to interoperability for organisations that wish to work together towards joint delivery of public services and/or exchange of information. It specifies a set of common elements such as a common vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices.
Interoperability Governance	Interoperability governance defines interoperability frameworks, institutional arrangements, organisational structures, roles and responsibilities, policies, agreements and other aspects necessary for ensuring and monitoring interoperability at EU and national level.
Interoperability Layers	The interoperability layers include: • four layers of interoperability — legal, organisational, information and technical; • a cross-cutting component called "Public service governance"; and • "Interoperability governance[153]".

TERM	Meaning
Interoperability Solution	Interoperability solutions include common frameworks, common services and generic tools facilitating cooperation between disparate and diverse organisations, either autonomously funded and developed by the ISA/ISA' Programme or developed in cooperation with other European Union initiatives, based on identified requirements of European public administrations[154]: • A framework (strategies, specifications, methodologies, guidelines and similar approaches and documents); • A service (operational consequences and infrastructures of a generic nature which meet common user requirements across policy areas); • A generic tool (reference platforms, shared and collaborative platforms, common components and similar building blocks which meet common user requirements across policy areas).
ISA^2	The ISA² programme supports the development of digital solutions that enable public administrations, businesses and individuals in Europe to benefit from interoperable cross-border and cross-sector public services. It runs to the end of 2020.
Loose coupling	Loose coupling refers to communications between systems that operate more or less independently of one another (asynchronously) and whose internal states are not strongly interdependent. The coupling takes the form of messages passed between the systems in question, typically implemented using some type of middleware layer or queuing system, so that the target system deals with requests as and when it can. Thus, the target system may not even be available at the time of the request, which is simply queued for later action.
Master data	The description of the core data assets and their relationships that are necessary for providing European Union Public Service provisioning.
Master Data Management	The governance and a capability aimed at ensuring the uniformity, quality, stewardship, semantic consistency for the accountability of master data.

TERM	Meaning
Memorandum of Understanding	A bilateral or multilateral written agreement between two organisations which sets out a number of areas and means by which they will cooperate, collaborate or otherwise assist one another. The exact nature of these activities depends on the nature of the two organisations, the domain of activity in question, and the scope of the cooperation envisaged.
Multichannel Delivery	A channel is a means used by an administration to interact with and deliver services to its users, and for users to contact public administrations with the aim of acquiring public services. The term 'user' includes individuals, businesses and organisations as consumers of public services. The set of different possible 'means' for electronic delivery constantly changes, and currently includes the use of web-based technologies, telephony, paper media, face-to-face contacts and many others, applications of these technologies such as the internet, e-mail, SMS, call centres or service counters, and devices to access these applications such as personal computers, mobile phones, kiosks or digital TV. Multichannel delivery refers to the provision of public services simultaneously and independently via two or more such channels, selectable by the user according to needs.
National Interoperability Framework (NIF)	**NIFs** are a set of frameworks, policies, strategies, guidelines and action plans defined by individual Member States to promote interoperability and to govern national IT systems and infrastructure within their own countries.

TERM	Meaning
Once-only principle	Individuals and businesses should have the right to supply information only once to a public administration. Public administration offices should be able to take action to internally share these data, in compliance with the data protection rules, so that no additional burden falls on individuals and businesses. Anticipated benefits: government should be • Smart (can answer questions asked of it) • Light burden (does not make duplicate requests for information) • Fool-proof (fraud reduction by use of consistent authoritative information) • Evidence-based decisions (uses full, complete and consistent information) • Trustworthy (reliable decisions) May be modified as to form (digital) and scope (cross-border).
One-stop shop	One-stop shop means a single channel (office or a webpage) that offers multiple services to individuals or businesses from this "one stop" in one place. This scenario is popular among municipalities in many countries, for example for a range of functions or departments in a single location.
Open Source or Open Source Software (OSS)	Defined by 10 criteria at the Open Source Initiative web site[155]. Term sometimes used to refer to Free Software[156]
Personal Data[157]	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Point of Single Contact	Single institutional interlocutor for a given service provider through which the latter can collect all relevant information and easily complete at a distance and by electronic means all procedures and formalities to access a service activity and to the exercise thereof[158].

TERM	Meaning
Principle	Principles are intended to establish behaviours and help to direct actions.
Profiling (of personal data) [159]	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Protocol	A set of conventions that govern the interaction of processes, devices and other components within and across systems.
Reusability	The degree to which IT solutions, information and data are used in contexts other than its original, intended or main purpose.
Reference data	Reference data are small, discrete sets of values that are not updated as part of business transactions, but are usually used to impose consistent classification. Reference data normally have low update frequencies. Reference data are relevant across multiple business systems belonging to different organisations and sectors.
Secure Data Exchange	This is a component of the conceptual model for European Public Services. Its aim is to ensure that all cross-border data processing[160] are done in a secure and controlled way.
Service Level Agreement	A formalised agreement between two cooperating entities; typically, a service provider and a user. The agreement is expressed in the form of a written, negotiated contract. Typically, such agreements define specific metrics (Key Performance Indicators — KPIs) for measuring the performance of the service provider (which in total define the 'service level'), and document binding commitments defined as the attainment of specific targets for certain KPIs, plus associated actions such as corrective measures. SLAs can also cover commitments by the user, for example to meet certain notification deadlines, provide facilities or other resources needed by the service provider in the course of service provision, problem solving, or to process inputs given by the service provider to the user.

TERM	Meaning
Service Orientation	Service orientation means creating and using business processes packaged as services.
Service Oriented Architecture (SOA)	Service oriented architecture is a paradigm for organising and utilising distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations (from OASIS Reference Model for SOA[161]).
Standard	As defined in European legislation (Article 2 of Regulation 1025/2012 on European Standardisation), a standard is a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory, and which is one of the following: • 'International standard' means a standard adopted by an international standardisation body, • 'European standard' means a standard adopted by a European standardisation organisation, • 'Harmonised standard' means a European standard adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation, • 'National standard' means a standard adopted by a national standardisation body.
Standards developing organisation	A chartered organisation tasked with producing standards and specifications, according to specific, strictly defined requirements, procedures and rules. Standards developing organisations include: • recognised standardisation bodies such as international standardisation committees such as the International Organisation for Standardisation (ISO), the three European Standard Organisations: the European Committee for Standardisation (CEN), the European Committee for Electro technical Standardisation (CENELEC) or the European Telecommunications Standards Institute (ETSI); • fora and consortia initiatives for standardisation such as the Organisation for the Advancement of Structured Information Standards (OASIS), the World Wide Web Consortium (W3C) or the Internet Engineering Task Force (IETF).

TERM	Meaning
Taxonomy	A taxonomy represents a classification of the standardised terminology for all terms used within a knowledge domain. In a taxonomy, all elements are grouped and categorised in a strict hierarchical way, and are usually represented by a tree structure. In a taxonomy, the individual elements are required to reside in the same semantic scope, so all elements are semantically related with one another to one degree or another.
Vocabulary	A vocabulary is a set of terms (words or phrases) that describe information in a particular domain.
Whole-government principle[162]	The principle that persons and businesses interacting with a government entity are interacting with the whole of the national government. This principle is complementary to the OOP, but differs in that it is not limited to – and does not directly imply - data re-use. It includes • The one-stop-shop principle – that individuals or businesses should not need to know how public administrations work or how competencies are allocated across state agencies but should instead be able to deal with a "single-window" representing public administration as a whole[163]. At EU level, these are called Points of Single Contact[164] (PSCs); • The "no wrong door" principle that there should be multiple channels for access to public services.

Annex II. Methodology

The analysis behind this report was conducted in phases. The first phase reviewed the literature (peer-reviewed and grey) relating to information sharing and the Once-Only principle in the European context. The second phase, discussed in in methodological terms in Section A below and in substantive terms in Annex III-Annex VI, reviewed the state of play in cross-border OOP implementation

- at Member State level from the perspective of a selected set of 'use cases' (four for businesses[165] and two for citizens[166]) involving 10 functionalities for businesses and 5 functionalities for citizens, based on interviews and desk research covering relevant pairs of countries (Annex III);
- A discussion of the public administration perspective based on interviews with selected national representatives (Annex IV.A);
- An analysis of business and individual attitudes towards data sharing and the once-only principle based on desk research and fifteen online surveys (one per each functionality) (Annex IV).

The third phase developed objectives and policy options, compared their potential impacts and developed recommendations. Specifically it provided:

- Indicative general and specific objectives (Section IV);
- A description of candidate individual measures (Section V.A. and Annex X.) and four high-level policy options (Section V.B);
- A preliminary or inception-level impact assessment, comprising a description of affected stakeholders (VI.A, Table 2), types of impact (VI.A, Table 3), 'landing place' scenarios in which to evaluate impacts (Section VI.B) and implementation dynamics (Section VI.C);
- A comparison of the impacts by scenario and option (Section VI.D); and
- Conclusions and recommendations for specific actors (Section VII).

Annex III. Use Case Analysis of Functionalities

Within the study *"EU-wide digital Once-Only Principle for citizens and businesses: Policy options and their impacts"*, two main dimensions are investigated in the actual and concrete implementation of OOP in Europe: by functionality and by Member State.

A. Introduction and specific methodology

The methodological approach (summarised in the box below) indicates the adopted criteria. The **10 functionalities for businesses and 5 functionalities for individuals** are investigated in **10 Member States**.

The methodological approach used to select functionalities and Member States

To have a better and concrete assessment of the actual implementation of OOP at national level and its potential EU-wide application, **a set of functionalities (15)** allowing individuals and businesses to get services from public administration has been selected. In order to better exploit existing studies in the domain and to be coherent with the EC approach, categories of services defined in eGovernment Benchmark Framework 2012-2015 were taken as the starting point for the selection of the functionalities.

Functionalities (and definitions) were selected from the eGovernment Benchmark Framework 2012-2015 Method Paper Update, 2015, with the additional aim to facilitate comparison between findings of this study and those of the eGovernment Benchmark Framework analysis[167]. The eGovernment Benchmark identifies 33 functionalities for business and 34 for individuals (organised in two categories: Job and Study). Elements considered for the purpose were[168]:

- SECTOR (if the service is provided by the private sector or public sector),
- GEO (if the service is delivered at national, regional or local level),
- A2 (if the service is available online).

In addition to this three elements, the following selection criteria used to prioritise functionalities to be selected:

- **Functionalities typically provided by public authorities** (to focus on essential information, Private sector operators, for instance insurance companies, may require more information than that mandatory by law);
- **Functionalities typically provided at national level** (to reduce the

complexity of comparing an indefinite number of procedures at different hierarchical levels among Member States; where the same functionality is provided at local level, the region in which the national capital is located was taken as representative of the typical national approach, e.g. "*Enrolling in higher education*");

- Functionalities for which the procedure is typically available online (to consider also the digital aspect of OOP); and
- Functionalities with more than "a predominantly informative purpose".

Result of this selection were **10 functionalities for businesses and 5 functionalities for individuals** related to **online available services** typically provided at the same (national) level of public administrations.

According to the study's Terms of Reference, desk research and interviews had to shed light on the different implementation perspective of an EU-wide OOP in 10 Member States, taking into account the legal, organisational, semantic, technical aspects. The selection of Member States was based on:

- geographical balance in EU28;
- contacts of the consortium (including the countries of origin); and
- at least 1 country in each category of the eGovernment Maturity[169] level, i.e. "Neophytes"; "High potentials"; "Progressive"; "Builders" "Mature" (Figure 3).

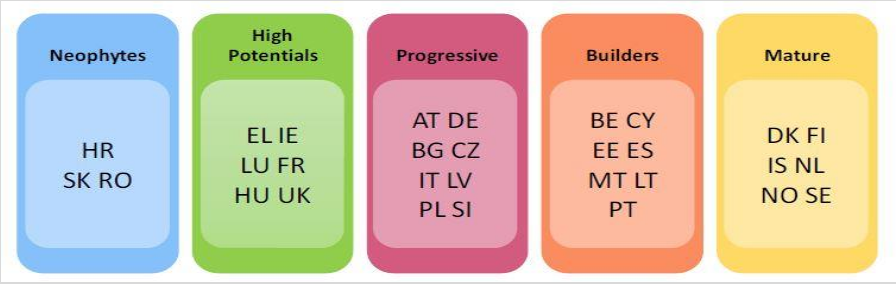


Figure 3: Clusters of countries with similar eGovernment Maturity (according to the eGovernment Benchmark Background Report).

Application of the above mentioned criteria together with a consultation with DG CONNECT representatives led to a **list of 10 Member States**.

The selected functionalities are listed in the following tables[170].

Table 11: Functionalities for businesses

	DEFINITION
BUSINESSES	
1. Register company name	This service ensures that persons forming a company obtain formal approval for the company's name.
2. Register domicile of business	Registering the company's address.
3. Register (a company or a branch of a company) in a business register[171]	Entry (of a company or a branch of a company) into business register as a 'legal person'.
4. Receive formal validation of signatures of representatives of the business	Some Member States require that a person's signature must be checked by government department before they can act as representative of a business.
5. Register with Social Security Office	Businesses must generally register with a country's Social Security office before hiring employees.
6. Register with compulsory healthcare	Registration to comply with any compulsory employee healthcare provisions.
7. Be compliant with social security obligations	Withholding of social insurance contributions from employee's wages and providing employers' contributions.
8. Be compliant with obligations related to work place security	Most Member States require businesses to have documented Health & Safety plans when hiring employees
9. Be compliant with tax related	Withholding of income (and possibly other) taxes from the employee's wages and paying

obligations	them to the government.
10. Register employee before first work day	Some Member States require employers to declare employees before the first day of working, normally at a tax office (to prevent fraud and illegal work).

Table 12: Functionalities for individuals

	DEFINITION
INDIVIDUALS	
1. Enrolling in higher education	Standard enrolment procedures for university or another higher education institutions i subsidised by an official administrative body in the country, including the provision of personal documents and/or eventual qualifications
2. Applying for student grants	Standard procedure to obtain student grants for higher education.
3. Obtaining financial aid for starting up as self-employed	Gaining access to financial and other assistance when becoming self-employed.
4. Registering for unemployment benefits	In order to obtain unemployment benefits and/or obtain help in finding a job, individuals must register at an administrative unemployment office.
5. Ensuring continuity of pension payments	Registration and payments to continue public pension payments during periods of self-employment or unemployment.

Member States identified as targets of this investigation are Belgium, Germany, Hungary, Estonia, Finland, Italy, Romania, Spain, The Netherlands, and The United Kingdom.

Desk research on the 15 functionalities and their implementation for the 10 selected Member States indicates that:

- Typically, procedures associated with services available to both domestic and cross-border users that are available online to domestic users can also be accessed by cross-border users;
- Authentication procedures for the selected 15 functionalities are still heterogeneous - some allow eID and other standardised personal identification means, but others require *ad-hoc* authentication for each step or specific of the authority/body providing information/data/documents;
- In many cases, documents needed to complete certain procedures can be submitted online without the need for further off-line steps (e.g. in-presence submission of documents, in-presence legal certifications, in-presence signature of documents or certificates), indicating a trend towards procedural simplification and reduction[172] of time-waste associated with in-presence execution of procedures;
- Prefilled forms, which can be used as a proxy for procedures for re-use of information and data already provided to public administrations, are available only in few of the sampled functionalities (e.g. tax related obligations); and
- In the vast majority of the cases, websites on which procedures concerning a functionality are available also provide specific information or indications to support cross-border users; nevertheless, in a number of cases it has been noted that forms for data/information collection are only in the national language(s).

These indications from the analysis of data of the eGovernment Benchmark Framework 2012-2015 give a perception of the administrative obstacles and burden as well of procedures associated with the selected functionalities for businesses and individuals. The online availability of the procedures can be considered as a relevant condition towards the implementation of OOP as it indicates that the traditional "in-presence" procedures have already been translated in on-line data collection systems with the capacity to categorise and store information in digital databases. Nevertheless, the poor availability of pre-filled formats suggests a scarce re-use of information previously provided and a lack of procedures for retrieving information from existing sources. Additionally, the need to submit documents to complete certain procedures indicates that the traditional certification-based paradigm has not completely changed towards a data-oriented one. This change will be key for an effective implementation of OOP as, in this case, the focus would be on the information and its transmission rather than on the authentication of documents and on the authenticating authority.

In order to understand the effective reduction of the administrative burdens for business and individuals, this study goes beyond the analysis of data of the eGovernment Benchmark Framework 2012-2015 and defined a set of **use cases** used to gather specific information on user experiences (including associated time and effort) when requesting specific services in cross-border situations.

Different perspectives are taken into account through the identified use cases:

- The one investigated through desk research and analysis of the procedures of specific functionalities
- The one of businesses and individuals through the OOP on-line questionnaire (http://formit-survey.eu/doop/)
- The one of public administration officials through interviews
- The one of the officials of individuals and businesses organisations (i.e. chambers of commerce) through interviews

Each use case is built around a neutral scenario composed of functionalities that could be requested in any EU Member State by individuals or businesses from another Member State. Each use case is then associated to a specific pair of Member States: the one from which the requesting actor comes or where information was previously provided, is called the *data holder country* and the one in which the actor requests a certain functionality is called the *data demander country*.

To improve comparative analysis among selected Member States, use cases are paired; a situation in which country X is the *data holder* and country Y is the *data demander* is paired with a case in which the roles are reversed for the same set of functionalities. Interviews with officials of national public administrations were used to validate the use cases, to understand whether and how much the selected functionalities are actually demanded by actors of the data demander country, if there are specific cross-border procedures for data and information exchange and which authorities/bodies of the data demander country are involved in the procedure.

The proposed combination of functionalities and Member States generated **four use cases for businesses and two use cases for individuals.** Table 13 below presents an overview of the six investigated use cases (identified with letters A, B, C, D, E, F) and their combination of functionalities and Member States.

Table 13: Overview of functionalities and countries

BUSINESSES' FUNCTIONALITY	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
#1 Register company name								UC-A]		UC-A]
#2 Register domicile of business		UC-D]							UC-D]	
#3 Register (a company or a branch of a company) in a business register	UC-C]					UC-C]		UC-A]		UC-A]
#4 Receive formal validation of signatures of representatives of the business		UC-D]							UC-D]	
#5 Register with social security office	UC-C]					UC-C]				
#6 Register with compulsory healthcare	UC-C]					UC-C]				
#7 Be compliant with social security obligations			UC-B]		UC-B]					
#8 Be compliant with obligations related to work place security	UC-C]					UC-C]		UC-A]		UC-A]
#9 Be compliant with tax related obligations			UC-B]		UC-B]			UC-A]		UC-A]
#10 Register employee before first work day								UC-A]		UC-A]

INDIVIDUALS' FUNCTIONALITY	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
#1 Enrolling in higher education		UC-E]					UC-E]			
#2 Applying for student grants		UC-E]					UC-E]			
#3 Obtaining financial aid for starting up as self-employed				UC-F]						UC-F]
#4 Registering for unemployment benefits		UC-E]					UC-E]			
#5 Ensuring continuity of pension payments				UC-F]						UC-F]

Business use cases

Starting a business branch

Requesting a licence for the carriage of goods

Bidding for a Public Procurement contract for construction services

Establishing a new association

Individual use cases

Enrolling in a Master course

Starting up as self employed

B. Functionalities Description

In this section we describe the functionalities in their full extent: first the Business functionalities, than the individuals' functionalities.

B.1. BUSINESS

1. Register company name

Definition

This service ensures that the entrepreneur obtains the company name he/she is seeking and the formal approval of the proposed name

Description of the procedure

This functionality is typically included in the procedures related with company registration/start up in the business register and is considered to be mostly a once-in lifetime event for a business, as it characterises its activity and will constitute a means of recognition of the business from both consumers, suppliers, partners and concurrent. The management of this procedure varies from national to local level but essentially implies the registration of a company/business name after checking procedure to avoid using the already existing or inappropriate company name. Any change of the company's name will need to undergo the same procedure.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Geographical level *	?	LOC	PUB	n/a	NAT	NAT	n/a	NAT	LOC	NAT
Type of provider**	?	PUB	NAT	n/a	PUB	PUB	n/a	PUB	PUB	PUB

[*] - National/regional/local; [**] – Public / Private
[n/a] – Not applicable; [?] – Information Not Available

Online availability of the procedure and key characteristics

According to the information available, this procedure is available online in the 50% of the cases considered as is handled automatically in Belgium. In all these cases, authentication is requested via online procedure: identification via eID is available only in one case out of five. In the majority of the relevant cases, subjects are requested to submit documents to complete the procedure: the online submission is available in 2 out of 5 cases. Finally, there is no evidence of prefilled forms but for Belgium where the procedure is handled automatically.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of the service	YES Auto-mated[14]	YES URL[15]	?	n/a	YES URL	YES URL	YES	NO[16]	YES URL	YES URL
Authentication request	YES	YES	?	?	?	YES	YES	YES	YES	YES
Online authentication procedure availability	YES	YES	?	?	?	NO	YES	NO	YES	YES
Availability of authentication via eID	YES	YES	?	?	?	NO	YES	NO	NO	NO
Is any kind of documentation needed to complete the procedure?	YES	YES	?	?	?	NO	YES	YES	NO	YES
Is it possible to submit required documentation online?	YES	YES	?	?	?	NO	YES	NO	NO	YES
Are personal data pre-filled?	YES	NO	?	?	?	NO	NO	NO	NO	NO

Online availability for non-national users

As it can be seen from the following table, data available are scarce and does not allow for a consistent and relevant assessment of the online availability of the functionality in object for non-national users. Information gaps will be filled by means of the information gathered thought the interviews.

[14] Service provided to the user without the user having to request it

[15] In Germany only notaries are allowed to register companies by filing their names in the Trade Register, which is an online register. Notaries carry out the registration process via the internet by using their qualified electronic signatures. User information can be funded in local websites such as those of Berlin, Munich, Frankfurt and Hamburg

[16] Website of reference for the functionality in object http://www.kvk.nl/inschrijven-en-wijzigen/formulieren/inschrijven-onderneming-eenmanszaak/

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of information for non-country nationals	Y Auto-mated[17]	Y	?	?	Y	N	Y	?	NO	Y
Online availability of service for non-country nationals	?	N	?	?	N	N	Y	?	NO	Y
Need national online identification/authentication	?	N	?	?	N	N	Y	?	Y	?
Need for translation or recognition of required documents	?	Y	?	?	Y	N	N	?	Y	?
Need for physical encounter to complete the procedure	?	Y	?	?	N	N	N	?	N	?

[17] Service provided to the user without the user having to request it

2. Register domicile (registered office) of a company

Definition

This refers to registering the company's address, i.e. the address of its registered office

Description of the procedure

In most Member States, the address of registered office links a company to the legal order of a country in which it was formed and therefore, constitutes the main point of reference for the provision of official communications and for the definition of applicable rules and procedures (e.g. for setting up or dissolving a company, as regards its activities and internal affairs)[18]. The registration of a company's registered office forms part of the company registration/start up procedure and this information needs to be updated and filed with the business register whenever location of reference is changed (even without substantial modifications to the business itself).

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Geographical level *	n/a	LOC	NAT	NAT	NAT	NAT	NAT[19]	NAT	REG	NAT
Type of provider **	n/a	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB

[*] - National/regional/local; [**] – Public / Private
[n/a] – Not applicable ; [?] – Information Not Available

Online availability of the procedure and key characteristics

According to the data reported in the following table, this functionality is available online in the 60% of the cases considered and is processed automatically in Belgium (with significant savings for involved subjects in terms of time and effort). Where the procedure is available online, the involved subject needs to authenticate via an online procedure (available in 90% of the cases) or via eID (available in 50% of the cases). The submission of documents is requested only in the 30% of the case for which online procedure is available, and in all

[18] In some Member States, the laws of the country where the company's central administration/headquarters are located will be applied as the main point of reference.

[19] Since 1 April 2010 the Single Communication has simplified relations between companies and the Public Authorities. All obligations can be completed at a single electronic hub, the Italian Business Register, which is the only place to which the electronic file containing the information for all the entities is to be sent. The Single Communication file is a set of files structured as follows: Single Communication form (document containing the applicant's details, the object of the communication and the summary of applications to different entities); forms for the Business Registry; forms for the Inland Revenue; forms for INAIL; any SCIA (Certified Notification of a Start of Activity) for the SUAP (Single Information Point for Productive Activity).

these cases the submission can be done online. Finally, pre-filled forms are available only in one case, which indicate low reuse of already submitted information.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of the service	YES [20]	NO[21]	YES URL	YES URL	NO [22]	YES URL	YES URL	NO[23]	YES URL	YES URL
Authentication request	YES	NO	YES	YES	YES	YES	YES	NO	YES	YES
Online authentication procedure availability	YES	NO	YES	YES	?	NO	YES	NO	YES	YES
Authentication via eID available?	YES	NO	YES	YES	?	NO	YES	NO	NO	NO
Documentation needed to complete the procedure?	YES	NO	YES	?	?	NO	YES	NO	NO	YES
Online submission possible?	YES	NO	YES	?	?	NO	YES	NO	NO	YES[24]
Are personal data pre-filled?	YES	NO	YES	?	?	NO	NO	NO	NO	?

Online availability for non-national users

As it can be seen from the following table, data available are scarce and does not allow for a consistent and relevant assessment of the online availability of the functionality in object

[20] In this case we consider the case of the Chamber of Commerce of the Region of Brussels considering it as representative for the situation of Belgium. Nevertheless, the service provided by other regional Chamber of Commerce may vary in its peculiarities.

[21] In this case the service is provided at local level: for the purposes of this description we took into consideration the case of Berlin as representative of the country situation (website currently under restructuring). Nevertheless the procedure my vary depending on the local administration considered [more information on local websites Munich and Cologne]

[22] Website of reference for the functionality in object https://www.prh.fi/en/kaupparekisteri/rekisterointipalvelut.html

[23] Website of reference for the functionality in object http://www.kvk.nl/inschrijven-en-wijzigen/formulieren/inschrijven-onderneming-eenmanszaak/

[24] In particular, for the change of the domicile of the registered office, companies can submit the form online if the company is in the PROOF (PROtected Online Filing) scheme.

for non-national users. Information gaps will be filled by means of the information gathered thought the interviews.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of information for non-country nationals	YES Automated[25]	YES[26]	YES URL	YES	YES	NO	YES	?	NO	YES
Online availability of service for non-country nationals	n/a	YES	YES	?	NO	NO	YES	?	NO	YES
Need national online identification/authentication	n/a	?	?	?	NO	?	YES	?	YES	?
Need for translation or recognition of required documents	n/a	?	?	?	YES	?	?	?	YES	?
Need for physical encounter to complete the procedure	n/a	?	?	?	NO	?	?	?	NO	?

[25] In this case we consider the case of the Chamber of Commerce of the Region of Brussels considering it as representative for the situation of Belgium. Nevertheless, the service provided by other regional Chamber of Commerce may vary in its peculiarities.

[26] In this case the service is provided at local level: for the purposes of this description we took into consideration the case of Berlin as representative of the country situation (website currently under restructuring). Nevertheless the procedure my vary depending on the local administration considered [more information on local websites Munich, Frankfurt and Cologne]

3. Register (a company or branch) with a business register

Definition

This service refers to registration of a company or a branch within a business register. By this procedure a company is created as a legal person (typically by means of a notary act). As part of that procedure, documents regarding company's name and registered office are submitted and registered. Depending on the Member State, formal validation of signatures of representatives of the business might be required.

Description of the procedure

Depending on the national organisation, this registration may correspond to the registration to the Chambers of commerce or to a Trade Association, or may correspond to the registration in a business register managed by a public authority. Chambers of commerce, as well as Trade associations, are networks of operators aimed at providing support to businesses in their life-cycle. In some cases, such as in Italy, the register of the Chambers of Commerce works as primary point of reference for a number of public functions. In addition, different bodies (e.g. a Ministry or a Chamber of Commerce) are responsible for running the business register in a particular country. Concerning the business registers, as of June 2017, the business registers interconnection system (BRIS) will be operational and will (1) make it possible for national business registers to electronically notify one another in certain fields and (2) make information which limited liability companies are obliged to file with the business registers in accordance with EU law (Directive 2009/101), e.g. company registration number, legal form, address, available to the general public via the European e-Justice portal.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Geographical level *	NAT	REG	NAT	REG	NAT	NAT	NAT	NAT	REG	NAT
Type of provider **	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB

[*] - National/regional/local; [**] – Public / Private
[n/a] – Not applicable; [?] – Information Not Available

Online availability of the procedure and key characteristics

This functionality is actually available online (up to the submission of documents and completion of the registration) in the 60% of the countries analysed. . Where online procedure is available, the founders of companies/businesses are always requested to authenticate with personal information (e.g. ID document references and/or login details) the procedure except for Estonia; additionally, Italy and The Netherlands provides the possibility to authenticate via eID. In the majority of cases, to complete the online

procedure founders of companies/businesses are requested to submit documents only via online means, which reduces the effort associated with the procedure. It is worth noting that the amount of documents to be submitted to complete the registration is minor where online procedure is available, whereas in presence procedures tend to require the provision of extensive documentation (e.g. Romania). This evidence seems to suggest that, although prefilled forms are typically not available, the online procedures have actually been designed to reduce burdens and costs for applying subjects.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of the service	NO[27]	YES URL	YES URL[28]	NO[29]	NO[30]	YES URL	YES URL[31]	YES URL	NO[32]	YES URL
Authentication request	NO	YES	NO	NO	NO	YES	YES	YES	NO	YES
Online authentication procedure availability	NO	YES	NO	NO	NO	YES	YES	NO	NO	YES
Availability of authentication via eID	NO	NO	NO	NO	NO	NO	YES	YES	NO	NO
documentation needed to complete the procedure?	YES	NO	YES	NO	YES	YES	YES	NO	YES	YES
Online submission required documentation?	NO	NO	YES	NO	NO	YES	YES	NO	NO	YES
Are personal data pre-filled?	NO	NO	NO	NO	NO	YES	NO	NO	NO	NO

[27] Registration on to the Banque Carrefour des Entreprises requires physical meeting either at the competent Tribunal of Commerce or at a business stop-shop (including Chambers of Commerce, such as the Brussels Enterprises Commerce and Industry)

[28] The registration can also be done in-presence at a notary premises

[29] The business register of reference in Spain correspond to the one of the Chamber of Commerce

[30] Through the website it is possible to download the forms needed and have a clear view of all documents requested, but actual submission should be sent in hard paper by normal mail

[31] The business register of reference in Italy correspond to the one of the Chamber of Commerce

[32] Website of reference for the functionality in object http://www.ccir.ro/

Online availability for non-national users

The tendency encountered in the analysis of the functionality in object is that where the procedure is available online for national users it is also available for non-nationals without any discrimination. The procedure does not actually vary for non-national users, but additional information is always provided in one or more languages to allow foreigners to better understand the procedure.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of information for non-country nationals	Y [33]	Y [34]	Y [35]	Y	Y [36]	Y	Y [37]	Y URL	Y	Y
Online availability of service for non-country nationals	N	Y	Y	Y	N	Y	Y	Y	N	Y
Need national online identification/Authentication	N	N	N	?	N	Y	Y	Y	N	N
Need for translation or recognition of required documents	N	N	N	?	Y	?	N	N	Y	N
Need for physical encounter to complete the procedure	Y	N	N	?	N	N	N	N [38]	Y	N

[33] Information are available in French, German, English and Italian and Spanish, but the format to fill in is in German.

[34] In this case the service is provided at local level – for the purposes of this description we took into consideration the case of Berlin as representative of the country situation. Nevertheless the procedure my vary depending on the local administration considered [more information on local websites Munich, Frankfurt and Cologne]

[35] Information are available in Estonian and English

[36] Information available in Finnish and English

[37] The services is available in Italian and English

[38] The in presence registration is made available as alternative option to online registration but is not compulsory needed.

4. Formal validation of signature of a company representative

Definition

Before a person can act as a representative of the company, his/her formal signature needs to be checked officially, e.g. at a governmental department.

Description of the procedure

The formal validation of the signature of the company representative is a prerequisite for a number of procedures at national and cross-border level. This procedure is heterogeneously managed and is not mandatory required in all Member states. In those Member States this formal validation forms part of the company registration/start up procedure or is required whenever there is a change of the business representative (even without substantial modifications to the business itself). Any change of the company's business representatives will need to be filed with the business register.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Geographical level *	?	?	?	?	?	NAT	?	?	NAT	NAT
Type of provider **	?	?	?	?	?	PUB	?	?	PUB	PUB

[*] - National/regional/local; [**] – Public / Private
[n/a] – Not applicable; [?] – Information Not Available

Online availability of the procedure and key characteristics

The procedure appear to be available online only in Hungary and the UK. No additional information was provided within the eGovernment benchmarking raw data. Information gap will be eventually filled profiting of the information gathered through the interviews.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of the service	NO	NO	NO	NO	NO	YES URL	NO	NO	NO	YES URL

Online availability for non-national users

The lack of service online availability is mirrored in the lack of information for non-national users available online about this procedure. Where possible, additional information will be gathered through the interviews.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of information for non-country nationals	NO	NO	NO	NO	NO	YES	NO	NO	NO	YES
Online availability of service for non-country nationals	NO	NO	NO	NO	NO	YES	NO	NO	NO	YES

5. Register with Social Security Office

Definition

This service refers to the registration within the Social Security Office

Description of the procedure

Social security refers to the policies and programmes intended to promote the welfare of the population through assistance measures concerning for instance pension funds, workplace security, healthcare related obligations and unemployment subsidies. For all these services to be addressed and protections guaranteed, all businesses have to register in the correspondent Social Security Office, which can be settle at either national or local level depending on the system's characteristics.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Geographical level *	NAT	NAT	?	NAT	NAT	NAT	NAT	NAT	LOC	NAT
Type of provider **	PUB	PUB	?	PUB	PUB	PUB	PUB	PUB	PUB	PUB

[*] - National/regional/local; [**] – Public / Private
[n/a] – Not applicable ; [?] – Information Not Available

Online availability of the procedure and key characteristics

The functionality in object is available online in the 60% of the cases considered and is handled automatically in Estonia. In all cases, the requesting subject needs to authenticate to access the functionality, either via online procedures or via eID accreditation (available in 5 cases out of 6). Documentation is typically requested with a correspondent online procedure available in all cases but in Romania. Prefilled forms are reported to be available in the 50% of relevant cases, suggesting an initial use of already provided data and information.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of the service	YES URL	YES URL	YES Automated [39]	YES URL	NO [40]	YES URL	YES URL	NO [41]	YES URL	NO [42]
Authentication request	YES	YES	YES	YES	?	YES	YES	YES	YES	YES
Online authentication procedure availability	YES	YES	YES	YES	?	YES	YES	NO	YES	NO
Availability of authentication via eID	NO	YES	YES	YES	?	YES	YES	NO	NO	NO
Is any kind of documentation needed to complete the procedure?	NO	YES	YES	YES	?	YES	YES	YES	NO	YES
Is it possible to submit required documentation online?	YES	YES	YES	YES	?	YES	YES	NO	NO	NO
Are personal data pre-filled?	NO	NO	YES	YES	?	YES	NO	NO	NO	NO

Online availability for non-national users

According to the data available, this functionality has information available online for non-national users in almost all cases considered (excluding Hungary and Romania): nevertheless the service is actually available online for non-national users only in the 40% of the cases.

[39] Service provided to the user without the user having to request it

[40] Website of reference for the functionality in object http://www.prh.fi/en/kaupparekisteri.html

[41] Website of reference for the functionality in object http://www.ondernemersplein.nl/zoeken/term-sociale%20zekerheid%20eenmanszaak

[42] Website of reference for the functionality in object http://search2.hmrc.gov.uk/kb5/hmrc/forms/view.page?record=WCHblKPNSXc&formid=3643

Nevertheless, it worth mentioning that translation of documents and certifications, which constitute a primary component of administrative costs, is requested only in Finland and Romania.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of information for non-country nationals	YES	YES	YES Auto-mated	YES	YES	NO	YES	YES	NO	YES
Online availability of service for non-country nationals	YES	YES	n/a	NO	NO	NO	YES	YES	NO	NO
Need national online identification/authentication	NO	n/a	n/a	YES	NO	NO	n/a	NO	NO	NO
Need for translation or recognition of required documents	NO	n/a	n/a	NO	YES	NO	n/a	NO	YES	NO
Need for physical encounter to complete the procedure	NO	n/a	n/a	YES	NO	NO	n/a	NO	NO	YES

6. Register with compulsory healthcare

Definition

This service refers to signing up for compulsory healthcare

Description of the procedure

This functionality refers to the need for a business to register with compulsory healthcare for the benefit of its employee and to ensure the compliance with legal requirements. Compulsory healthcare may vary in terms of jurisdictions and coverage according to the context in object.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Geographical level *	NAT	NAT	NAT	NAT	NAT	NAT	NAT	NAT	LOC	NAT
Type of provider **	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB

[*] - National/regional/local; [**] – Public / Private
[n/a] – Not applicable ; [?] – Information Not Available

Online availability of the procedure and key characteristics

The functionality in object is available online in the 50% of the cases and appears to be provided automatically in Estonia and Italy. For the relevant cases, online authentication is always requested except in Netherlands, and authentication via eID is available in the 40% of the cases. In the majority of the cases, it seems that no additional documents are requested to be submitted, with relevant impacts on the procedure's costs in terms of time and effort. Nevertheless, prefilled forms are rarely available, suggesting a low reuse of data and information already provided.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of the service	YES URL	YES URL	YES Automated [43] URL	YES URL	YES URL	NO[44]	YES Automated [41]	YES URL	NO	NO

[43] Service provided to the user without the user having to request it

[44] Website of reference for the functionality in object http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99700083.TV

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Authentication request	YES	YES	YES	YES	?	NO	?	YES	NO	NO
Online authentication procedure availability	YES	YES	YES	YES	?	NO	?	NO	NO	NO
Availability of authentication via eID	NO	YES	YES	YES	?	NO	?	NO	NO	NO
Is any kind of documentation needed to complete the procedure?	NO	NO	YES	YES	?	NO	?	NO	NO	NO
Is it possible to submit required documentation online?	NO	NO	YES	YES	?	NO	?	NO	NO	NO
Are personal data pre-filled?	NO	NO	YES	YES	?	NO	?	NO	NO	NO

Online availability for non-national users

As it can be seen from the following table, the functionality in object is actually available online for non-national users only in Finland and The Netherlands, for which no additional information appear to be available. Due to this and other information gaps related with the online availability of this functionality for non-national users, interviews will be used to gather additional information on this subject.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of information for non-country nationals	NO	YES	YES Automated [41]	YES	YES	NO	YES Automated [41]	YES	NO	YES

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of service for non-country nationals	NO	NO	?	NO	YES	NO	?	YES	NO	NO
Need national online identification/authentication	NO	NO	?	YES	?	NO	?	?	NO	YES
Need for translation or recognition of required documents	NO	YES	?	NO	?	NO	?	?	YES	NO
Need for physical encounter to complete the procedure	NO	YES	?	YES	?	NO	?	?	NO	YES

7. Social security obligation

Definition

Withholding of contributions for social insurances from employee's wages

Description of the procedure

Social security refers to the policies and programs intended to promote the welfare of the population through assistance measures concerning for instance pension funds, workplace security, healthcare related obligations and unemployment subsidies. All businesses have to comply with social security related obligations: these services can be provided at both national and regional level by deputed public agencies.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Geographical level *	NAT	NAT	NAT	NAT	NAT	REG	NAT	NAT	REG	NAT
Type of provider **	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB

[*] - National/regional/local; [**] – Public / Private
[n/a] – Not applicable; [?] – Information Not Available

Online availability of the procedure and key characteristics

Based on the information available, this functionality is typically available online with the request of authentication which can be made via ad hoc online accreditation (in the 60% of the cases) and or via eID (in the 40% of the cases). Additional documents to complete the procedure are requested only in the 40% of the cases with online submission procedures available in the majority of these cases, whereas prefilled information is available only in the 30% of the cases. In Belgium, this functionality is provided automatically without the subject in object having to request it, with significant savings of time and effort.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of the service	YES Automated[45]	YES URL	YES URL	YES URL	?	YES URL	YES URL	YES URL	YES URL	YES URL

[45] Service provided to the user without the user having to request it

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Authentication request	YES	YES	YES	YES	?	YES	YES	YES	YES	YES
Online authentication procedure availability	YES	YES	YES	YES	?	NO	YES	NO	YES	NO
Availability of authentication via eID	YES	YES	YES	YES	?	NO	NO	NO	YES	NO
Documentation needed to complete the procedure?	YES	NO	YES	YES	?	NO	NO	NO	YES	NO
Is it possible to submit required documentation online?	YES	NO	YES	YES	?	NO	NO	NO	NO	NO
Are personal data pre-filled?	YES	NO	YES	YES	?	NO	NO	NO	NO	NO

Online availability for non-national users

In the eGovernment raw data, JOB functionalities were not analysed in the cross-border case.

8. Obligations related to work place security

Definition

In most Member States it is required to have a documented Health & Safety plan when hiring employees

Description of the procedure

This functionality refers to all reporting obligations relevant to ensure the workplace security, from both the physical and procedural point of view. To ensure the healthiness, businesses are typically request to provide periodical reports about the state of the workplace to the referent authority, unstructured data and information, and to undergone periodical controls. This functionality can be managed at either national or local level.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Geographical level *	NAT	LOC	NAT	NAT	NAT	n/a	NAT	NAT	LOC	NAT
Type of provider **	PUB	PUB	PUB	PUB	PUB	n/a	PUB	PUB	PUB	PUB

[*] - National/regional/local; [**] – Public / Private
[n/a] – Not applicable ; [?] – Information Not Available

Online availability of the procedure and key characteristics

As it can be seen from the following table, data available are scarce and does not allow for a consistent and relevant assessment of the online availability of the functionality in object and its key features. Information gaps will be filled by means of the information gathered thought the interviews.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of the service	NO	NO	NO	YES URL	NO	N/A	NO	NO	NO	NO
Authentication request	?	?	?	YES	?	N/A	?	?	?	?
Online authentication procedure availability	?	?	?	YES	?	N/A	?	?	?	?

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Availability of authentication via eID	?	?	?	YES	?	N/A	?	?	?	?
Is any kind of documentation needed to complete the procedure?	?	?	?	?	?	N/A	?	?	?	?
Is it possible to submit required documentation online?	?	?	?	?	?	N/A	?	?	?	?
Are personal data pre-filled?	?	?	?	?	?	N/A	?	?	?	?

Online availability for non-national users

In the eGovernment raw data, JOB functionalities were not analysed in the cross-border case.

9. Tax related obligations

Definition

Withholding of income tax and possibly other taxes from the employee's wages

Description of the procedure

Tax related obligations constitute a crucial point for businesses with potential relevant drawbacks in case of inappropriate handling. They can be addressed at national or local level according to the system and include tax number registration, provision of information and data on the business activities, provision of information related with hired personnel and recording of tax payments.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Geographical level *	NAT	LOC	NAT	NAT	N/A	NAT	NAT	N/A	LOC	N/A
Type of provider **	PUB	PUB	PUB	PUB	N/A	PUB	PUB	N/A	PUB	N/A

[*] - National/regional/local; [**] – Public / Private
[N/A] – Not applicable; [?] – Information Not Available

Online availability of the procedure and key characteristics

Based on information provided, this functionality is available online only in the 40% of the cases, and is provided automatically in Belgium. For all relevant cases, users need to authenticate, either via online accreditation procedure or via eID without any relevant difference reported. Additionally, in all these cases there is a need to submit documents which can be done via online procedures in all cases (not in Romania) with relevant savings of time and efforts to complete the procedure.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Service online availabe	YES Auto-mated[46]	NO[47]	YES URL	YES URL	NO [48]	NO [49]	NO [50]	YES URL	YES URL[51]	NO

[46] Service provided to the user without the user having to request it

[47] Website of reference for this functionality http://www.existenzgruender.de/checklisten_und_uebersichten/steuer_versich/index.php

[48] Website of reference for this functionality https://oma.yrityssuomi.fi/en/home

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Authentication request	YES	NO	YES	YES	NO	NO	YES	YES	YES	NO
Online authentication procedure available	YES	NO	YES	YES	NO	NO	NO	YES	YES	NO
Authentication via eID available?	YES	NO	YES	YES	NO	NO	NO	YES	YES	NO
Additional documentation needed?	YES	NO	YES	YES	NO	NO	YES	YES	YES	NO
Online submission of documentation possible?	YES	NO	YES	YES	NO	NO	NO	YES	NO	NO
Are personal data pre-filled?	YES	NO	YES	YES	NO	NO	NO	YES	NO	NO

Online availability for non-national users

In the eGovernment raw data, JOB functionalities were not analysed in the cross-border case.

---

[49] Website of reference for this functionality http://www.nav.gov.hu/magyar_oldalak/nav/szolgaltatasok/adokulcsok_jarulekmertekek/munkajar?honap=2012_10

[50] Website of reference for this functionality http://www.registroimprese.it/comunica#tab=cosa&under-tab=corsi

[51] In this case the service is provided at local level: for the purposes of this description we took into consideration http://itmonline.inspectiamuncii.ro/itm/welcome.do. Nevertheless the procedure my vary depending on the local administration considered [more information on local websites URL, URL and URL]

10. Register employee before first day

Definition

In some Member States, employers should announce the start of an employee before the first day of working, normally at tax office (to prevent fraud and illegal work)

Description of the procedure

The registration of new employee is a key element in the hiring procedure of a company: by means of this registration, the employer transmits to the competent authority all data and personal information concerning the new employee. The procedure and the competent authorities may vary, but employees are requested to keep these records updated according to any changes occurring concerning the employee.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Geographical level *	NAT	NAT	NAT	NAT	N/A	NAT	NAT	N/A	LOC	N/A
Type of provider **	PUB	PUB	PUB	PUB	N/A	PUB	PUB	N/A	PUB	N/A

[*] - National/regional/local; [**] – Public / Private
[N/A] – Not applicable; [?] – Information Not Available

Online availability of the procedure and key characteristics

According to the information available, this functionality is available online in all relevant cases, with the need to authenticate in all cases but in Germany. Authentication via eID is not foreseen in the case of Romania and Hungary, whereas it is possible in all other considered cases. In the 50% of the cases, the user is requested to submit additional documents, but for all these cases the submission can be done online.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of the service	YES URL	YES URL	YES URL	NO URL	N/A	YES URL	YES URL	N/A	YES URL[52]	N/A
Authentication request	YES	NO	YES	YES	N/A	YES	YES	N/A	YES	N/A
Online authentication procedure availability	YES	NO	YES	YES	N/A	NO	YES	N/A	YES	N/A
Availability of authentication via eID	YES	NO	YES	YES	N/A	NO	YES	N/A	NO	N/A
Is any kind of documentation needed to complete the procedure?	YES	NO	YES	?	N/A	NO	YES	N/A	NO	N/A
Is it possible to submit required documentation online?	YES	NO	YES	?	N/A	NO	YES	N/A	NO	N/A
Are personal data pre-filled?	YES	NO	YES	?	N/A	NO	NO	N/A	NO	N/A

Online availability for non-national users

In the eGovernment raw data, JOB functionalities were not analysed in the cross-border case.

[52] In this case the service is provided at local level: for the purposes of this description we took into consideration http://itmonline.inspectiamuncii.ro/itm/welcome.do . Nevertheless the procedure my vary depending on the local administration considered [more information on local websites URL, URL and URL]

CITIZENS

1. Enrolling in Higher Education

Definition

Standard procedure to enrol students in a university or another institution of higher education subsidised by an official administrative body in the country, including the provision of personal documents and/or eventual qualifications

Description of the procedure

After selecting an institution, an individual willing to enrol needs to address standardised modules to declare this willingness, providing personal data and information (including indications of previous studies) and details related to the selected course. After this step, individuals might be requested to take an admission test and/or undergo a check of achievements in previous studies (especially when changing institution) and pay enrolment fees. All these procedures are typically handled at regional or local level.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Geographical level *	REG	LOC	NAT	REG	NAT	REG	LOC	NAT	NAT	NAT
Type of provider **	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB

[*] - National/regional/local; [**] – Public / Private
[N/A] – Not applicable; [?] – Information Not Available

Online availability of the procedure and key characteristics

As reported in footnote, in the majority of the cases analysed, enrolling in higher education is a process managed at local level by each institution in object: for the purposes of the analyses in object the following table reports the status of the service provided for the university of the capital city, considered representative for the national case. Nevertheless, key features may vary, and additional links are reported in footnote.

Information available indicates that for all cases analysed but Hungary, the functionality is available online and does request an authentication procedure, which typically (60% of the cases) is not associated with eID accreditation. The procedure does not always request the submission of additional documents, but when it does, there is a fifty-fifty possibility to have the possibility to submit them online, thus reducing the costs associated with the completion of this procedure. Additionally, in the 40% of the cases considered, there are available pre-filled forms, which indicate an effective reuse of data previously submitted within the same organisation or in other ones.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of the service	YES URL[53]	YES URL[54]	YES URL[55]	YES URL[56]	YES URL	NO URL[57]	YES URL[58]	YES URL	YES URL[59]	YES URL
Authentication request	YES	YES	YES	YES	YES	NO	YES	YES	NO	YES
Online authentication procedure availability	YES	YES	YES	YES	YES	NO	YES	YES	NO	YES
Availability of authentication via eID	NO	NO	YES	YES	YES	NO	NO	YES	NO	NO

[53] The reported URL correspond to the case of the Université Libre de Bruxelles (considered representative for the national case). Nevertheless the key feature may vary according to the university in object (Université Catholique de Louvain, Universiteit Gent, Université de Liège).

[54] The procedure is managed at university level. The URL reported in the table refers to the University of Frankfurt: nevertheless the same key features were reported also for the university of Munich and Hamburg

[55] https://www.sais.ee/ is a unified and general websites for higher education institutions in order to carry out the procedure of enrolling.

[56] The URL reported in the table refers to Universidad Complutense de Madrid: nevertheless, eGovernment raw data referred the same key features for other universities (Universidad de Barcelona, Universidad de Granada, Universitat de Valencia). Although the "enrollment in a university is a service provided for each University that depends on the Regional government, there is one website at the central Government that acts as a single point (Single Access Point) to have access to the "enrolling" service for all the Universities in Spain (http://www.universia.es/).

[57] The reported URL correspond to the case of the University of Budapest (considered representative for the national case). Nevertheless the key feature did not vary among the universities considered in the eGovernment raw data (e.g. University of National Excellence).

[58] The reported URL correspond to the case of the Sapienza University of Roma (considered representative for the national case). Nevertheless the key feature may vary according to the university in object (University of Torino, University of Naples, University of Milan)

[59] The reported URL correspond to the case of the University of Bucharest (considered representative for the national case). Nevertheless the key feature did not vary among the universities considered in the eGovernment raw data (University of Vest, University Babes Bolyai).

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Is any kind of documentation needed to complete the procedure?	NO	NO	YES	YES	YES	NO	YES	NO	NO	NO
Is it possible to submit required documentation online?	NO	NO	YES	NO	YES	NO	NO	NO	NO	NO
Are personal data pre-filled?	NO	NO	YES	YES	YES	NO	NO	YES	NO	NO

Online availability for non-national users

For what concerns online availability of the functionality for non-national users, many information are missing, reducing the opportunity to provide a complete assessment of the state of availability of this functionality. Nevertheless, information available indicate that information for non-national users are available online in the 80% of the cases analysed and that the procedure is actually available online in the 60% of the cases. It is interesting to underline that Estonia has a dedicated web page for non-nationals to gather additional and dedicated information to enrol in national higher education (https://estonia.dreamapply.com/) which act as single point of contact increasing the efficiency of the service provided and reducing costs associated with duplication of information provision.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of information for non-country nationals	Y	Y	Y [60]	Y	Y	Y	Y	NO	?	Y

[60] Foreign students can also apply for a study programme in Estonia via https://estonia.dreamapply.com/

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of service for non-country nationals	Y	Y	Y	N	Y	Y	N	N	?	Y
Need national online identification/authen-tication	N	?	Y	?	?	N	N	Y	?	?
Need for translation or recognition of required documents	N	?	N	?	?	N	Y	N	?	?
Need for physical encounter to complete the procedure	N	?	N	?	?	N	N	N	?	?

2. Applying for student grants

Definition

Student procedure to obtain student grants for higher education

Description of the procedure

The application for student grants is a fundamental financial support to ensure the equal opportunities to access studying opportunities for young individuals. Student grants are intended to support the costs that an individual has to face during the studying period, including costs of learning supports, institutional fees and, eventually, costs of stays. This support is typically attributed based on a selection procedure that assesses criteria such as household income and results in previous education. Student grants can be provided by national, regional or local funds, as well as by the university itself.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Geographical level *	REG	NAT	NAT	NAT	NAT	?	LOC	NAT	?	NAT
Type of provider **	PUB	PUB	PUB	PUB	PUB	?	PUB	PUB	?	PUB

[*] - National/regional/local; [**] – Public / Private
[N/A] – Not applicable ; [?] – Information Not Available

Online availability of the procedure and key characteristics

Based on the information available we can consider that typically the procedure for applying for a student grant is typically available online with a request for authentication, either by means of ad hoc authentication data or via eID procedures. In the majority of the cases analysed, the procedure requires the submission of document which is not available online: this increases the costs and efforts associated with this procedure.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of the service	YES URL	YES URL	YES URL	YES URL	YES URL	?	YES URL[61]	YES URL	?	YES URL

[61] The reported URL correspond to the case of the Sapienza University of Roma (considered representative for the national case). Nevertheless the key feature may vary according to the university in object (e.g. University of Milan). The following link can be used as single point of

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Authentication request	YES	YES	YES	YES	YES	?	YES	YES	?	YES
Online authentication procedure availability	NO	NO	YES	YES	YES	?	YES	YES	?	YES
Availability of authentication via eID	NO	NO	YES	YES	YES	?	YES	YES	?	NO
Is any kind of documentation needed to complete the procedure?	NO	NO	YES	YES	YES	?	YES	NO	?	YES
Is it possible to submit required documentation online?	NO	NO	YES	YES	YES	?	NO	NO	?	NO
Are personal data pre-filled?	NO	NO	YES	NO	YES	?	NO	YES	?	NO

Online availability for non-national users

According to the information available, supporting information for non-national individuals intending to apply for a student grants are typically available (regardless the fact of having same information provided in multiple languages or ad hoc information for non-national users). Nevertheless, the procedure to actually apply for a student grant online is available only in the 40% of the cases. It worth mentioning that in all cases considered but Italy, non-national users does not need to translate or having documents officially recognised to complete the procedure. Additionally, in none of the cases analysed but Finland, there is a need for applying individual to have a physical encounter with a deputed officer to complete the

contact to gather information on available student grants
http://www.andisu.it/pagine/bandi_universitari

procedure. These two factors consistently reduce the costs a non-national individual have to bear while applying for a student grant.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of information for non-country nationals	NO	YES	YES	NO	YES	YES	YES	YES	YES	YES
Online availability of service for non-country nationals	NO	NO	YES	NO	YES	YES	NO	YES	NO	NO
Need national online identification/authentication	NO	NO	YES	NO	NO	NO	NO	YES	NO	NO
Need for translation or recognition of required documents	NO	NO	NO	NO	NO	NO	YES	NO	NO	NO
Need for physical encounter to complete the procedure	NO	NO	NO	NO	YES	NO	NO	NO	NO	NO

3. Obtaining financial aid for starting up as self-employed

Definition

Gaining access to financial subsidies when starting as a self-employed

Description of the procedure

Starting-up as a self-employed is a feasible opportunity for all individuals with a business idea and the intention to implement it. To this end, an individual has to address a number of steps including get allowances, register as a self-employed and address the appropriate procedures related with VAT declaration. Individuals with the intention to start as self-employed can benefit from the support of both national or local agencies providing technical support and nationally or regionally provided financial facilities (e.g. grant and loan at a subsidised rate) to support the self-employment initiative.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Geographical level *	REG	LOC	NAT	NAT	NAT	NAT	NAT	NAT	NAT	NAT
Type of provider **	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB

[*] - National/regional/local; [**] – Public / Private
[N/A] – Not applicable; [?] – Information Not Available

Online availability of the procedure and key characteristics

Information was not available about the service in object. The sole information available on the eGovernment benchmarking raw data concerns whether or not the service is available online. The information gap about this service will be filled by means of the information gathered through the interviews.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of the service	NO URL	NO URL	YES URL	YES URL	YES URL	NO[62]	YES URL	YES URL	NO[63]	YES URL

For both the cases of Belgium and Germany, the URL reported in the table refers to one single local authority situation, but the same was reported for the other localities analysed.

Online availability for non-national users

In the eGovernment raw data, JOB functionalities were not analysed in the cross-border case

[62] Website of reference for the functionality in object http://www.afsz.hu/engine.aspx?page=ak_tamogatasok&switch-content=ak_tam_tajekoztato&switch-zone=Zone1&switch-render-mode=full

[63] Website of reference for the functionality in object http://www.anofm.ro/acordarea-de-credite-avantajoase

4. Register for Unemployment Benefits

Definition

As soon as an individual become unemployed he/she must register as unemployed at an administrative office to receive unemployment benefits and eventually help in finding jobs

Description of the procedure

Unemployment benefits are granted to individuals that has recently become unemployed after a continuative period working under a certain employee and for reasons that are not related with his/her willingness or behaviour in the working environment. Unemployment benefits are intended to support the individual during the transition from a previous occupation to a new one. Typically, unemployment benefits are determined according to the time of employment and the previous salary of the individual in object, and are provided by national agencies.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Geographical level *	NAT	NAT	NAT	NAT	NAT	NAT	NAT	NAT	NAT	NAT
Type of provider **	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB	PUB

[*] - National/regional/local; [**] – Public / Private
[N/A] – Not applicable; [?] – Information Not Available

Online availability of the procedure and key characteristics

According to the information available, registration for unemployment benefit is available online in all countries taken into consideration but in Hungary and Romania. Authentication is requested either in the form of an ad hoc accreditation or via eID in the majority of the cases. Applicants are requested to submit documentation to complete the procedure, but this submission is not available online, therefore increasing effort in terms of time and costs associated with the completion of the procedure. Nevertheless, in the 40% of the cases, there are prefilled forms which indicate the effective reuse of previously submitted data, either within the same agency or in other connected ones.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of the service	YES URL	YES URL	YES URL	YES URL	YES URL	NO[64]	YES URL	YES URL	NO[65]	YES URL
Authentication request	YES	YES	YES	YES	YES	NO	YES	YES	YES	YES
Online authentication procedure availability	YES	YES	YES	YES	YES	NO	YES	YES	NO	YES
Availability of authentication via eID	YES	NO	YES	YES	YES	NO	YES	YES	NO	NO
Is any kind of documentation needed to complete the procedure?	YES	YES	YES	YES	NO	NO	YES	NO	YES	NO
Is it possible to submit required documentation online?	YES	NO	YES	YES	NO	NO	NO	NO	NO	NO
Are personal data pre-filled?	YES	NO	YES	YES	NO	NO	NO	YES	NO	NO

Online availability for non-national users

In the eGovernment raw data, JOB functionalities were not analysed in the cross-border case

[64] Website of reference for the functionality in object http://www.afsz.hu/engine.aspx?page=allaskeresoknek_munkanelkuli_ellatas_eu_egt

[65] Website of reference for the functionality in object http://www.anofm.ro/faq

5. Ensuring continuity of pension payments

Definition

Making sure to continue pension payments when becoming unemployed

Description of the procedure

Pension related functionalities are relevant for all people in their active age (15-64 years old) as concerns the security guarantee of economical sustainability for the period behind active age. Pensions are determined according to the earnings of active-life, the age-related accrual rate and are influenced by a life expectancy coefficient. All-along active life time, individuals are expected to keep accurate records on their earnings as well as benefits received for unsalaried periods, as to guarantee the accuracy of pension calculation. Along all this accumulation time, pensions can be managed by pension providers, by pension insurance companies, by industry-wide pension funds or by the company pension funds.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Geographical level *	AUTO	AUTO	AUTO	AUTO	NAT	?	AUTO	?	?	NAT
Type of provider **	PUB	PUB	PUB	PUB	PUB	?	PUB	?	?	PUB

[*] - National/regional/local; [**] – Public / Private
[AUTO] – Automated functionality; [?] – Information Not Available

Online availability of the procedure and key characteristics

Data reported in the following table suggests that for the majority of the country selected, this functionality is handled automatically by the referent authority, which means that there is no need for the user to process a request to ensure the continuity of pension payment. This approach might be intended to contain processing costs. On the other hand, in both cases in which this functionality is not handled automatically, there is a need for the user to submit document to complete the procedure, via channels other than the online upload, increasing the cost in terms of time and effort associated with this procedure.

	BE	DE	EE	ES	FI	HU	IT	NL	RO	UK
Online availability of the service	YES Automated [66]	YES Automated[64]	YES Automated[64]	YES Automated[64]	YES URL	?	YES Automated[64]	?	?	YES URL
Authentication request	YES	YES	YES	YES	YES	?	NO	?	?	NO
Online authentication procedure availability	YES	YES	YES	YES	YES	?	NO	?	?	NO
Availability of authentication via eID	YES	YES	YES	YES	NO	?	NO	?	?	NO
Is any kind of documentation needed to complete the procedure?	YES	YES	YES	YES	NO	?	NO	?	?	NO
Is it possible to submit required documentation online?	YES	YES	YES	YES	NO	?	NO	?	?	NO
Are personal data pre-filled?	YES	YES	YES	YES	YES	?	NO	?	?	NO

Online availability for non-national users

In the eGovernment raw data, JOB functionalities were not analysed in the cross-border case

[66] Service provided to the user without the user having to request it

Case study: Starting a business branch

1. Involved countries: The United Kingdom (holder) and The Netherlands (demander)

Brian is the unique shareholder and director of a successful limited liability SME in the UK that has been active in the national market since 2005. He would like to open a branch in Rotterdam, based on his positive trading experience with consumers in the Netherlands. To further develop his Dutch business, he would like to establish a branch office that would, at least for the next 3 years, employ only himself and a (local) secretary. Having developed a well-structured business plan, arranged financing and gathered information on administrative requirements, he is ready to kick start the venture by taking to following steps:

- Register with a business register[173] in the Netherlands;
- Find an appropriate location for his business, register the office of the branch and address all obligations related to work place security
- Register for VAT number assignment and understand and address all tax related obligations
- register an employee before first work day

In the Netherlands, foreign companies can establish a business branch that (unlike a *de-novo* local business) as an extension of the foreign company. Responsibility for its actions lies with the parent company.

Preliminary activities that Brain has to before the establishment of his business branch include:

- Check if the business is one of regulated professions in the Netherlands[174]. In this case he needs his professional competence and qualifications certified or has to obtain a European Professional Card (EPC), which has been providing a form of European OOP implementation for this functionality since January 2016[175];
- Choice of a locally unique branch name that complies with the *Handelsnaamwet* and its registration with the Chamber of Commerce[176] (*Kamer van Koophandel* or *KvK*) one week either side of the start of business[177]. The registration can be done online via the Message Box platform using a STORK level 4 e-signature or the Public Key Infrastructure (PKI). The KvK will pass the name along to the tax authorities (*Belastingdienst*).

Then such a branch should be registered at the local Chamber of Commerce with competences for the area in which it will be established. The Chamber of Commerce will provide the branch with a certificate of registration and a unique number of recording; only after this registration does the branch register with tax and social security authorities.

Documents to be submitted for branch registration at the Chamber of Commerce must be certified by a notary of the country of origin and followed by an authorised Dutch translation. The documents to be submitted are:

1- proof of existence of the foreign company – its certificate of registration, name and registered office address and names and details for the board of directors and secretary (or any form of management);
2- minutes of the meeting when the branch was established; and
3- branch name and address, name and powers of the appointed representatives and activities which will be performed by the branch.

- Documents concerning the establishment of the UK company were already submitted in the country of origin and are stored in the national UK business register. At the moment, there are no evidences that this information is directly retrieved from the business register in the Netherlands. This fact indicates that 1) the procedure includes the provision of information previously submitted to another PA (replication of information submission), and, by consequence, that 2) there is a concrete potential to reduce the administrative burden of this procedure by allowing the direct exchange of information between competent authorities.

For what concerns the remaining steps, the following applies:

- in terms of tax-related obligations, Brian needs to:
    - Register as an employer with the tax authorities, to obtain a payroll tax number for payroll tax returns;
    - Make required tax deductions for wage tax, (employee and employer) national insurance contributions and the employer's health insurance (*Zorgverzekeringswet*) contribution;
- In terms of registering employees before first work day, Brian probably will not have to file 'first day notifications,' which in the Netherlands it is only required for the first 3 years of operation from businesses that have been involved in fraud or have employed illegal workers;
- In terms of obligations related to work place security Brain should
    - Ensure that the chosen premises adhere to
        - the local zoning plan (*bestemmingsplan*)
        - environmental regulations; and
        - fire safety regulations
    - … or get a permit (*Omgevingsvergunning*) for all of these.

2. Involved countries: The Netherlands (demander) and the United Kingdom (holder)

Marc, the only shareholder and director of a successful limited liability company in the Netherlands, active in the national market since 2005, would like to open a branch in Nottingham, based on his positive trading experience with consumers in the UK. To further develop his business in the UK, he would like to establish a branch office that would, at least for the next 3 years, employ only himself and a (local) secretary. Having developed a well-structured business plan, arranged financing and gathered information on administrative requirements he is ready to kick start the venture by taking the following steps:

- Register with a business register[178] in the UK (also requiring the formal validation of signatures of representatives of the business and registering a name of the branch if different from the name of the company)
- Find an appropriate location where to set his business, register the office of the branch and address all obligations related to work place security
- Register for VAT number assignment and understand and address all tax related obligations
- (To register employees before first work day is not required in the UK for employers who have already registered as employers, but they must obtain and retain documentary proof of the worker's right to work and certify compliance to the Government).

Within one month after the establishment of the branch in UK, Marc's company has to register at the Companies House. The registration requires the submission of the following information:

- a completed 'Registration of an overseas company opening a UK establishment' application (form OS IN01),
- a certified copy of the company's constitutional documents (e.g. the statute); if the original is in a language other than English, a certified translation is needed;
- a copy of the company's latest set of accounts (if the original is in a language other than English, a certified translation is needed).

All information related to the establishment and data of the administration position of the parent company are obviously already available in the country of origin (typically within fiscal authorities or chambers of commerce) but need to be resubmitted again by the company in the UK. Additionally, the administrative burden of this procedure is increased by the need to submit certified translations of the above documents in case originals are not issued in English.

Besides costs associate with the certified translation of documents (if any), the direct monetary costs associated with this procedure consists of a £20 standard registration fee or a £100 fee if the registration is urgent.

This procedure applies only if the business branch is the first one of a certain company in the country, otherwise the company can fill in a form (OS IN01) that states that the documents have already been delivered for the establishment of another branch in the UK. This is an evidence of re-use of data, although it applies only to the information and data previously provided within national boundaries.

3. Indications of administrative burden

Comparative description – To start a business branch in the United Kingdom or the Netherlands, foreign applicants have to follow specific procedures that imply the submission of documents certifying the existence and financial position of the parent company. In both countries these documents must be submitted as certified copies together with certified translations of documents not issued in the language of the country of destination.

Indications of administrative burden - The need to provide certified copies of required documents is a source of significant administrative burden arising from duplication (i.e. information contained in the documents having already been submitted to the relevant authority in the parent company country) and from transaction (i.e. costs of having these certificates notarised in the country of origin and authoritatively translated). In addition, the UK imposes a £20 standard registration fee (£100 for urgent cases).

Main gaps and barriers - The main barrier associated with this branch registration procedure is semantic and legal - parent company certificates need to be notarised and officially translated to guarantee the reliability of the information provided. Many business representatives commented during the interviews that the language issues are common while interacting cross-border and that they typically expect to be able to use English for procedures and exchanges.

Non-monetary impacts - The procedure does not seem to generate particular non-monetary impacts. Leaving aside the costs of certification and translation, no other factors seem to impede or discourage applications by foreign businesses.

The experience of SMEs registering a company name in cross-border situations

Small and Medium Enterprises (SMEs) are most likely to be affected by administrative burdens due to their limited resources (also considering

professionals dedicated to administrative procedures). The online survey implemented under Task 1 provided insight into the experience of two SMEs in registering a company name in a country different from the one in which the business was legally based. One respondent pointed out that language barriers constituted a significant constraint, highlighting as main difficulties the understanding the procedure and the translation of forms not available in English. The other respondent, who requested the same service in another country, reported a particularly positive experience in the email exchange with the help service of the public administration of the destination country.

Concerning the re-use of data in this procedure, both respondents indicated that the provision of a standard means of identification for businesses as the VAT number did not permit the destination-country administration to retrieve any information previously provided in the country of origin. Nevertheless, the respondents did not agree on the opportunity to save money in case of not having to re-submit information and documents. This result might be explained by the fact that registration of *new* entities typically requires a minimal amount of information although already provided: this scenario can justify the perception of limited potential costs savings in not resubmitting information in another country.

Administrative burdens of business start-ups in other European countries

Interviews with businesses representatives from different countries revealed some interesting indications of administrative burdens associated with business start-ups. We asked business' representatives to briefly describe the procedure in place in their country required to establish a company and then to estimate how much time is needed to complete it. Due to the differences in the national procedures, these estimations refer to the overall time needed to accomplish all the mandatory steps requested in each country for the establishment of the legal entity. In particular, information provided on the time needed to complete these procedures makes an estimation based on Standard Cost Model (SCM) possible for Italy, Austria, Belgium and Germany. Being the basic SCM formula:

Administrative cost = Price x Quantity

= (Tariff x Time) x (Number of operations x Frequency)

The intent is to estimate the administrative burdens associated with business start-ups from the perspective of the company itself. To this purpose, we assume that: 1)

the frequency is 1 (i.e. once during the business life cycle); 2) the number of operations is 1 (i.e. the costs borne by a single business) allowing a comparison in terms of unit cost.

The following table reports the time required, the average national salary and the estimation of the procedure costs based on the application of the SCM.

	Italy	Austria	Belgium	Germany
Time taken for the procedure in hours (and wording days)	160 (20 wds)	About **2** (0,25 wds)	24 (3 wds)	120 (15 wds)
Average national salary*	€11.8	€12.69	€16.42	€14.9
SCM-based estimation	€1888	€25.38	€394.08	€1788

* Data refers to the year 2010 - SOURCE: EUROSTAT Structure of earnings survey: hourly earnings [earn_ses_hourly]

The table reported above indicates that administrative burdens suffered are highly variable across the considered countries. Part of this difference can be attributed to perception of respondents. Time taken ranges from hours needed to fill in and submit forms of a procedure completely on-line to days needed from the opening and to the closing of a more traditional procedure, including bureaucratic delays which were recurrently reported as a significant problem in many countries. Regarding the OOP, most of the business respondents confirmed that the proportion of information requested during the procedure that had already been submitted to PAs was very low (e.g. Germany 10% - 25%, Belgium less than 10%).

Case study: Requesting a licence for carriage of goods

1. Involved countries: Estonia (holder) and Finland (demander)

LILIA Ltd. is a road transport company based and operating in Estonia for delivery of commercial goods (non-food) since 2009. The company intends to expand its business in Finland and it should obtain appropriate licences for carriage of goods. To this purpose, the main steps are:

- To collect documents and information requested by the application procedure (including business specific details such as VAT number, evidence of TAX compliance, evidence concerning SOCIAL SECURITY OBLIGATIONS);
- To submit the application (eventually requiring in presence submission or validation of the company representative's signature).

Based on the information collected, road carriage of goods within the EEA area is regulated by Article 3 of Council Regulation No 881/92, which also requires a Community licence for transport operators. The Community licence covers all EEA member states (including Finland), so an established Estonian transport operator does not have to request a new transport licence from the Finnish authorities.

If the Estonian business does not have its own Community Licence, it can obtain one in Finland from the Finnish Centres for Economic Development, Transport and the Environment (ELY Centres) that requires:

- Evidence of good standing;
- Certification of vocational competence from the Finnish Transport Safety Agency,
- Proof of legal competence and financial soundness; and
- A completed licence application form (only available in Finnish)[179].

Typically, a licence application is processed in approximately 3–4 weeks.

What is needed to have already submitted in Estonia are evidence of good standing, and proof of legal competence and financial soundness.

The officials of public administrations interviewed in Finland commented during the interview that cross-border issuance and management of goods transport licences is of particular interest in light of the digitised fast-track procedures already implemented between Finland and Russia. This approach generated benefits in terms of facilitation of the procedure, fraud reduction and transport security improvement.

2. Involved countries: Finland (holder) and Estonia (demander)

Otelma Ltd. is a transport company based and operating in Finland that has been delivering commercial goods (non-food) since 2009. The company intends to expand its business in Estonia and it should obtain appropriate licences for carriage of goods. To this purpose, the main steps are:

- To collect documents and information requested by the application procedure (including business specific details such as VAT number, and evidence relating to tax compliance and social security obligations);

- To submit the application (eventually requiring in presence submission or validation of the company representative's signature).

As already indicated in the previous case, road carriage of goods within the EEA area (regulated by Article 3 of Council Regulation No 881/92) requires a Community licence for transport operators. The Community licence covers all EEA member states (including Estonia), so an established Finnish transport operator does not have to request a new transport licence from the Estonian authorities.

If the Finnish business does not have its own Community Licence, it can obtain one in Estonia from the Association of Estonian International Road Carriers (ERAA), which requires applicant to provide:

- A completed application (only available in Estonian);
- A document certifying appointment of a transport manager; and
- A document certifying the transport manager's professional competence.

The application for a Community licence can be submitted via digitally signed email.

What is needed to have already submitted to the Finnish public administration (provided the company has not previously applied for the Community Licence) are those certifying the appointment and professional competence of the transport manager.

3. Indications of administrative burden

Comparative description – Both countries analysed (Estonia and Finland) recognise the Community License issued by any EEA Member State. As consequence a foreign company willing to obtain a license in one of the two countries has to follow the same procedure of a national applicant company.

Indications of administrative burden – Typically, Finland processes a license application in 3-4 weeks; no time indications were available for Estonia. In Estonia requests can be submitted via email with digital signatures; the option is not available (according to the information retrieved) in Finland. Additionally, in Finland one of the required documents has to be obtained from a national agency different from the one to which submitting the procedure (i.e. the Finnish Transport Safety Agency providing the certification of vocational competences); this increases the burden associated to this procedure.

Main gaps and barriers – Language barriers are relevant in both cases; the application forms are provided only in the national official language (i.e. Estonian and Finnish).

Non-monetary impacts – The mutual recognition of a Community License minimises applications from non-national users and – in consequence – the need to retrieve information previously submitted to public administrations in the data demander country.

Case study: Bidding for Public Procurement in construction services

1. Involved countries: Hungary (holder) and Belgium (demander)

CART Ltd. is a Hungarian construction company with more than 15 years of experience in constructing public buildings at national level. The company is now interested in bidding for a public procurement contract in Belgium for constructing a new headquarter for the Brussels Police Force. In addition to the formal proposal submission requirements, the Terms of Reference specify that candidates must be compliant with all national security-related obligations. After considering costs, benefits and the odds of winning, CART Ltd. decided to submit a bid. To this end, they had to:

- Prepare the proposal and all documents requested in the Terms of Reference (including standard company information about registered office, legal representatives available in the national business register); and
- Register with social security office, register with compulsory healthcare and address all nationally requested obligations related to workplace security in order to demonstrate its compliance with national requirements.

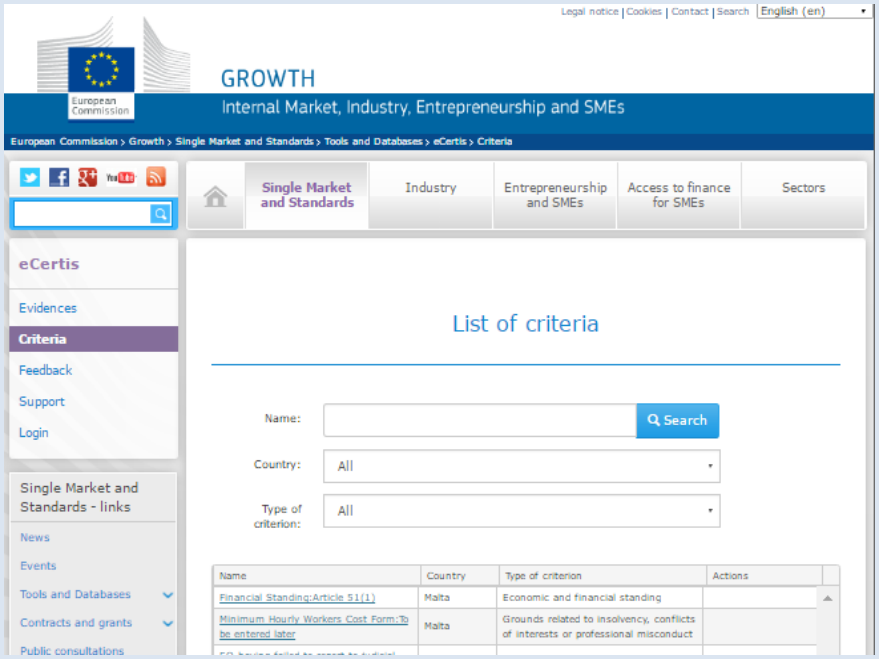
According to information gathered during the interview with officials of public administrations, in Belgium all federal Public Procurement procedures must be electronically published and allow online submission of bids. Concerning bids by non-domestic companies, identification and qualification were highlighted as a key issue for the public administration responsible for the procurement procedure. At present, this is tackled through a mandatory declaration of honour.

If than a foreign business is selected as winning tenderer for a certain public contract, information provided should be verified, either via direct links with existing systems of foreign public administrations (if available) or by asking the company to provide legally relevant evidence. Analogous checks in case of a Belgian winning tenderer are done by retrieving information using the company number.

- A valuable support in checking certificates issued by other Member States is provided by the e-Certis platform (further details in the box below).

The European Commission's services to issue the electronic European Single Procurement Document and e-Certis

E-Certis (http://ec.europa.eu/ecertis) was created to facilitate the identification of certificates requested in public procurement procedures. It supports both the buyers and tenderers in the identification of the documents submitted as evidence of fulfilment of exclusion and selection criteria in a given procedure. To fulfil this need e-Certis presents and allows comparison of the certificates issued as evidence in any Member State, while keeping them organised under common headings and matching equivalent documents across the different national datasets.



E-Certis is integrated with the service for issuing the electronic European Single Procurement Document (ESPD). It is a self-declaration of the financial status, abilities and suitability for a public procurement procedure of a company. The eESPD service, (https://ec.europa.eu/growth/espd) provided free of charge by the European Commission, allows buyers to prepare the template on the basis of which the tenderers will be evaluated, and the tenderers to fill it in. The eESPD service has been designed to help Member States comply with the new Public Procurement Directive. Funding has been provided to providers of e-tendering solutions to integrate the eESPD data model and facilitate automated filling-in of eESPD with data available in business registers.

ESPD and e-Certis provide an important contribution in the reduction of the administrative burden associated with public procurement procedures and play a crucial role in the transition to full e-procurement. They reduce administrative burden and increase access to cross-border tendering opportunities. The vision aims at ensuring the integration between the eESPD service, e-Certis service and the repositories storing the actual data, thus enabling implementation of once-only principle in e-procurement.

2. Involved countries: Hungary (holder) and Belgium (demander)

Metieu Ltd. is a Belgian construction company with more than 15 years of experience in constructing public buildings at national level. The company is now interested in participating in a public procurement procedure in Hungary. In addition to the formal proposal submission requirements, the Terms of Reference specify that candidates must be compliant with all national security-related obligations. After considering costs, benefits and the odds of winning, Metieu Ltd. decided to submit a bid. To this end, they had to:

- Prepare the proposal and all documents requested in the Terms of Reference (including standard company information about registered office, legal representatives available in the national business register); and
- Register with social security office, register with compulsory healthcare and address all nationally requested obligations related to workplace security in order to demonstrate its compliance with national requirements.

As the official of the Hungarian public administration stated, in Hungary every tender of at least €750,000 EUR is published on TED and open to companies from all Member States, in line with EC requirements. According to the Terms of Reference, specific documents may be required case by case, but basically tenderers have to submit court-certified documents, evidence of representative authorisation and relevant background evidence from the official business information sources (e.g. Chambers of Commerce). As noted by the interviewee, the bidder must collect and submit all these documents, including those already in the possession of national authorities and official business organisations. Additionally, foreign bidders must bear costs of court certification. The e-Certis system is not used to control the relevance of certificates from another Member State.

- Finally, according to the interviewee, Hungarian registered companies benefit some simplified procedures. For example, background checks performed by an office of the Ministry of Interior office recall the most recent balance sheets directly from the business register instead of requesting the Hungarian company itself. This direct system of verification is not available for companies registered outside the country.

eProcurement Directive and expected improvements in public procurement

Significant simplifications of the Public Procurement procedures have been introduced by the new PP directives. Some common aspects, already in the revised EC eProcurement arrangements[180], are now implemented. Digitisation of public procurement includes:

- Replacement of former requirements for all bidders to provide a range of documents showing that they met any exclusion and selection criteria with a single electronic self-declaration form (the European Single Procurement Document or ESPD[181]). Only the winning bidder will have to produce documentary proof (Note that the ESPD is related to the OOP via the Virtual Company Dossier[182] - VCD - service, which allows buyers to handle electronic ESPDs and bidders to have the forms filled automatically);
- The rollout of the eCERTIS mapping tool[183], which provides information on the type of documentary evidence requested for fulfilment of different eligibility criteria in public procurement procedures in the EU;
- The integration of ESPD and the eCERTIS service with existing systems and other measures to support transition to end-to-end eProcurement[184]
- The gradual adoption of the electronic invoicing started with the Directive

2014/55/EU[185] in April 2014. The European Committee for Standardisation (CEN) has been asked to develop a standard for such invoices by May 2017 and eInvoicing availability will be required of all Contracting Authorities by November 2019; by April 2016, all Contracting Authorities were obliged to ensure the electronic availability of tender opportunities and tender documents; by April 2017, Central Purchasing Bodies will have to implement electronic bid submission (e-Submission, including full electronic communication). e-Submission will be mandatory for all Contracting Authorities by the following year (October 2018); and

- the inclusion of the Once-Only Principle at the heart of the vision for an eProcurement ecosystem.

The overall timeline for these developments is summarised in the following Figure[186]:

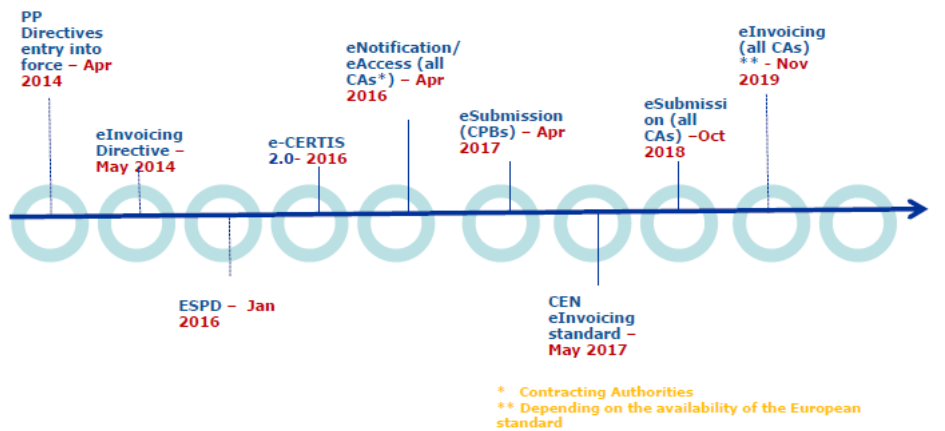


Figure: European-level eProcurement timetable

3. Indications of administrative burden

Comparative description – In Belgium all federal procurement must be electronically published and must allow for online submission of the bid. Similarly, in Hungary, according to the thresholds set by the European Commission, any procurement of a value superior to 750.000 EUR has to be published on the TED system and open to foreign applicants. In both countries, part of the required documents is strictly related to the type of the procurement, whereas those related to evidence on the (legal and financial) background of the bidder are common in all the procedures.

Indications of administrative burden - In the Hungarian case, the winning bidder has to bear all costs of court certification of required documents. The time and resources needed to complete this procedure vary according to the specificities of the tender procedure.

Main gaps and barriers – In both the cases the main barrier is caused by a combined organisational and technical issue and concerns an asymmetric treatment of national and cross-border winning bidders in completing background checks. In line with the new Public Procurement Directive (2014/24/EU), both officials of the public administrations in the two countries confirmed that self-certification is enough for the bidders and that only the winning bidder's information are checked. However, national winning bidders' information (especially for financial capacity and legal standing) is directly obtained from existing sources, while cross-border winners are required to provide documentary proofs. This asymmetry is attributed to lack of cross-border arrangements and organisational and technical solutions for exchange of information and data related to businesses among public administrations.

Non-monetary impacts - In the Belgian procedure, the main barrier reported during the interview with the officials of public administration concerns the identification and qualification of the bidder, which also has non-monetary impacts in terms of security improvements and fraud risk reduction (e.g. proving the authenticity of the proposing bidder). This issue is currently addressed through the inclusion of a mandatory Declaration of Honour among the documentation to be submitted.

Case study: Establishing a new association

1. Involved countries: Romania (holder) and Germany (demander)

ARMIC is a Romanian association, established in 2007, that has a long experience of cooperation with MESS, a dynamic German research foundation established in Berlin in 2001. In light of their shared experience and mutual interest, they decided to establish a new association (ARME) based in Germany, to pursue joint research. After designing the statute and the work plan for the first year of the activities of the association, they have to:

- Register the association and its statute by formally validate the signatures of their representatives; and
- Register the domicile of the association.

In Germany, associations are categorised as not-for-profit organisations recognised under the federal civil law. An association (*Verein*) can be registered or not, depending on its purposes and scope. Registered associations are formally

established by a notary deed that must contain the statute of the association approved by at least seven members.

The direct costs of the procedure are estimated at €105, comprising about €30 of notary fees and around €75 for entry in the *Vereinsregister*. To register an association, the following documents are needed:

- The statute (*Satzung*) approved by at least 7 members, which should describe the purposes and rules of the association;
- minutes of the first meeting of the association during which the statute was approved meeting (including names of all members present); and
- identity documents for all funding members.
- According to the information collected, identification documents of all funding members are the unique documents required and no further information previously submitted to national public administrations is needed.

2. Involved countries: Germany (holder) and Romania (demander)

KARG is a German, established in 2007, that has a long experience of cooperation with EMPIRIA, a Romanian research foundation founded in Bucharest in 2001. In light of their shared experience and mutual interest, they decided to establish a new association (KAEM), based in Romania, to pursue joint research. After designing the statute and the work plan for the first year of the activities of the association, they have to:

- Register the association and its statute by formally validating the signatures of their representatives; and
- Register the domicile of the association.

Under Romanian law, associations are categorised, together with foundations, as not-for profit organisations. Their registration involves two phases; a court decision to accept, refuse or request additional documents (to be completed within 3 days) and the administrative procedures to finally validate the new association.

In general terms, the documents needed to register an association under Romanian law include:

- proof of eligibility for the chosen name;
- IDs of the founder members;
- Proof of headquarters;
- Proof of the initial capital
- a criminal records check for founder members or fiscal certificates for legal persons; and

- statutes of the association and a draft of specific regulations.

According to these indications, a German representative wishing to become a founder member of a new Romanian association would have to supply his/her ID and Certificate of Good Conduct (following a check for a possible criminal record); the latter in particular reflects information already in the possession of German public administrations.

3. Indications of administrative burden

Comparative description – In both countries considered (Germany and Romania), associations are categorised as non-for profit organisations.

Indications of administrative burden – The majority of documents and information to be submitted were not previously provided to any public administration as they refer to a new organisation (i.e. association). The unique information that might have been previously submitted to other public administrations concerns the identification of the funding members. In Romania, registration of a new association requires both a court decision and an administrative procedure. These mandatory steps increase the burden associated with this procedure.

Main gaps and barriers – Language barriers constitute the principal issue; all documents need to be submitted in the national language of the destination country.

Non-monetary impacts – In both cases, applicants should obtain approval for the articles of the statute of the association with possible time delays for the kick-starting of the association.

Case study: Enrolling in a Master course

1. Involved countries: Germany (holder) and Italy (demander)

Julia is a German student who, after completing her bachelor's degree in Germany and spending one year in volunteer work, decided to apply for a Master in Italy in the field of International Relations. After selecting an interesting course at the University La Sapienza in Rome, she got information on the website about university fees and costs of living in Italy. To realise her plans, she has to:

- complete the procedures needed to apply for a place and, with luck, enrol in the selected higher education course (providing the documentation needed for recognition of her German Bachelor's Degree); and
- apply for a student grant (as grants are subordinated in Italy to unemployed status she will also have to register for unemployment benefits).

Although some extra documents might be requested by specific universities, in general, a foreign student seeking admission to and enrolment in an Italian University is requested to submit:

- a certified photocopy of the undergraduate University-level qualification;
- a document called "*Dichiarazione di valore in loco*", providing indication on previous academic qualifications; this document is issued by the competent Italian diplomatic authority and contains information related to the validity of the qualification and the type of issuing institution;
- Transcripts of records issued by the competent academic authority; and
- Subjects of courses already taken and related acquired credits.

All this information is already available directly from the issuing institution (which may not be public) but it may not have been previously submitted to any (other) public administration. Nevertheless, the amount of documentation and certifications requires a consistent administrative burden.

- To apply for student grants, the procedure differs on the type of grant and by the issuing organisation.

2. Involved countries: Italy (holder) and Germany (demander)

Pietro is an Italian student who, after completing his first degree in Italy and spending one year in volunteer work, decided to apply for a Master in Economics in a German University. After selecting an interesting course at the University of Berlin, he got information on the website about application procedures, university fees and costs of living in Germany. To realise his plans, he has to:

- Complete procedures needed to apply for a place and, enrol in the selected higher education course (providing documentation needed for recognition of his Italian Bachelor's Degree); and
- apply for a student grant.

Although some extra documents might be requested by each university, in general, a foreign student seeking admission to and enrolment in a German university has to submit:

- an officially certified copy of his prior education qualification in the original language;
- a certified translation of the transcript of subjects and marks;
- an officially certified copy of any secondary education qualifications with an overview of the subjects and grades;
- a copy of the passport; and

- proof of language proficiency in the form of an officially certified copy or an online verification code.

Most of these documents are already in the possession of the national education institute where previous titles were recognised or of the national public administration (e.g. the Ministry entitled for education and training).

- To apply for student grants, the procedure differs on the type of grant and by the issuing organisation.

3. Indications of administrative burden

Comparative description – In both cases analysed (Germany and Italy), the procedure requires a number of certified translations of documents from different agencies and public administrations. In both countries, candidates are required to provide evidence of previous academic qualifications, transcripts of records and details of the nature and content of the courses.

Indications of administrative burden – Additional elements that increase the burdens of this procedure are: in Germany, the need to provide proof of language proficiency; and in Italy, the need to obtain one of the certifications (namely the "*Dichiarazione di valore in loco*" specifying the details of the academic degree obtained in the country of origin) directly from the Italian diplomatic authority. All evidence required for this procedure is already available directly from universities where students obtained the degree, but the entire burden and cost of providing this evidence falls on the applicant student.

Main gaps and barriers – Language barriers are the main issue; all documents need to be submitted in the form of certified copies or certified translations, at the applicant's expense.

Non-monetary impacts – the procedure is evidently highly burdensome (in terms of time and cost) and is therefore likely to affect smoothness of cross-border student mobility. It is also possible that the lack of standardisation may lead to asymmetric treatments of national and foreign students. No indications of the extent of these impacts are available.

The experience of students enrolling in higher education

Among the functionalities selected for this study, enrolling in higher education institution in European country different from the country of origin is one of the most exploited functionalities. According to the answers collected in the OOP

Survey (conducted under Task 1 of this study), the majority of respondents who provided answers on the procedural aspects for enrolling in a higher education institution abroad reported the benefits of a remote-mode interaction (via websites and/or emails). In a case of a student enrolling in a higher education institution in Belgium who had had previous interactions with the Belgian public administrations authorities, some information could have been retrieved using the applicant identification number. Nevertheless, for the majority of respondents, neither information retrieval nor pre-filled forms were available.

The respondents to the OOP Survey confirmed that the main burden associated with this procedure is the need to submit certified translations of previous qualifications and familiarisation with the whole procedure (although information was available on websites in languages other than that of the destination country). Additionally, in the majority of cases, part of the procedure or the final submission needed to be completed in presence.

The majority of respondents to the OOP Survey indicated that not having to submit documents and information in possession of their universities would have allowed them to save between 1 and 4 hours; applicants to German universities estimated potential savings from 1 to 5 days (probably due to the need to provide certified documents as described in use case).

Estimating the administrative burden of enrolling in higher education in Italy

According to indications collected from a respondent to the interviews with experience related to enrolling procedures in the Italian universities, the entire procedure can take between 5 and 15 days depending on the country of origin of the applicant. Some of the requested documents and certifications must be retrieved from authorities and/or institutions in the country of origin of the applicant, making the time to completion of the procedure highly variable. Nevertheless, among European countries the "Diploma supplement" (released in the language of the country of the institution and in English), is commonly recognised and facilitates the enrolment procedure.

In light of these considerations, the average time required for the enrolment procedure can be used for estimating the administrative burden of enrolling in higher education. The issue of the applicable average tariff, although students are not included in the population for which average salary is estimated (because usually they are not employed), is solved by using as proxy the national average hourly earnings (as if it was performed by an active worker). Being the objective of this exercise an estimation of the administrative burden, it can be considered acceptable as the one-off nature of procedure (i.e. number of operations and yearly frequency of this procedure both set to 1). Based on these assumptions:

Administrative costs = (Tariff x Time)

Italy: 8 hours/day x 10 days x €11.41 /hour = €912.8

Spain: 8 hours/day x 10 days x €11.8 /hour = €944

[Tariff data refers to the year 2010 - SOURCE: EUROSTAT Structure of earnings survey: hourly earnings [earn_ses_hourly]

The PLOTEUS portal on learning opportunities in the European space

The PLOTEUS Portal (https://ec.europa.eu/ploteus/en) is a tool provided by the European Commission to support the mobility of students within Europe by facilitating access to information on learning opportunities. It includes information on higher education institutions, on vocational courses, on training opportunities at local and international level and on European and national qualification frameworks. Specific information is provided (in all Member State languages) on exchange programs, grant opportunities, recognition of diplomas and qualifications

and practical information for relocating in Europe.

By helping applicants to better understand the procedural steps and authorities with which they have to deal to enrol in higher education institutions throughout Europe, this tool contributes to reduce the administrative burden generated by the complexity of these procedures and by the obstacles to gather the relevant information.

Case study: Starting up as self-employed

1. Involved countries: Spain (holder) and the United Kingdom (demander)

Carlos is a Spanish man with 10 years of professional experience in the field of accommodation and leisure for a multinational company. He decided, for personal reasons, to move in the UK to become a self-employed consultant for SMEs in the same business field. He collected information on the benefits available to self-employed people in the UK. To kick-off his initiative he will have to:

- Complete the procedures for obtaining financial aid for starting up as self-employed; and
- Ensure the continuity of pension payments to guarantee that both the working periods (the previous in Spain and the upcoming in the UK) will be appropriately accounted for the determination of his pension.

The procedure to become a self-employed person in UK (also referred to as a "sole trader") requires the applicant to register as individual with HM Revenue and Customs (HMRC). To this end the following cases are envisaged:

- A new sole trader who's not filed tax returns before will need to register a new business (the procedure is fully available online but additional details are available only under login), and enrol for Self-Assessment tax returns and Class 2 (and maybe Class 4) National Insurance;
- A new sole trader who's previously filed tax returns and has a government tax account will only need to register for Class 2 National Insurance and complete the module "Register if you're a self-employed sole trader (CWF1)" available as an online procedure; and
- A former sole trader wishing to start up again only needs to complete CWF1.

Registration is reported to take about 10 days for completion and validation. No specific indications are available concerning the procedure for non-nationals. It most probably will fall under the category of "new sole trader".

It does not automatically follow that national insurance contributions in all countries where the person has worked are aggregated to determine the length or amount of qualifying contribution, as the UK pension combines elements of defined-benefit and defined-contribution plans. There is a complex calculation intended to ensure that the individual is not disadvantaged by having contributed in more than one country and that contributions are not lost. This does introduce an asymmetry between those with and without contributions in other countries, but not in terms of individuals. These contributions provide access to a range of benefits, including: Incapacity Benefit; contributory Employment and Support Allowance; Bereavement Benefits; State Retirement Pension; and Maternity Allowance, but not contribution-based Jobseeker's Allowance. This benefit depends on the individual's previous Class 1 (employee) contribution history. Under certain conditions[187], self-employed individuals on low incomes may also quality for working tax credit.

2. Involved countries: the United Kingdom (holder) and Spain (demander)

Richard is a British man with 10 years of professional experience in the field of accommodation and leisure for a multinational company. He has decided for personal reasons to move in Spain to become a self-employed consultant for SMEs in the same field. He collected information on the benefits available to self-employed people in Spain. To kick-off his initiative he will have to:

- Complete the procedures for obtaining financial aid for starting up as self-employed; and
- Ensure the continuity of pension payments to guarantee that both the working periods (the previous in the UK and the upcoming in Spain) will be appropriately accounted for the determination of his pension.

According to interview information provided by the official of the public administration, a Business Person (BP) has the opportunity to retrieve all information on the requirements for setting up in Spain on the PSC website (www.eugo.es). According to information available there, a foreigner seeking to register as self-employed in Spain would have to apply for an Identity Number allocation of Foreigners (NIE). The competent authority for this procedure is the Ministry of Interior and the procedure is managed by the Directorate General of Police. The applicant has to provide:

- proof that he/she is not in Spain in an irregular immigrant;
- explicit reasons for the request; and
- identity document.

The application process takes about 5 days to be finally validated but the application can only be submitted in person. None of the required documents are likely to be in the possession of another public administration. Specific information on grants and incentives can be retrieved from the same website (link to the search tool) but procedures might vary according to the type of support requested and the issuing authority.

3. Indications of administrative burden

Comparative description – In both countries analysed (Spain and the UK) all relevant information concerning this procedure is easily accessible online through the government gateway or national Points of Single Contact. None of the information required to complete the procedure is likely to have been previously submitted to other public administrations. The UK makes a simplified procedure available for former self-employed individuals (within national framework) who want to start up again: they do not need to register again for self-assessment tax returns or national insurance.

Indications of administrative burden – According to available information, in the UK the completion of this procedure – including validation – takes up to 10 days. According to the indication provided by a business representative operating in Spain, this procedure typically takes between 7 to 10 days –exceeding the 5 days reported on the official website. Additionally, the applicant will have to complete part of the procedure with third parties (e.g. notary, bank) and in presence, increasing the associated administrative burden.

Main gaps and barriers – An organisational barrier emerged in Spain; the documentation can only be submitted in person at the competent authority.

Non-monetary impacts – Before accessing this procedure in Spain a foreign applicant needs to apply for an Identity Number for Foreigners (NIE).

Estimation of the administrative burden of registering as self-employed in Spain

According to the indications provided by business representative operating in Spain, the procedure to register as self-employed could take between 7 and 10 days; as the official indications suggest that the procedure should take up to 5 days. For our assessment we consider an average time of 7 days. Using data from EUROSTAT (*Median hourly earnings, all employees (excluding apprentices) by sex [earn_ses_pub2s]*) Spanish median hourly earnings are €9.41 (in 2010, the latest data available) and €12.62 EUR for the UK. A tentative estimation of the administrative burden associated with this procedure using the Standard Cost Model approach is based on:

Administrative costs = Price x Quantity

= (Tariff x Time) x (Number of operations x Frequency)

Basic assumptions are: 1 operation (corresponding to a single applicant) and 1 request for registration per year). On the basis of these assumptions:

Administrative costs = (Tariff x Time)

Spain: 8 hours/day x 7 days x €9.41/ hour = €526.96

The UK: 8 hours/day x 7 days x €12.62 / hour = €706.72

C. Summary of evidence from use cases

In order to enrich the baseline scenario of the current OOP implementation, factors affecting the administrative burden of individuals and businesses identified in the analysis of the use cases are summarised in the following table.

Table 14: Factors affecting administrative burden

Use Case	Administrative burden increasing factors	Administrative burden **reducing** factors
A. Starting a business branch	• Provisions of certified copies of documents issued by another country (including notary costs) • Submission of certified translations of documents (including certified translation costs) • Submission of information previously provided (more than 50%)	• Availability of the online procedure (including better efficiency in terms of time and money)
B. Requesting the license for the carriage of goods	• Necessity to obtain certificates from multiple agencies • Submission of information previously submitted (less than 50%) • Application form available only in the national language	• Possibility to submit the application via email in digitally signed forms • Existence of a European Community Licence
C. Bidding for public procurement in construction services	• Provision of certified copies of documents issued by another country • Submission of information previously provided (about 50% *depending on each procedure*) • (*if the applicant is selected*) Provision of additional documents for background checks	• Possibility to submit the application online
D. Establishing a new association	• Necessity to deal with multiple agencies to complete the procedure • Submission of all documents in the national language	
E. Enrolling in a Master's course	• Necessity to obtain certificates from multiple agencies • Submission of information previously provided (about 100%) • Submission of certified translations of documents (including certified translation costs) • Necessity to prove language proficiency	• Possibility to have an online self-assessment test and use the related code to complete the procedure

Use Case	Administrative burden increasing factors	Administrative burden **reducing** factors
F. Starting up as self-employed	• Necessity to complete some tasks mandatorily in presence • Submission of the application mandatorily in presence • Submission of information previously provided (less than 50%)	• Procedure partially available online

The analysis of use cases suggest that administrative burden is increased by:

- On average, re-submission of more than 50% of the information and data already provided to a public administration/institution in another country;
- Submission of certified copies or certified translations of the documents;
- Necessity to deal with multiple agencies/administrations.

Administrative burden is decreased by full or partial availability of the online procedure.

Annex IV. Stakeholder Perspectives

This section documents perspectives and insights on OOP implementation based on interviews with selected national representatives and analysis of business and individual attitudes based on desk research and fifteen online surveys.

A. OOP from the perspective of national representatives

Public administrations can be regarded both as implementers of OOP-related initiatives and as potential direct beneficiaries of the cost savings and efficiency improvements that can be generated from OOP implementation. The following paragraphs provide an overview of the indications on OOP implementation as reported during semi-structured interviews with officials of public administration in the sample of the ten selected countries.

1. Relevant national legislation and policy initiatives for OOP implementation

In the sample of the ten selected countries, implementation of OOP is significantly heterogeneous in method, maturity level, legal relevance and focus.

For example, Estonia, Netherlands and Belgium have national legislation in place that not only refers explicitly to the Once-Only Principle but also enforces its implementation. The fundamental reference for OOP implementation in the Estonian legislative framework is art. 43 of the Public Information Act[188], which states "*(2) Establishment of separate databases for the collection of the same data is prohibited*". The effect of this prescription is to encourage public administrations to retrieve data from the registers in which they are already stored instead of duplicating data requests and their storage. This still allows authorities to request information that they already possess (e.g. for confirmation), but the Economic Activities Code Act[189] clarifies the situation in its "Prohibition on requiring information twice" stating that "*(1) It is prohibited for economic administrative authorities to require from undertakings [...] information which is entered in a database established pursuant to law, except for information which allows the identification of an undertaking and contact details of an undertaking*". Although this provision is specifically addressed to economic administrative authorities, it explicitly refers to the OOP implementation in this domain. The Netherlands formulated requirements for all legislation relating to base registries, which include the obligation to use data from those base registries for specific government services. Specific legislation for all 12 base registries is in place now, including a Base Registry for Persons. Belgium implemented the OOP for federal services in 2014 by means of the Loi 5 Mai 2014[190]. This law requires federal public

administrations to use the identification number of each user and to retrieve data available on official registers. Although the full take-up of this provision has yet to be completed, the law itself constitutes a vital starting point for the implementation of the principle at federal level and is driving its implementation at regional and local level.

Code of Digital Administration (CDA - legislative decree 82/2005) regulate in Italy the re-use of existing computer software within Italian public administration and digital exchange of documents. Article 58 of CDA specifies that data access and use should be regulated by ad-hoc framework agreements among PA in line with the AgID guidelines (*Linee guida per la stesura di convenzioni per la fruibilità di dati delle pubbliche amministrazioni - versione 2.0*) after having feedback by the Italian Authority for the protection of personal data.

Other countries recognise OOP as something that needs to be developed in the near future (e.g. Hungary recognises it as a key objective in a National Green paper) or are tentatively exploring its implementation through direct exchange of information and data among certain public administrations (as in the Romanian case). The same is true of the UK, where initial and limited pilots in highly specific domains (such as the Tell Us Once service for reporting deaths) are giving way to more general initiatives, such as the "Regulatory Futures" initiative that are closely tied to obligations in the Small Business Enterprise and Employment Act 2015 (SBEE)[191].

Finally, the case of Finland provides a clear example of how legal provisions can limit the OOP implementation. Although extensive use has been made at national level of base registries, a typical principle embedded in all regulations concerned with data and information collection is the Fair Information Processing Principle of *purpose limitation* that implies that "*data collected within a public procedure can only be used for the purposes for which they were collected"*. As a result, vast amounts of data in the possession of public administrations cannot be reused for different purposes[192]. To fully implement the OOP and consequently to exploit data and information already available to public administrations, important modifications in the national legal framework should be done[193].

In Spain, the administrative legal framework, configured mainly by law 39/2015 regulating mainly interaction with individuals and by law 40/2015 of October 1st, regulating mainly interaction between public administrations recognises the right of individuals not to deliver data and documents already in the hands of public administrations. Additional provisions put this into practice by means of: the exchange of information through the administrative networks and the use of the data intermediation platform and other services. This legal framework establishes

that there is an implicit consent by the individual unless an explicit opposition is stated. The re-use of Public Sector Information is regulated by Law 37/2007, of November 16, and by the Royal Decree 1495/2011, of October 24 (which transposes the Directive 2003/98/CE to the national legal code) specifying therein the basic principles regarding reuse matters, together with an Interoperability Agreement. This framework excludes explicitly the exchange of data and documents between public administrations for administrative purposes.

2. Importance of demand for cross-border services as a driver for OOP implementation

The cross-border service demand is a significant driver for implementation of data exchange and procedural simplification for foreign individuals and businesses.

In 2013 in Belgium more than 200,000 foreigners, mostly from other Member States, registered in the country. This tendency matches both the general trend to increasing flows of workers across European borders and the specific role of Brussels as institutional centre which attracts both individuals and businesses. In other countries (e.g. Estonia, Finland), cross-border demand for public services is focused on mobility flows from neighbouring countries. In Finland the main flows of individuals and businesses originated in other Nordic countries (such as Sweden and Estonia) while for Estonia the principal inflows of business and outflows of individuals involve Finland (motivating the consolidated collaboration between the two countries).

Hungary has limited inflows of foreigners and consequent limited demand for cross-border services and the implementation of systems to facilitate access to non-nationals (but intra-EU)' access to public administration services is guided by the need to comply with European regulations and initiatives.

The Netherlands pointed out that necessary investments have been and will be made for development of EU-wide services. Where not necessary or economical, implementation is given low priority – at least until national OOP implementation has occurred across all Member States. The Dutch authorities are also involved in multiple Large Scale Pilots as the exchange of experience is seen as useful and important.

The UK has experienced large and targeted inflows of workers in the wake of accession, primarily as a result of its early implementation of freedom of movement for individuals of the Accession countries, compared to the overwhelming majority of 'old' Member States. However, the arrival of large numbers of e.g. Polish workers did not trigger a move towards cross-border OOP implementation in part as a result of fundamental incompatibilities in data availability, coverage, format and quality.

As noted, domestic implementation remains fragmented, though this is set to change and the primary drivers for cross-border OOP implementation are highly sector-specific, being associated with e.g. financial services and taxation on the business side and with criminal records and citizenship status on the personal side.

Other countries, such as Spain and Italy, experience large flows of (regular and irregular) extra-EU migrants and manage the supply of services with different approaches not having (or not directly using) detailed information on the demand of public services of foreign individuals. Spain offer public services to foreign individuals by providing them an identification fiscal number (allowing distinction with Spanish individuals). Such code allows foreign individuals to have their "Spanish" identity and benefits deriving from that (e.g. social security). Businesses of other EU MS have to follow general rules already established at the European level.

3. Best practices for the implementation of re-use and exchange of data among public administrations

Identified initiatives for data re-use and exchange among public administrations, in particular in cross-border situations, have a clear focus on frequently used services and on facilitating interactions with countries having relevant mobility flows.

A selection of significant initiatives for re-use and exchange of data among public administrations mentioned during the interviews with officials of public administration follows.

- The Estonian national system for data and information exchange among public administrations is based on the X-Road infrastructure, which was also recently implemented in Finland and is expected to allow (in the near future) exchange of data and information between the two countries on tax payers. The X-Road infrastructure is a secure exchange system based on Internet protocol, which works with eID numbers and with a metadata model that makes possible to understand in which of the various connected registers data are stored. The solution adopted by Estonia is not to create a single data repository to collect all data and information already stored in local or sectoral registers, but rather to create an effective and secure system to connect distributed data repositories (provided they meet certain interoperability and security standards).
- In Finland the exchange of data and information with other Nordic Countries is done through the Population Register Centre's Nordic Moving service (developed over many years), which allows automated exchange of data and information in particular on pensions in Nordic countries.
- With the implementation of legislation on base registries and a government-wide reference architecture, Once-Only is becoming more and more apparent

in the Netherlands, supported by services such as a Catalogue, a "Service Bus" for electronic provision of feedback.

- In Spain the General Access Point facilitates the communication of individuals and businesses with Public Administrations. It allows access to government information, it gives the possibility of doing paperwork and it permits to know at any time the state of processing of cases (in accordance with Law 11/2007, Art. 8 and RD 1671/2009). Additionally, in Spain, the eGovernment portal, PAe (administracionelectronica.gob.es), is the Public Administration channel that unifies and centralises all available information about eGovernment in the country. It serves as a gateway for all information on the status, development, analysis, news and initiatives around eGovernment. The Point of Single Contact (www.eugo.es portal is part of EUGO network) is targeted at Professionals and Service Providers in general (business owners and entrepreneurs) of EU Member States that wish to carry out their business activity in Spain. It is also aimed at the consumers (or recipients) of these business activities, providing them with information about existing professional and consumer associations and about how to make a complaint. It also informs them regarding the Competent Authorities that issue authorisations, are responsible for registers, etc., under the terms established by Law 17/2009 of November 23 on the free access to and exercise of service activities.
- The advantages of an approach focused on a unique authentication access for users as a preliminary step to achieve OOP are the key argument in Italy. SPID (http://www.spid.gov.it/) is the public system for the creation of a unique digital identity to access public and private services in Italy. It represents a unique access point (by authentication) for users to national services. OOP at national and at European level requires an identity of individuals recognised at the European level.
- In Belgium a forthcoming initiative (launched by the CIEC, *Commité International Etat Civil*) is a platform for exchanges of birth certificates with France, Luxembourg and Turkey.

4. Expected benefits and perceived obstacles of OOP implementation

According to indications of officials of public administrations, efficiency improvement and security aspects are the benefits most frequently associated with the OOP, whereas the most significant obstacles are the heterogeneity of administrative approaches, legal and semantic issues, lack of trust among public administrations and political resistance.

In details respondents identified among the most significant obstacles the existence of different national eID systems which make communication among different national systems very difficult, the lack of good quality metadata, the "normalisation" of data across registries (for example "address" of the house where a person lives in the Netherlands is only be one single (primary) address while in the Belgian registers this could be multiple addresses. National and sub-national legal

frameworks, language issues, organisational problems (such us lack of common procedures), lack of a European Digital identity and absence of common semantic standards were indicated as the main limitations for the EU-wide OOP implementation.

In the UK approach (as in the Spanish one) the primary focus is not on direct benefits for public administrations but on the users. Data centre rationalisation for reasons of cost and security had long ago laid the groundwork for OOP implementation, but recent progress has been supplemented by a desire to "bri*n*g the service to the customer" – in other words, more efficiently to serve business and individual needs and to reduce burdens specifically falling on them (to complement the earlier emphasis on reducing burdens falling on government). One manifestation of this has been the early implementation of OOP-like services such as Tell Us Once (which automatically notifies a very wide range of public and private entities following registration of a death - recently extended to births - precisely because it was recognised that the procedures required would be particularly burdensome at the time they were needed. It was only later discovered how large the savings to government were. Further aspects of this include the deployment of the "Find-It" tool to locate data among the vast array of loosely interconnected public authority databases and the implementation several years ago of a "Government Gateway" providing both service access and access to and control of stored data, which can be (re)used by individuals and authorities alike (given consent). The chief impediments are differences in administrative procedures and service procurement of the necessary technology, coupled with adverse perceptions based on longstanding difficulties with e.g. reusable health data.

The main benefits were associated with the potential reduction of cost for management of data and information for public administrations involved in the exchange, with more efficient service provision to individuals and businesses concerning taxes, and – in the long run – significant time and cost savings for all stakeholders. Some respondents focused the attention on the fact that the most significant benefits are reduction of administrative burden for services associated with higher transaction volumes such as those related to pensions, health and education.

5. Indications for OOP implementation at European level

Main indications from interviewed officials of public administrations in the selected countries concerning OOP implementation at European level are:

- OOP implementation deserves to be combined with the simplification of the entire procedure of data collection, retention and use to maximise potential

benefits for both individuals and businesses and public administrations themselves;

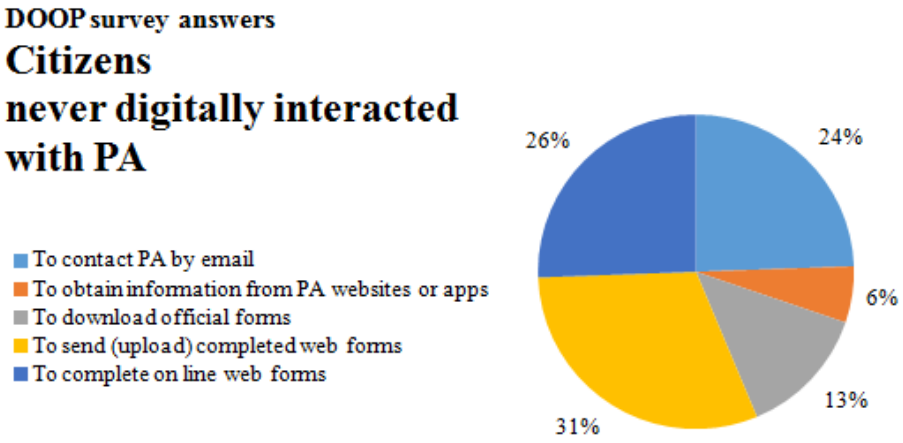
- Implementation of the OOP requires to start by addressing simple and baseline issues (such as the realisation of mutually recognised identification means - eID) and then to proceed by exploiting and re-using what already exists rather than creating *de novo* additional components;
- priority should be given to most used services, and/or those offering the direct, immediate, visible, trust-enhancing and/or valuable benefits (not limited to cost saving and administrative burden reduction) to individuals and businesses and public administrations;
- The quantification of benefits and burden reduction can be reinforced by explicit linkage to "Better Regulation" burden reduction targets[194];
- Actions for improving trust among public administrations are needed in order to increase exchange data as well as to reach agreements on language issues (e.g. determining that data provided in another language will be recognised);
- Semantic interoperability should be achieved together with a harmonisation of baseline requirements (in terms of information/data/documents) to obtain a public service cross-border;
- Along with legal harmonisation and management of data protection and privacy issues, it is important to proceed with implementation of pilots to allow governments and users alike to familiarise themselves with the new approach and to obtain direct experience of its potential benefits;
- Legal limitations in several countries that constrain sharing of data in ways that prevent trans-border OOP need to be reassessed to test whether they are still justified. Supportive legal and evaluative frameworks are therefore seen as necessary; and
- A key challenge to be addressed is to find ways of giving users with effective and proportional control over the data and information they provide to public administrations along with meaningful consent mechanisms. This is a microcosm of the more difficult issue of data ownership in general, but may be easier to address and may contribute to progress on the overall issue. Progress here can also improve transparency and trust towards public administrations and public services, and in the process improve the coverage, quality and utility of data provided.

B. OOP from the business and individual perspective

1. The individuals' perspective

Among the respondents of the OOP Survey, 48% declared to be individuals currently living in country which is different from their country of origin. Responding individuals are characterised by some experience with eGovernment services. Only a minor part (6%) has never used PA websites or apps in the last 12 months to interact with Public Administration. Individuals in the sample are also

used to download forms (i.e. percentage of individuals that has never done in the last 12 months is 13%). Taking into account all the proposed ways of interaction for eGovernment about half of individuals confirmed that they have been used *At least once, but not every month* in the last year.

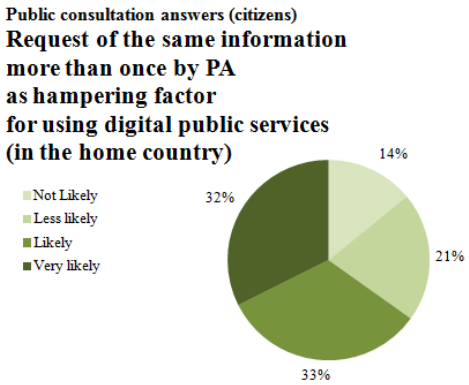


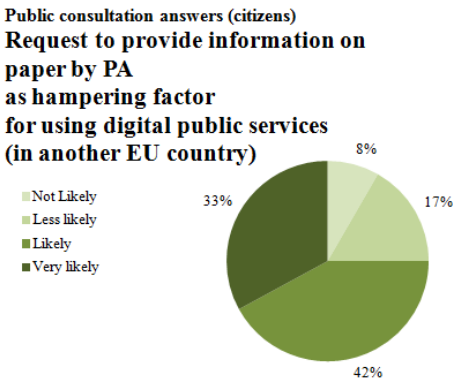
70% of the respondents were individuals that **completed at least one on line web forms** in the last year. 80% of those respondents used them to obtain from 2 to 5 different public services and almost 60% never found pre-filled fields with required personal data.

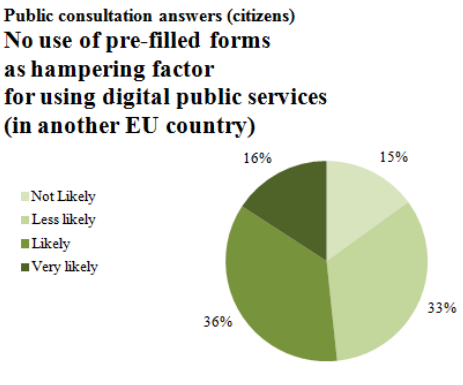
42% of the individuals responding to the OOP survey were asked to provide the **same information/documents already provided** to another public agencies/authorities or officials in the last 12 months, and were asked to share information/documents already provided to another public agency/authority **for a different purpose** (44%).

65% of responding individuals to the Public consultation indicate that the same information is requested more than once by the national PA.

75% of responding individuals to the Public Consultation indicate that the requests for paper submissions of information are a hampering factor for usage of digital public services in another EU country. 52% considers the absence of pre-filled forms as a *likely* or *very likely* factor hampering the usage of the digital public services.







Expectations of individuals in requesting public services cross-border are strictly related to the OOP application. 39.6% of those answering to the Public consultation *would be able to have electronic access to the personal data already provided in the home country* and 48.3% *would be able to access personal data in foreign country and control any further use to which it might be put.* Additionally, 19% of the individuals had had to resubmit to the host country information/documents/data already submitted in the home country.

In the OOP survey, responding individuals were asked for their perception on the expected time and money savings in case of not needing to resubmit information/documents to the host country that were already submitted in the country of origin, and in case of online management of the entire procedure. In general, **re-submission of information/documents** for obtaining services in another EU country has been largely recognised as an activity generating waste of time and loss of money by individuals answering to the OOP Survey:

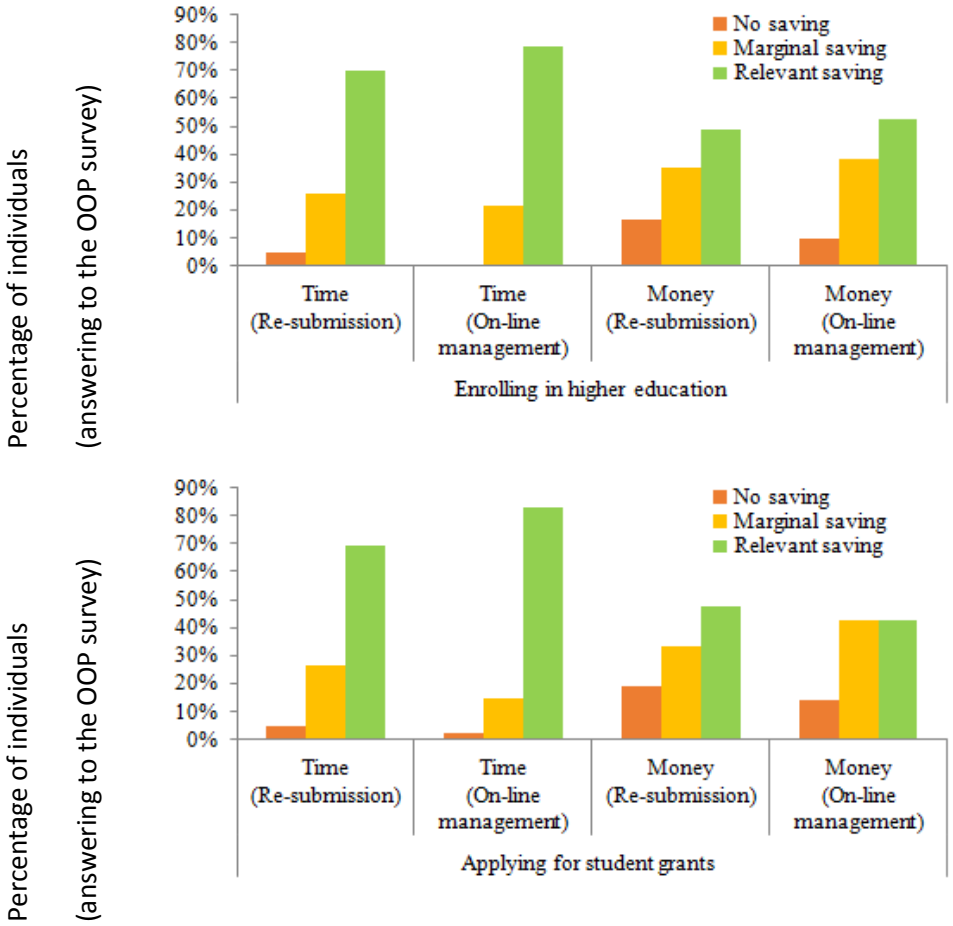
- ***significant savings of time*** were expected by 69% to 79% of respondents (depending on the specific functionality) if not required to re-submit information and documents for those functionalities. 5% of individuals do not expect any time savings;
- ***significant savings of money*** were expected by 45% to 51% of respondents (depending on the specific functionality) if not required to re-submit information and documents. 9% to 16% of individuals expect no monetary savings.

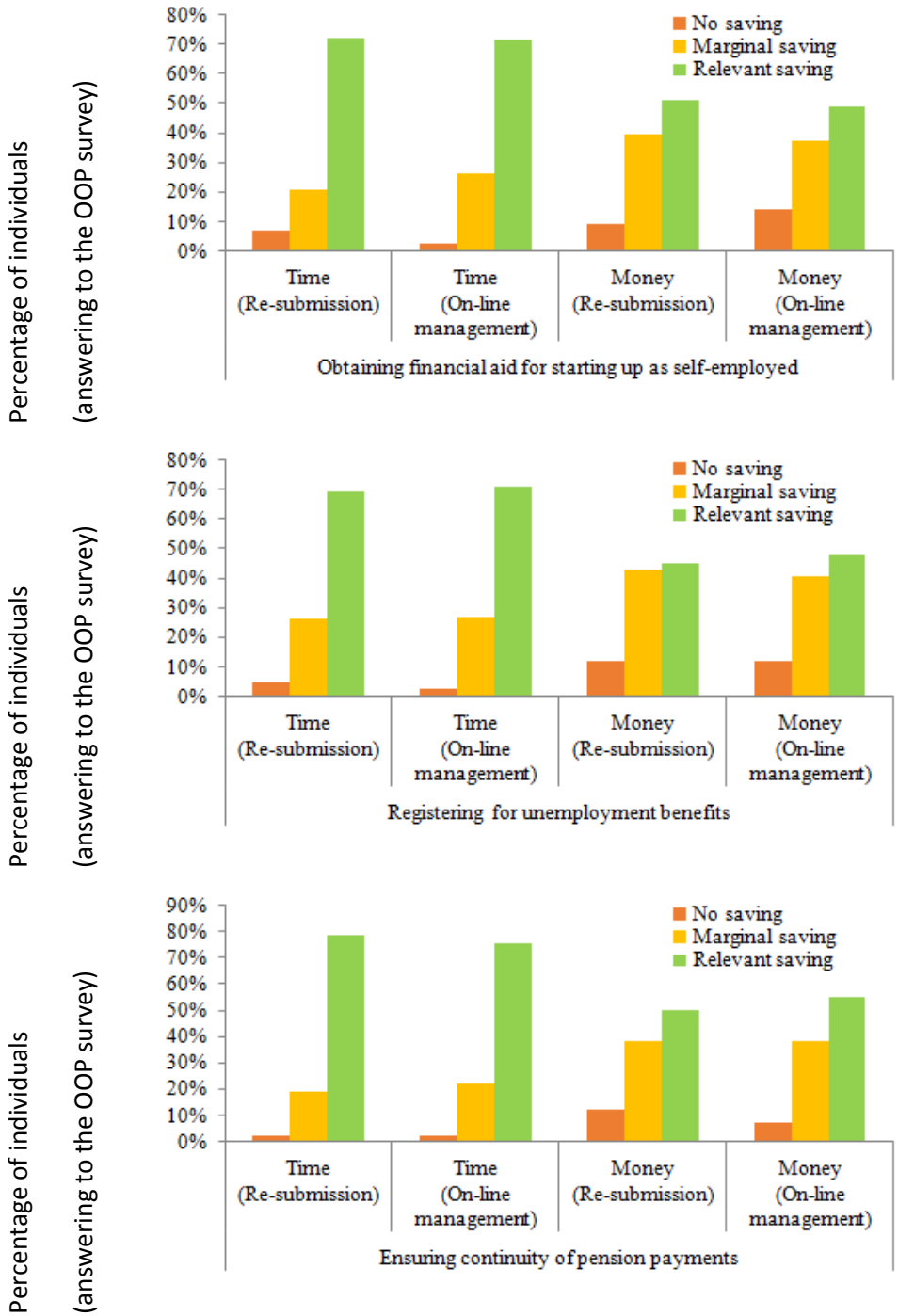
On-line management of the entire procedure is seen as even more promising from the responding individuals' perspective according to the OOP survey:

- ***significant savings of time*** were expected by 71% to 83% (depending on the specific functionality) in case of on-line management of the entire procedure. *No saving of time* is expected by 2% of the individuals.

- ***significant savings of money*** were expected by **43% to 55%** (depending on the specific functionality).

Figures below show the percentage of individuals answering to the OOP survey indicating perception of saving (both in time and in money) in case of no need of re-submission of information/data and in case of on-line management of the entire procedure needed to request of each of the five functionalities for individuals investigated in this study[195].



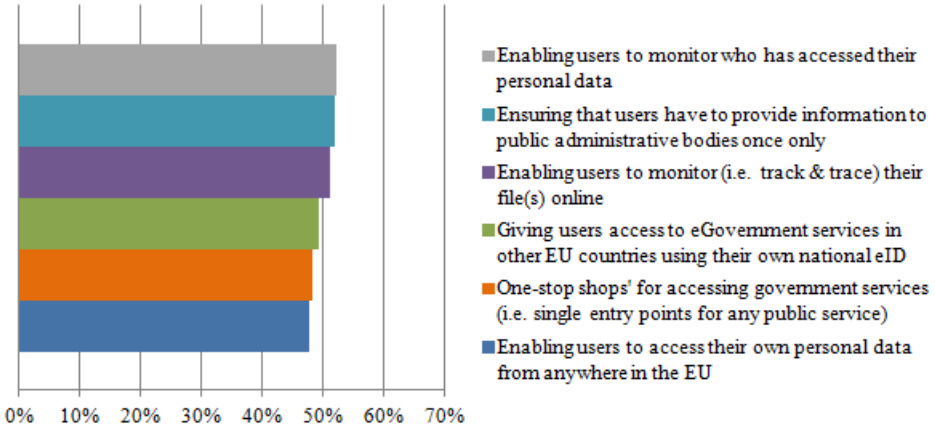


Overall, higher time savings are expected in case of digitalisation of the whole procedure than when it is no longer needed to resubmit information and documents. The Only exception is *ensuring continuity of pension payments.* Whereas data are insufficient to be conclusive on this, it may well be that digitalisation of procedures for obtaining services may become less significant for older individuals.

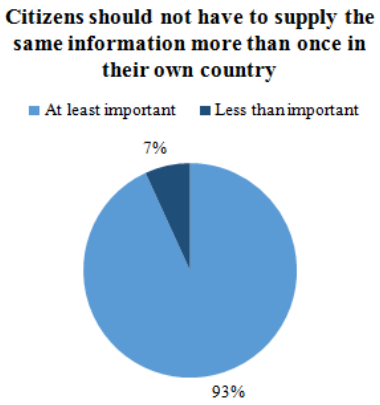
In terms of highest interest for improvement of eGovernment services over the next 5 years (and related to ones selected for individuals in this study) respondents to the Public Consultation scored as follows:

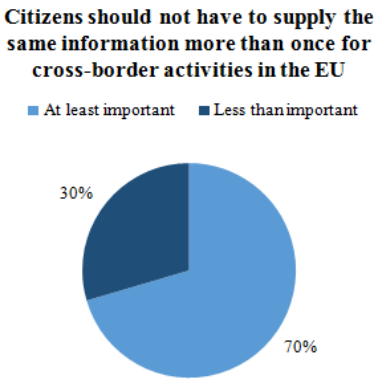
4- Enrolling in higher education and/or applying for a study grant in another EU country: 52%;
5- Looking for a job: 51%;
6- Enrolling in higher education; and/or applying for a study grant in your own country: 50%;
7- Becoming unemployed: 37%.

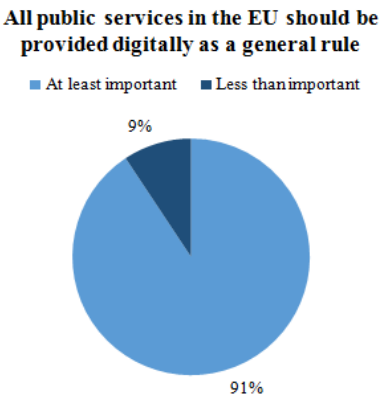
In the figure below, the measures to improve eGovernment services are rated in order of importance by individuals responding to the Public Consultation.

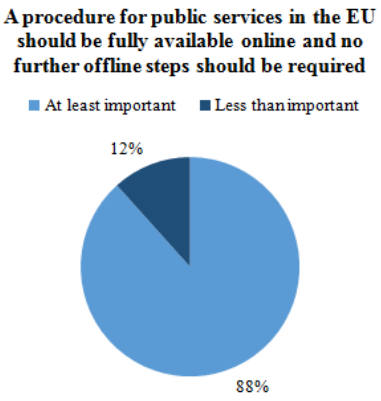


General results on the saving perception are confirmed by the individuals' indications on the relevance of potential application of four principles related to OOP. Both *the opportunity to avoid to resubmit information/data* and *digitalisation of procedures* are considered important in the national context by more than 90% of the individuals responding to the OOP survey. In case of cross-border activities, 91% indicates digitalisation of all public service to be important, 88% finds completing on-line procedures important, and 70% of individuals responding indicate to find the opportunity to avoid having to resubmit data important.



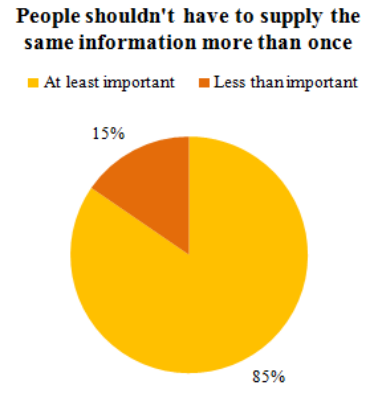


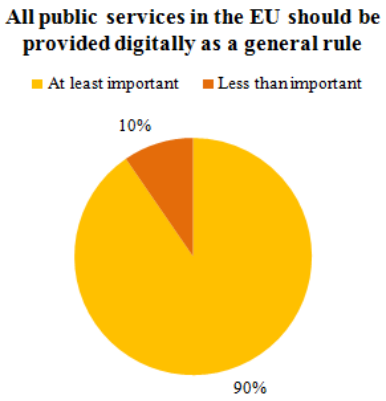


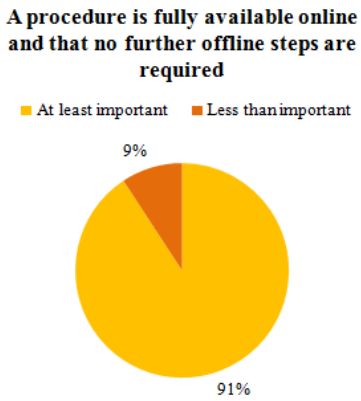


Similar indications come from the Public consultation. Digitalisation is considered *at least important* by 90% of individuals that believe that *All public services in the EU should be provided digitally as a general rule* and by 91% of individuals that believe that *A procedure should be fully available on-line and that no further offline steps are required*.

The opportunity to avoid to resubmit information/data is considered *at least important* by 85% of the respondents, No distinction between the national context and cross-border activities.





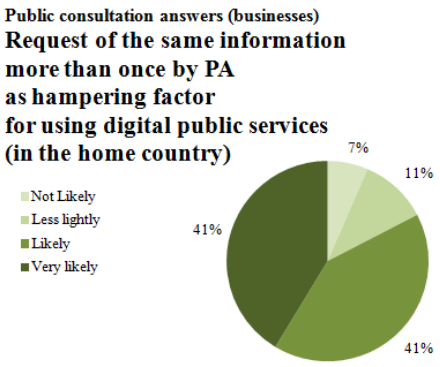


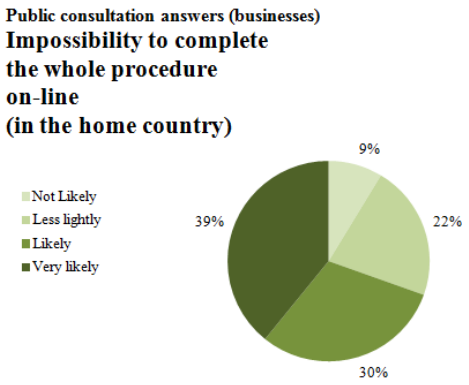
2. The businesses' perspective

Among the responding businesses to the OOP Survey, 67% of businesses declared working cross-border (either at international or European level). Only 1 business declared to have never interacted with PA through email, using websites or apps, downloading/uploading/completing forms. Taking into account all the proposed ways of interaction for eGovernment about one third of businesses confirmed that they have used this this year *At least once, but not every month.*

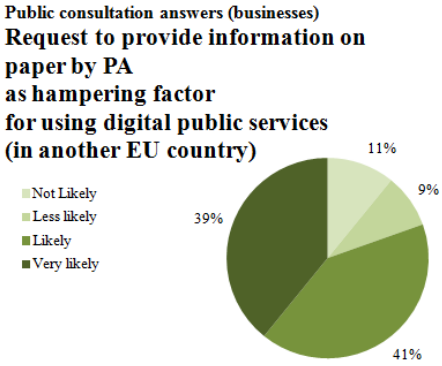
92% of the businesses responding have completed on line web forms in the last year for 2 to 10 different public services. Almost 75% never found pre-filled fields with required data of the business.

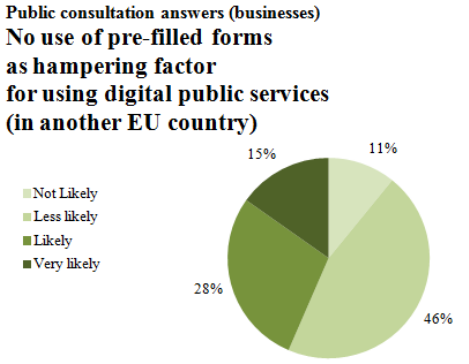
Evidence from the Public Consultation demonstrates that request of the same information more than once by the national PA is a more important hampering factor for businesses. 82% of businesses responded to find this at least "important" against 65% of the individuals. The impossibility to complete the whole procedure on-line is considered at least an important factor by 69% of the businesses when contacts are needed with public administration at national level for obtaining a public service.





Request of paper in addition to information provided on-line largely is considered as *at least an important factor* hampering the usage of digital public services in another EU country by 80% of businesses responding to the Public consultation, against 75% of individuals. The absence of pre-filled forms is considered an important hampering factor by 43% of responding businesses.





Only 6.5% of the businesses highlighted as difficulty in transferring information/documents/data between the national PA and the foreign the necessity to resubmit to the host country information/documents/data already submitted in the home country.

According to OOP survey respondents, businesses were asked more frequently to provide the **same information/documents already provided** to another public agencies/authorities or officials in the last 12 months than individuals (54% of businesses versus 42% of individuals). They were also more often asked to share information/documents already provided to another public agency/authority **for a different purpose** (62% instead of 44% of individuals).

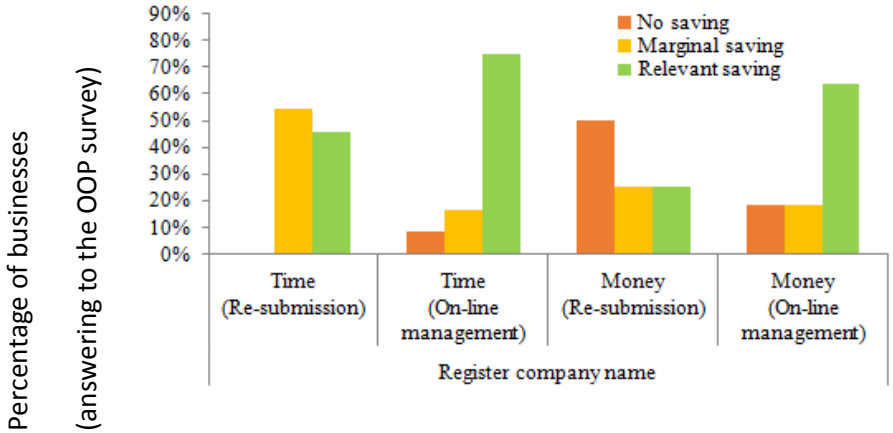
Re-submission of information/documents for obtaining services in another EU country is considered as an activity generating waste of time and loss of money also for businesses:

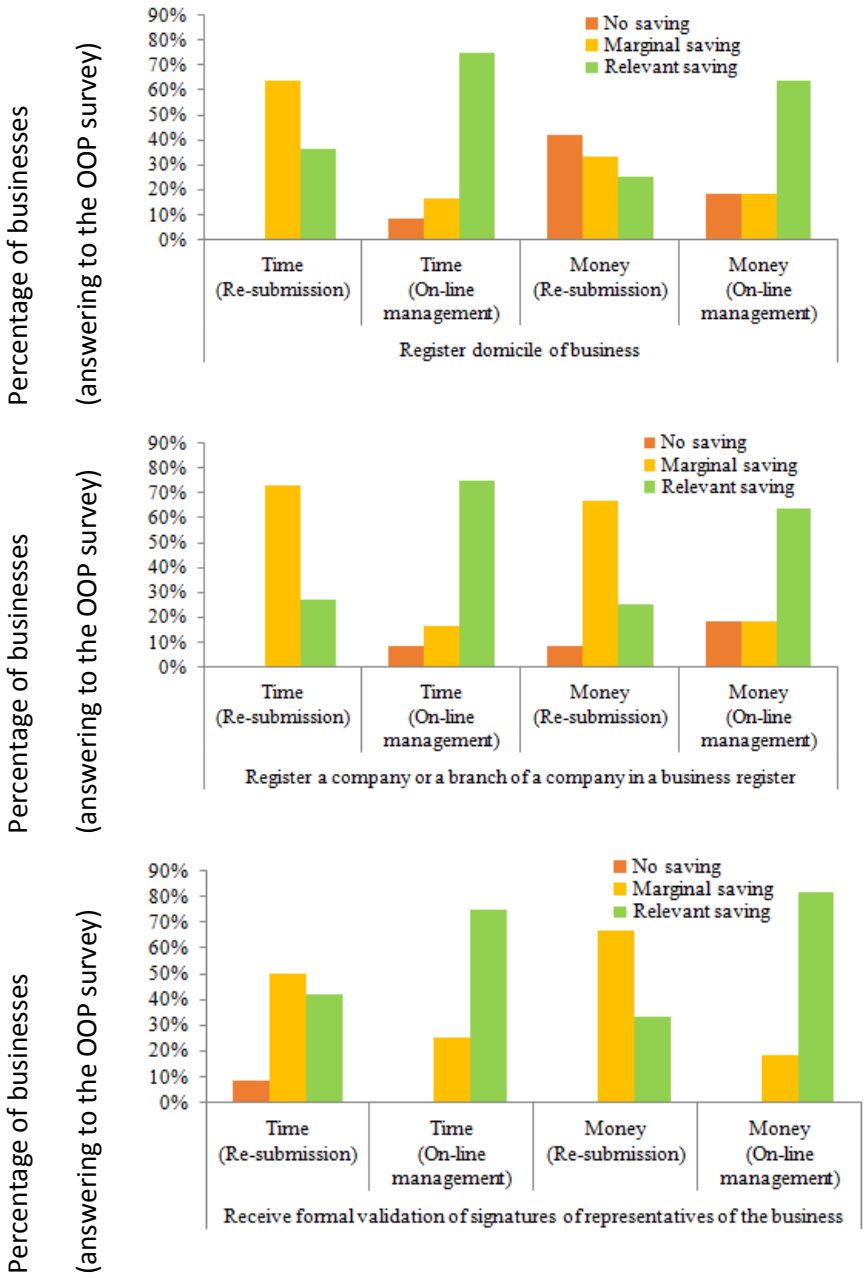
- ***Significant savings of time*** *were expected by* 27% to 91% of the business respondents to the OOP survey, varying strongly across the 10 functionalities, if not required to re-submit information and documents. On average, 4% expects *No saving of time;*
- ***Significant savings of money*** were expected by 25% to 73% of responding businesses, depending on the specific functionalities.

Online management of the entire procedure seems to be perceived from businesses as more advantageous in terms of time respect to the benefit of not re-submitting information and documents.

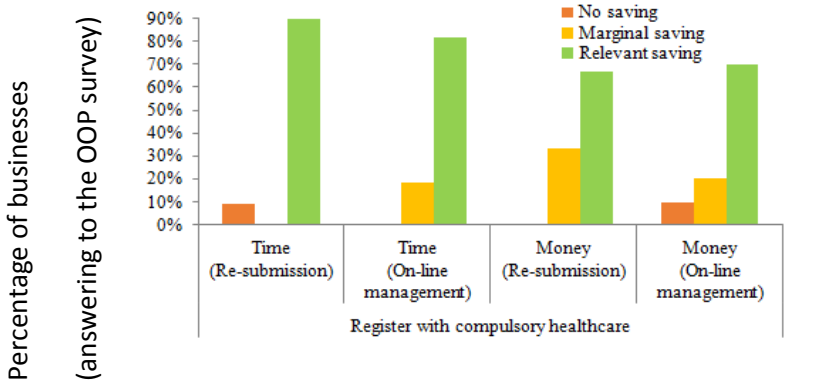
- ***Significant savings of time*** were expected by **75% to 83%** of responding businesses (depending on the specific functionality). *No saving of time* was perceived at maximum by the 8% of the businesses:
- ***Significant savings of money*** were expected by **60% to 82%** of businesses responding (depending on the specific functionality).

The figures below show the differences per functionality in responses by businesses to the OOP survey.[196].Data collected from businesses show that the overall potential saving are seen as largely positive, with some differentiation across the different functionalities.

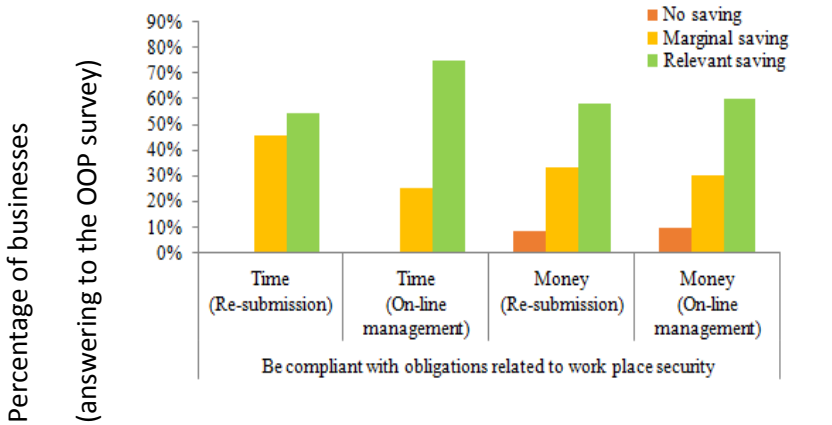


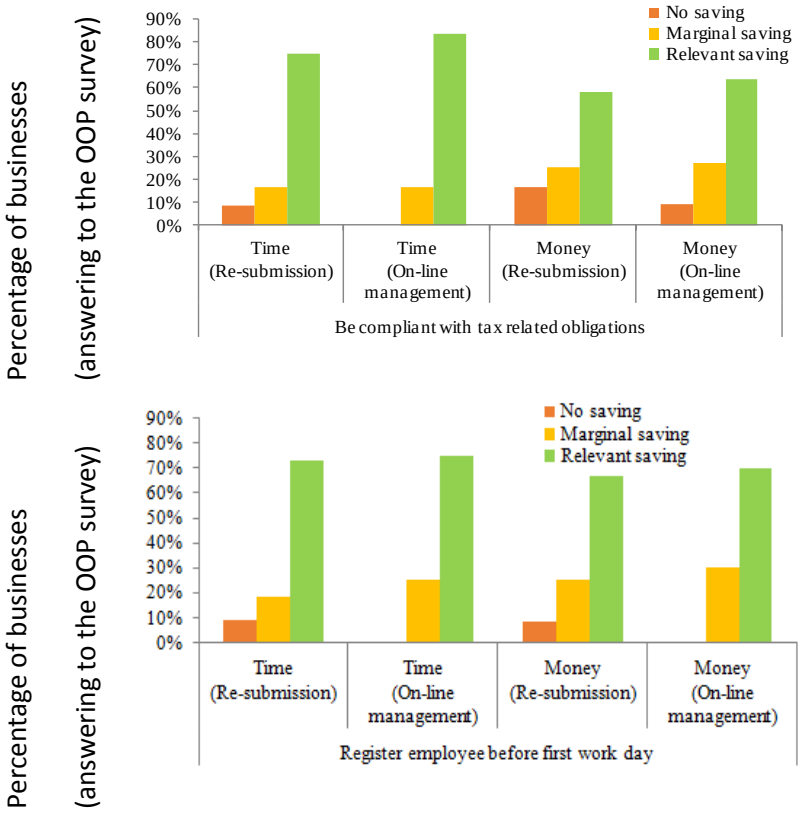

Percentage of businesses
(answering to the OOP survey)
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
No saving
Marginal saving
Relevant saving
Time (Re-submission)
Time (On-line management)
Money (Re-submission)
Money (On-line management)
Register domicile of business
Percentage of businesses
(answering to the OOP survey)
No saving
Marginal saving
Relevant saving
Register a company or a branch of a company in a business register
Percentage of businesses
(answering to the OOP survey)
No saving
Marginal saving
Relevant saving
Receive formal validation of signatures of representatives of the business


Percentage of businesses (answering to the OOP survey)
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
No saving
Marginal saving
Relevant saving
Time (Re-submission)
Time (On-line management)
Money (Re-submission)
Money (On-line management)
Register with Social Security Office


Percentage of businesses (answering to the OOP survey)
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
No saving
Marginal saving
Relevant saving
Time (Re-submission)
Time (On-line management)
Money (Re-submission)
Money (On-line management)
Register with compulsory healthcare


Percentage of businesses (answering to the OOP survey)
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
No saving
Marginal saving
Relevant saving
Time (Re-submission)
Time (On-line management)
Money (Re-submission)
Money (On-line management)
Be compliant with social security obligations

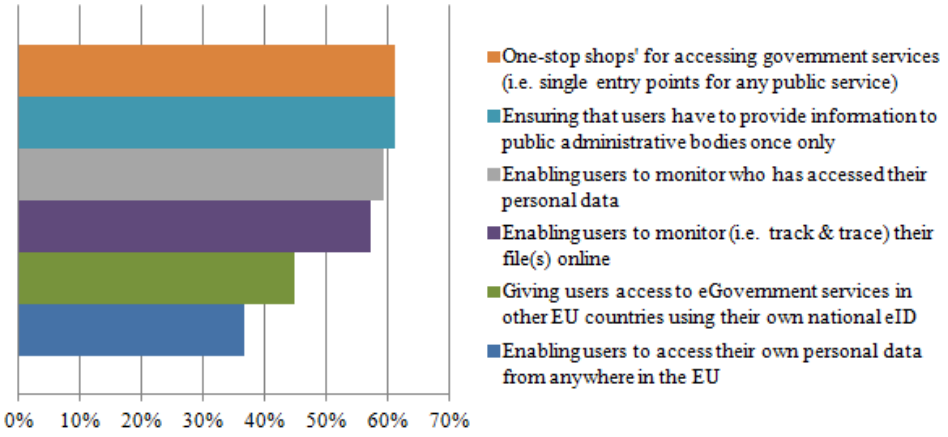

Percentage of businesses (answering to the OOP survey)
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
No saving
Marginal saving
Relevant saving
Time (Re-submission)
Time (On-line management)
Money (Re-submission)
Money (On-line management)
Be compliant with obligations related to work place security



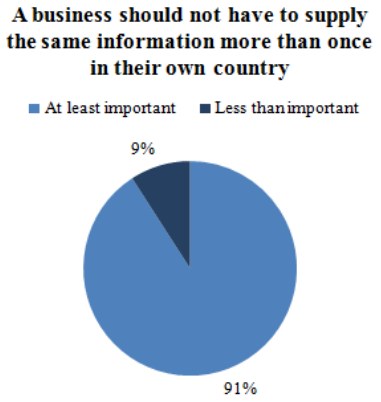
In terms of opportunities for an improvement of eGovernment services over the next 5 years (and related to the ten selected for businesses in this study), responding businesses scored the following functionalities highest:

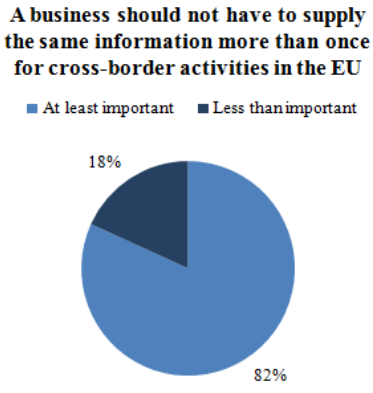
- On-line procedure for all tax-related matters: 76%;
- On-line procedures to obtain government certificates: 73%;
- Full digitalisation of the public procurement process: 45%.

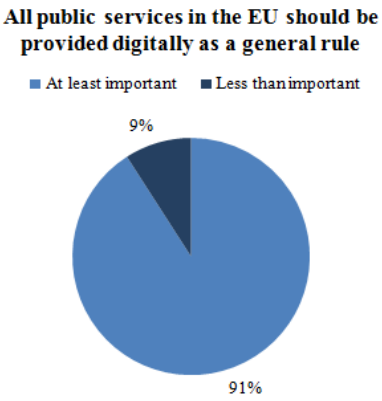
In the figure below the different measures to improve eGovernment services are rated in order of perceived importance according to business respondents to the Public Consultation.

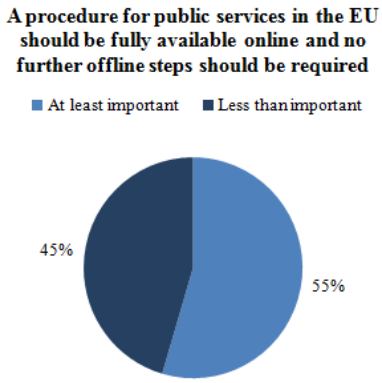


General results on the saving perception are reinforced by the businesses' indications on the relevance of potential application of four principles related to OOP. The opportunity to avoid to resubmit information/data is considered at least important in the national context by 91% of the businesses responding to the OOP survey and at least important in case of cross-border activities by 82% of them. Digitalisation is considered important as well (i.e. by 91% in case of digitalisation of all public service), Having a procedure for public services in the EU fully available on line without offline steps is considered important by Only 55% of businesses.



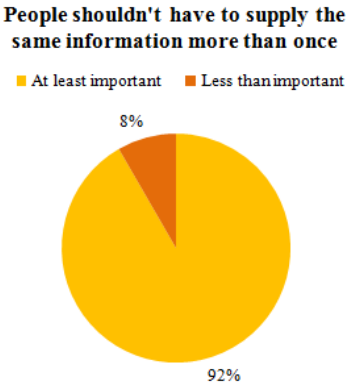


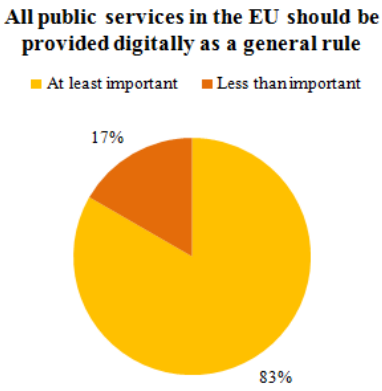


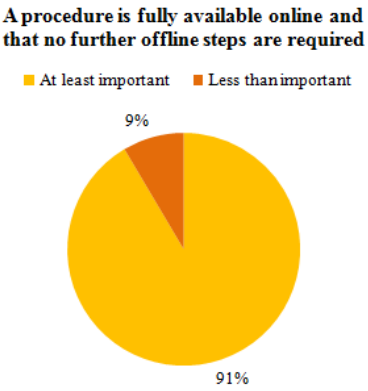


According to the Public consultation, digitalisation is considered *at least important* by 83% of businesses that believe that *All public services in the EU should be provided digitally as a general rule* while businesses believing that *A procedure should be fully available on-line and that no further offline steps are required* are 91%.

The opportunity to avoid to resubmit information/data is considered *at least important* by 92% of the respondents to the Public consultation, No distinction is made between the national and the cross-border context.







Annex V. Status Of Enablers in the Member States

The objective of this annex is to provide significant initiatives on which enablers have been better implemented and which are still behind the expectation in order to give hints on key priorities to improve the EU-wide OOP implementation.

A. Interoperability and data exchange [KF1]

1. Data protection

Data protection as an enabling factor refers to the solutions implemented to guarantee that data and information of individuals and businesses are treated in compliance with national and European standards. These solutions might include requesting data-holders consent to the use of data, opt-in/opt-out mechanisms, provision of transparent information about the entities which have accessed and used data, and reliance on the control of a data protection authority.

- All countries have implemented within their national legal framework the Directive 95/46/EC on the protection of individuals with regard to the processing of data and on the free movement of such data; as a consequence, all countries in the sample considered have a referent authority at national level for the protection of personal data;
- Spain has adopted an opt-out mechanism to guarantee the data-subject the right to express its explicit opposition to the exchange and re-use of data among public administrations;
- In Belgium, individuals can access the portal of the Ministry of Interior and control which public administration visualised his/her data in the previous month; In the Italian framework, the Code of Digital Administration specifies that any data access and use is regulated by ad-hoc framework agreements among the public administrations involved which should undergone the approval of the Italian Authority for the Protection of Personal Data.

2. Data quality

This refers to the systems used to guarantee the accuracy and the update of data and information stored. Measures in this domain can pertain the implementation of solutions for the direct update of the same data in multiple repositories or the use of effective metadata systems to control stored data.

- The pilot initiatives implemented in the UK are a good example of data quality measures; indeed, by means of the Tell-Us-Once systems a wide range of public and private entities are automatically notified in the event of death or birth, guaranteeing that the information is directly updated in all linked systems;

similar initiatives for the automatic notification of changes of residencies have been reported to be implemented in Finland and Estonia;

- Additionally, Find-It (also implemented in the UK) facilitates the research of data among the different public authorities' databases.

3. Administrative collaboration and re-use of data

Under this category, all already implemented initiatives to facilitate the exchange of data and information among public administrations should be included. These might be constituted by bilateral agreements for the re-use of data, local cooperation agreements or systems, as well as solutions and approaches implemented at European level.

- In 2015, the Finnish government completed an exploratory study on the ways in which local authorities and national agencies deal with the provision of cross-border digital services and exchanges of information[197]; the study outlined that for the following services cross-border direct exchanges of data are already implemented:
    - The Tax Administration's new KVATI application, through which basic information gathered from Finland's taxation at source is sent to an individual's new country of residence;
    - Finnish Centre for Pensions' transfer of migrant workers' insurance numbers between the country of nationality and the country of employment within EU and ETA countries; and
    - The Population Register Centre's exchange, with other EU countries, of information on individuals entitled to vote in elections to the European Parliament.
- Under the European Patients Smart Open Services pilot project (epSOS), Finland and Sweden developed a pilot service (ePrescription) for interoperable electronic prescriptions between pharmacies in the Finnish Tornio Valley and pharmacies in Sweden. Main issues emerged during the implementation of the pilot concerned semantic specifications such as data format and descriptions. Nevertheless, this pilot initiative provides evidences of the conceptual and technical feasibility of interoperable electronic prescriptions across national borders.
- Over the years, the Register Centre's Nordic Moving Service has been created to allow for the exchange of data and information about people moving among Nordic countries; in particular the basic personal information of an individual moving from one Nordic country to another, as well as life events and change of conditions of pension recipients, are automatically notified to the population registration authorities of the country of origin.
- In the recent years, Estonia has shared with Finland its X-Road solution for the exchange of data among registers of public administrations; the infrastructure is now operative and is expected to reach a critical mass of Finnish register connected by the end of 2016; the aim is to use this system in order to -first of

all- allow tax-related information exchange among these two countries (for both individuals and business);

- At European level, the eCODEX (e-Justice Communication via On-line Data Exchange) LSP represents a significant example of initiatives for data exchange at European level based on the connection and improvement of interoperability among existing national systems in the field of eJustice;
- Under the e-SENS project, specific attention has been dedicated to the development of a building block pertaining the transmission of documents; the building block elaborated, eDelivery, is based on a four-corner topology and intends to standardise communications among intermediate gateways; in the solution envisaged, the Message Exchange Protocol was based on the version 3 of OASIS ebXML Messaging Services - ebMS3 (due to its growing implementation in commercial and open source solutions).

4. Legal requirements

Legal requirements as potential enablers refer to all law and regulations implemented at national – and potentially at European level- aimed at facilitating the implementation of the OOP.

- Estonia, Netherlands and Belgium have already implemented laws that enforces the implementation of the Once-Only principle; in Estonia the approach selected was to explicitly force public administrations to re-use data already available in other public administration registries (art.43 of the Public Information Act); in Belgium, by means of Loi 5 Mai 2014 all federal administrations have been required to implement the OOP and use eID numbers to retrieve data form official registers; finally, in The Netherlands, legislation related to base registers oblige public services to make use of data contained therein;
- In the Spanish case, OOP is recognised as a right of the individuals not to deliver data and documents already in the hands of public administrations by means of the law 40/2015 of October 1st.

5. Technical architecture

Technical architecture as an enabler factor refers to the design of the whole infrastructure that would enable the exchange of data and information among public administrations.

- In the case of Estonia, the solution implemented to facilitate data exchanges among public authorities was not to replicate all data previously stored in a single repository, but rather to design a secured connection system among distributed data repositories; the technical architecture implemented for the re-use of data provided to public administrations is based on a secured Internet-based communication protocol (X-Road) which allows for the exchange of information and data on a single individual (recognised thanks to

his/her identification number); this protocol is well tested and implemented, includes metadata that allow for the recognition of data stored in each database and security means that guarantee the protection of the distributed system and of the transmissions therein; the system has been exported and implemented in Finland to facilitate the exchange of data and information between these two countries on tax-payers;

- In Spain, the "red SARA" (System of applications and connections of public administrations) is a system based on communication protocols and base services that facilitates the exchanges of information among public administrations, based on cloud services; the implementation of this system was requested by law (Article 43 of Ley 11/2007 LAECSP) and is under the authority of the Ministry of Enterprises and Public Administrations. Additionally the Data Intermediation Platform is a type of horizontal service intended to simplify administrative procedures, so that individuals or businesses do not have to deliver data or documents already held by public authorities, and to reduce fraud in applications and related procedures. The Data Intermediation Platform currently serves as an intermediation platform for 40 verification data types, including unemployment situation and grants; cadastre information; checking of the fulfilment of tax and social security obligations; academic degrees; Civil Registries for birth, death and marriage; Pension Information.
- At European level, the TESTA system (Trans-European Services for Telematics between Administrations) is the IP-based network that supports a platform for secure information exchanges among a majority of EU institutions, Agencies and Member States.

6. Semantic solutions

Semantic enablers are all those solutions and components elaborated to match concepts within different national meaning's systems and facilitate the mutual comprehension of documentations and information handled by public administrations.

- Very basic problems have been reported thus far, such as heterogeneity in the definitions of specific concepts (e.g. company) and in the provision of some information (e.g. address components' ordering street + number vs. number + street).
- In Estonia, a crucial component of the OOP system is the central data catalogue RIHA, a centralised catalogue composed of metadata and information which underpins the functioning of the entire system; to join X-Road it is compulsory to be compliant with the metadata of this database.
- ISA (*Interoperability Solutions for European public administrations*) has work to address semantic issues in particular by developing core vocabularies for persons, registered organisations, core locations and core public services. For the messaging model, the system of interconnection of business registers (BRIS) has also used the Core Business Vocabulary developed by ISA.

- e-Government Core Vocabularies "as simplified, re-usable and extensible data models that capture the fundamental characteristics of a data entity in a context-neutral fashion" have been made available on the Joinup platform[198].
- the eSens project (http://www.esens.eu/) has dedicated specific attention to address semantic problems associated with legal and official documents, in particular by working on semantic resources, concepts and codes as well as on semantic mapping; these elements are fundamental to create machine-understandable descriptions of data and facilitate the future development of automated search and translation system.

7. Language solutions

Language enablers are all those solutions and components elaborated to tackle language barriers emerging during administrative procedures, such as the need for certified translation of documents and availability of forms only in the national language.

- MT@EC – Machine Translation Service is a statistical machine translation system implemented by the European Commission to provide high quality translations in all EU28 languages of documents and information; this tool provides both a web-users interface (for human access) and a machine-to-machine interface (accessible via web-service protocols); this system has been suggested by some national respondents as a viable solution to make information reported in eGovernment website directly available in multiple languages;
- Additionally, where countries officially recognise more than one language as official one, documents are typically available in multiple languages, thus providing potential benefits for incoming foreigners sharing one of the languages officially recognised (e.g. Swedish people moving to Finland).

B. Base registries [KF2]

Base registries can constitute a powerful enabler of OOP especially when these datasets are officially recognised and retrieving information from these sources is requested by law.

- At the EU level, ISA - interoperability solutions for European public administrations[199], launched an action for the period 2010-2016 and extended with the ISA2 programme aims to assess the needs and requirements for a framework that will enable access to authentic data sources at Member State level, with the final objective to achieve cross-border access to the base registries of data held by Member States. The action is also considering good practices on building successful interconnections of base registries and good practices on access to base registries. Several case studies and good practices were already identified, with some potentially mature solutions highlighted (e.g. the EUCARIS - European CAR and driving license Information System – a

single network within the area of road transport connecting national registration authorities); furthermore, ISA² has consistently worked on the implementation of a cartography of reusable solutions for building Base Registries based on sound practices at European and MS level, and on the establishment of an observatory on the state-of-the-art on Base Registries;

- In some countries base registries are at the base pillars for the re-use of data in the domain of public administrations, such as in Finland, Estonia, Belgium and The Netherlands; indeed in the Netherlands there are specific legislations in place for all 12 Base Registries, including one Base Registry for Persons.

C. eID and eTrust services [KF3]:

1. Electronic identification (eID) systems

eID as a potential enabler refers to the solutions adopted or piloted to provide individuals and businesses with single mean of identification which can be used to access multiple services and retrieve data and information associated to this identifier.

- In some countries eID are already well consolidated systems, such as Finland, Estonia, Portugal, Spain, Austria and Belgium, making it possible for individuals and businesses to access online services; additionally, such as in the case of Belgium and Estonia, these systems are used to support the data exchange among different public administrations by providing a single identifier to which all data and information of a certain data-holders are associated and by means of which these data and information can be retrieved from different sources;
- Initiatives have been launched also at European level to elaborate and implement electronic identification systems, such as in the case of the LSP STORK 2.0 and the ECAS system; ECAS – *European Commission Authentication System* is the system implemented to access the majority of website and services run by the European Commission: ECAS provides users with single interface to manage a set of data provided to the EC as well as to keep trace of previous interactions; finally, the STORK 2.0 large scale pilot project (https://www.eid-stork2.eu/) is working towards the elaboration of European electronic identification and authentication area by addressing issues such as the need for common specifications and interoperable building blocks. The project has finalised in 2015 and now the results are being consolidated by eSENS and CEF Digital;
- Single-sign-on systems are also diffused, as in the case of The Netherlands and Italy; The Netherlands have implemented a system called DigiD (www.digid.NI/) to allow individuals and businesses to log in with a high number of eGovernment websites and obtain related services; similarly, Italy is currently implementing its system called SPID (System for Digital Identity, http://www.spid.gov.it/) which will grant individuals with a single combination of credentials to access a vast number of public services[200]: the system was

designed to include three progressive levels of security to better address the needs of different types of services.

- Finally, once implemented at national level the eIDAS regulation (Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market) would have a great impact on eID and trust systems usability by guaranteeing that individuals and business can re-use their national eID schemes to access public services in other EU Member States; in the framework of the Connecting Europe Facility, the eID solution propose is based on the results of the STORK project (*Secure idenTity acrOss boRders linKed*) and consists of two core software components, namely a package of modules to allow the communication among eIDAS enabled MSs (in a centralised or distributed fashion) and additional tools for testing the system; so far the STORK system has been implemented in several MSs within different domains (e.g. eDelivery applications, address changes notifications, university enrolment, etc.).

2. Trust

Trust as a potential enabler refers to the measures and solutions adopted to improve the individuals and businesses' perception of reliability and accountability of public administrations in the use and re-use of data and information. These measures might include awareness rising campaigns, definition of complaint procedures or use of unique interface for the interaction between public administrations and individuals and businesses.

The implementation of a One-stop-shop for collecting information on public services has been reported during the interviews with individuals and businesses' representatives as a valuable means to improve the accountability of national systems from the perception of individuals and businesses; this approach has been adopted in Spain (PAe webpage[201] centralising all information about eGovernment), UK (Government Gateway[202] providing both information and services access) and at European level through the realisation of the Points of Single Contact (EUGO network).

Annex VI. Gaps and barriers

Interoperability barriers have been separated for the purpose of analysis into the following categories:

- Legal
- Organisational
- Semantic
- Technical

Associated with these barriers are specific 'symptoms' linked either to the existence and significance or to their role in contributing to the overall problem. These are developed in more detail below.

A. Legal

Information processing is governed by a range of laws at European and Member State level. Some of the legal impediments to OOP operate within countries; where different or incompatible approaches have been taken, they affect cross border reuse of information based on national laws[203]. Where European Regulations (notably GDPR) apply or are due to come into force, national differences will eventually become less serious. OOP must have a legal basis, but this is not derived from OOP-specific legislation; legal frameworks facilitate, mandate or prohibit data-sharing arrangements or act to increase or decrease the advantages of adopting OOP. In general, laws may control data and information stocks and flows (e.g. determining which data can be used for specified government purposes and when), enabling organisational changes or even by controlling the information management environment (e.g. by requiring data submitted to public administrations to be held in unique locations or by creating specific opt-in or opt-out powers for data referents).

Legal basis for OOP processing

The essence of the legal barriers, as reflected in current policy literature and confirmed by national representatives of public administrations, of citizens and of businesses interviewed, is the need for an unambiguous, reliable and mutually-recognised legal basis for processing (collecting, storing, using, sharing and reusing) data for OOP purposes. Such *acceptability* of OOP processing operates differently for personal and for non-personal (including business) data (see Annex VII), but some issues are common to both settings. Specifically with regard to cross-border OOP, this entails a legal basis for collection, retention, exchange and reuse of information about citizens and businesses between Administrations across borders

and for use of these data in the same way as those obtained directly from data referents.

Legal basis for document and digital equivalence

One impediment to the creation of a uniform legal basis for OOP processing is the insistence of many public administration procedures on having information provided in specific documentary form, which may differ from country to country and purpose to purpose. Given such document-centred structures, OOP implementation requires equivalence among documents drawn up in different ways and for different purposes; this is necessarily complicated by practical issues that would not affect digital information exchange. For example, documents relating to a given service request in different countries may include different information, be authenticated in different ways or by different people and be difficult to replicate or transmit. These barriers would remain under a literal cross-border OOP implementation. Indeed, some could be worse across borders than within a single country, considering:

- costs and delays of document handling;
- the need to establish mutual recognition for multiple documents;
- practical and legal difficulties of removing data that should not be shared from another country's documents or assembling information from several documents whose *mutual authenticity* must be assured; and
- (especially for personal data) the challenges of maintaining as an integral part of the documentation evidence of how and for what purposes it has been changed and used.

All these are much easier to manage in the digital world, so legal equivalence between documents and the information they contain (or even a recognition of the superiority of digital information for some purposes) would help OOP adoption[204].

Conversely, a specific legal basis for OOP should lead to greater experience and awareness of the limitations of document-based requirements and help make the case for a legal basis for equivalence or mandatory use of digital information.

Even where there is no problem in establishing the quality, relevance and substance of data previously submitted to different national authorities, rules that prescribe the documentary form and contents of such information may prevent re-use or inhibit initiatives to establish EU-wide OOP. This is not a general barrier; the Services Directive[205] provides a significant precondition for OOP implementation; in particular, Chapter III (Administrative Simplification) requires Member States to accept *any equivalent certificate or attestation document issued by another Member State* (Article 5)[206]. The final articles of the Services Directive make explicit reference to the intention to establish an electronic system for the exchange of

information among Member States[207]. A similar system is envisaged in the Intelligent Transport Systems Directive[208] of the European Parliament laying down the framework for the deployment of. Nevertheless, only a few specific services and forms of information are legally required to be available electronically cross-border. These include registration of a new legal entity or branch[209] for businesses and the Cross-border Healthcare Directive[210] for citizens which mentions electronic prescriptions and patient summaries.

EU level endorsement

Widespread Member State resistance to many data transfers has led some to suggest a horizontal legal basis at EU level. This is unlikely wholly to eliminate obstacles to OOP, which reflect both general acceptability principles and requirements applying to specific data and purposes. However, a legal mandate on the (optional or obligatory) acceptability of data under certain conditions would be consistent with the provisions in the eIDAS Regulation.

Pan-European legal information

According to the citizens and businesses representatives, there are gaps in the accessibility of information about national laws and their peculiarities, especially to non-national potential users. In particular, it was pointed out that it is very difficult for a non-national user to find applicable regulation, the competent authority and the proper administration for each specific service.

Horizontal or EU-wide databases

Multilateral concerns over acceptability could be further addressed by measures that provide legal bases for horizontal databases (virtually if not actually at EU level) of reusable data. Such databases would have to provide the same answer to a question asked in different EU countries, whether within the originating Member State or another. If they contain personal data, they raise substantial and significant data protection, privacy and fair information processing concerns. In general, they face political and practical obstacles. Most Member States would oppose EU level databases except in specifically defined cases. There are also substantial organisational and process obstacles to controlling data ingress, processing and egress, especially across borders. Where agreement exists on commonly accessible datasets, the most feasible approach is interconnection of national databases subject to interoperability standards at different government levels, where necessary backed up by central semantic and metadata repositories and translation algorithms. The legal dimensions of this have yet to be established, as interoperability is sometimes hindered by legal requirements for specific processes and is itself fully enshrined in legislation. A central database containing authentic and up-to-date copies of national data – if feasible and practicable – could address

some privacy and security concerns by restricting the identities and purposes involved in data processing. An example is provided by ECRIS[211], which is limited as to data type, the purposes of processing and access[212]. Inclusion of other data (i.e. not criminal records) on a voluntary basis could offer procedural simplification and acceleration. However, such a database would require amending a range of Directives and related national laws that include conditions on data management and re-use. In the case of personal data, the GDPR also requires appropriate technical and operational safeguards to mitigate risks to the rights and freedoms of natural persons.

Legal issues vary for different data types

Measures to overcome such legal obstacles to OOP should reflect different types of data and different purposes. These differences are already evident in practice: basic business data are available for free under open access conditions; access to land registry data is purpose-limited and may attract a fee; and legal registry data may be restricted to public authorities but may be further restricted to require warrants for access by police officers.

Tensions between OOP and different laws and principles

Beyond the need for a legal basis, there is a potential tension between OOP and compliance with specific laws and regulations, and a possibility of overlap among the powers of different regulators (e.g. national data protection supervisory authorities and financial conduct regulators). This is almost inevitable in view of the necessary specificity of laws and the abstract clarity of principles. Areas where such tensions will need carefully to be considered include:

- Data protection and personal privacy;
- Implementation and verification of meaningful and reliable consent;
- Security - including cybersecurity and information security;
- Proprietary or confidential business data;
- Fair processing principles, among which purpose limitation[213], data minimisation, adequacy, accuracy and retention stand out;
- Data sharing rules, which are sometimes governed by statutory codes of conduct intended to clarify the requirements of black-letter law[214];
- Lack of equivalence between documentary and digital information[215]; and
- Different information requirements for otherwise-equivalent services in different jurisdictions.

Finally, a frequently reported legal barrier – primarily with regards to citizens, but in some aspects also for businesses – involves privacy rights. The protection of personal data recognised by Directive 95/46/EC[216] and reinforced by the GDPR

provides an effective framework to guarantee both the security of data and the possibility of exchanging them for OOP purposes. However, the GDPR also imposes some practical impediments and limitations (e.g. as regards consent and information) that inhibit OOP processing or limit its potential benefits (see Section III.III.A). In some cases[217] exchange of data among public administrations needs to be approved by data protection authorities.

B. Organisational

Organisational barriers pertain to non-technical requirements imposed on cross-border interactions that might deter or distort OOP implementation. The following discussion concentrates on Economic and Social gaps and barriers. They include concrete constraints such as lack of suitable resources, cultural impediments and dynamic or path-dependent factors. The re-use of data submitted to different public administrations may be complicated by organisational factors that make it hard to request or provide data, by differences in data storage and access arrangements, by different service and procedural architectures or by the need for political endorsement at suitable levels.

1. Economic gaps and barriers

These come in two forms: monetiseable costs of procedural and legal changes and broader economic impacts stemming from reduced barriers to cross-border activity.

In terms of the narrower (commercial and fiduciary) impacts, while OOP implementation may be expected to reduce administrative burden and associated costs for individuals and businesses in the short-term and for public administrations in the medium to long term, the deployment and maintenance of supporting systems[218] requires potentially costly and even risky investment. Other organisational costs may arise from e.g. substitution of legacy systems, change management and the need for communication campaigns targeting individuals and businesses and even other public administrations. According to the interviews, cost savings generated by OOP implementation may ultimately justify the initial investment and additional resources required – in particular human ones.

Insights from the EU NL 2016 session on the Once-Only principle

The Netherlands EU Presidency 2016 (June 2nd, 2016) event on Digital and Open Government hosted a session dedicated to Once-Only Principle implementation experiences and perspectives. The invited panellists were Siim Sikkut (Estonia), Bart Drewes (The Netherlands), Cedric van Damme (Belgium) and Jonathan Cave (part of the working team of this study). The National representatives presented the experiences of OOP implementation in their country and discussed the adopted approach and the strength points. Economic and cost-benefits-related considerations emerged and confirmed the relevance of the pay back perspectives for Public Administration. In particular:

- The Estonian representative underlined that the OOP implementation generated several services simplification gains, making it possible to re-allocate resources to other services or activities; cost-savings emerged from the OOP implementation are currently subject of a study; the goal is not to collect exact and punctual estimation of the costs but the magnitude of economic benefit;
- The Dutch representative commented that at national level the implementation of the OOP produced important reductions of administrative burden and generated costs savings for 163 million of Euro per year; even though these monetary gains can seems less impressive in unitary terms (10 euro per person = 15 minutes of saving time), the added value of the initiative is the public value of these simplifications and indirect benefits;
- The Belgian representative reported that this system have generated an estimated money saving of about 100.000.000 euro/year; this estimation has to be refined in the next years when the system will be more consolidated.

When the discussion was opened to the audience, one suggestion to the national representatives was for considering also costs/benefits of individuals and businesses and not only savings experienced by public administrations. Although this limitation, discussion provided significant indications on the potential economic benefits generated by the OOP implementation.

Finally, interviews with all public administration national representatives confirmed that such fiduciary considerations strongly influence the form and uptake of cross-border data and information exchange. Priority is given to services most frequently used by individuals and businesses (e.g. tax), where the high volume and visibility of transactions allow such initiatives to reach a "social break-even-point" quite quickly. Note, however, that these are not necessarily the situations and services offering the greatest potential for burden reduction let alone those where progress may have the greatest spill-over effect on OOP in other areas. There is also no guarantee that cross-border initiatives will optimise economic impacts in the strict sense; barriers to cross-border service provision may (at least implicitly) be supported by domestic individuals claiming services or benefits and by rival firms, while the countries from which service claimants come may be unwilling to commit

resources to helping another Member State meet its obligations more efficiently, even when their own individuals and businesses stand to benefit.

2. Resource limitations

One frequently-cited obstacle is the lack of resources needed to adopt OOP or simply to manage the change process. This can refer to money, hardware, ICT or other skills. It is important to recognise that the lack of resources and other organisational barriers often represent an inability to capture at the level of a single public administration, benefits accruing to the organisation or country as a whole, or to beneficiaries. Additionally, even directly beneficial changes may be difficult to authorise if the rewards cannot be adequately quantified or are regarded as to delayed or uncertain.

3. Resistance to sharing

A second barrier, more linked to organisational culture than organisation *per se* is a systematic unwillingness to share data with other administrations or other offices. The literature on government abounds with examples of such informational stovepiping[219], both within Member States and especially across borders, which does not need to be connected to an actual transfer or dilution of power.

4. Lack of necessary alignment

A third barrier is the lack of harmonisation of different processes, meaning both the processes using data from a single service request (e.g. verifying eligibility vs. providing and evaluating services) and the processes that might wish to re-use data. The lack of harmonisation might also be technological or semantic, but is often simply a matter of work-flow management and decision procedures; these can frustrate attempts to locate all the places from which relevant data may be obtained or to which they should be propagated.

5. Inconsistent and slow uptake

There are also organisational and dynamic obstacles arising from the overall complex of public administrations. Their relative isolation has led to a variety of different approaches and rates of progress at the single-country level. For cross-border OOP, the slow overall pace of OOP uptake within countries makes it hard to build a European OOP by interconnection, linkage or transfer of functions or data to common platforms[220].

The same inconsistent and patchy uptake across countries and service areas combined with the diversity or incompatibility of drivers weakens different Member State and administrative incentives to develop and adopt common

elements (including semantic and technical elements, and also common national legal approaches) for reasons of inertia and adoption cost.

6. OOP as a service

An alternative approach, which rests directly on organisational change, is to provide key building blocks as services rather than requiring individual offices to develop or adopt them in-house. This 'agency' model, based on explicit service level agreements among administrations, has been used successfully in some aspects of e.g. procurement or cybersecurity, where there were sufficiently common 'in-house' measures in place. But for information re-use, the State of Play assessment and interviews indicate that fragmentation and underuse hinder the deployment of common services, including catalogues and/or 'find-it' services to locate and evaluate sources of data suitable for re-use.

7. Cultural awareness

Even basic *awareness* of OOP is limited by 'organisational culture' factors (most of which are already present within countries, let alone across borders):

- OOP is built on top of existing systems, so the non-OOP default is always present and is what all parties are accustomed to;
- Each 'point of contact' from a public administration with a citizen or business is used to collecting specific data and data referents are accustomed to providing those data, so neither points of contact nor data referents may be fully aware of the existence of alternative sources, let alone the possibility of using different data to meet the same requirements;
- Lack of trust in data re-use by data referents and third-party data providers means that the level of citizen or business demand for OOP may be modest, or even that steps taken to introduce it may be resisted;
- Resistance to data interchange may not be based on concrete expectations, but may simply reflect an attitude that "data are power" or manifest as an insistence on maintaining 'bespoke' (localised) formats, processing methods, etc. which have the effect of limiting the visibility and transparency of alternative data and of directly impeding interoperability;
- In general, most organisations display a lack of incentives, willingness and ability to assess burdens, identify where they should be minimised and reduce them; and
- There are only limited mechanisms for cost- and responsibility- sharing across office, policy and national boundaries including payments to help data controllers meet the costs of responding to access or information requests from other authorities within a country, let alone from authorities in other countries;

- Last, but not least, barriers relating to the use of different languages and differences in legal base for multiple relevant aspects often have a strong cultural dimension.

Finally, specific applications of OOP may arouse societal resistance. The most frequently-cited societal barrier relates to the specific needs of Europe's ageing population. The issue relates to the cost and scarcity of the specific services requested (e.g. healthcare and pensions) but also to the modalities of service request and handling. As with other eGovernment services, there are difficulties stemming from the generally lower skills, awareness, trust and acceptance of digital technologies by the elderly. They are generally less familiar with online services and handling of personal data profiles; ancillary problems (e.g. language) may also be less visible and thus more problematic in e-enabled environments. To avoid exclusion or even harm by implementing digital solutions associated with OOP (e.g. unique eID identifiers or digitalisation of familiar procedures), tailored communication and awareness campaigns are needed. It may be necessary to retain, for a transitional period at least[221], non-electronic or even face-to-face alternatives for completing procedures. In this case, as business representatives pointed out, it will be necessary to evaluate specific costs associated with maintaining multiple channels to ensure that the savings generated by digitised OOP procedures would not be minimised or even reversed. In an ideal world, the digital infrastructure needed to support OOP-related data exchange requires investments that would be compensated by cost savings from reduced use of human resources or otherwise. Retaining in-person channels may be perceived as preventing this payback, meaning that deployment and maintenance costs will be counted as purely additional.

C. Semantic

Semantic gaps and barriers pertain to language barriers and problems with consistent interpretation of words and concepts. All national public administration representatives cited language and translation issues as primary barriers to EU-wide OOP implementation. On-line forms for requesting public services are typically available only in approved national languages; documents granted by other Member States must often be translated[222]; and individual and business representatives reported language problems in gaining access to services in other Member States, especially requirements for certified translations.

Cross-border semantic issues were also raised by national public administration representatives regarding both the way information is reported and differences in information in apparently-equivalent documents (e.g. certificates).

Examples of semantic differences

The Finnish national representatives noted that the concept of a 'company' varies in breadth across Member States.

Citizen representatives noted that some countries (e.g. Finland and Italy) express addresses as "Street name + number;" others place the number first or use post code and house name or number: this minor difference can constitute a semantic problem in particular for automated systems. The spread of multiple address lookup services creates a situation whereby the same address may be expressed in multiple ways interchangeably in a given system or across multiple systems (e.g. the electoral roll, tax records and Post Office databases in the UK). These differences may be more important for some purposes (e.g. fraud prevention) than for others.

The Dutch national representative underlined the necessity of good quality metadata and ultimately normalisation" of data across registries, recognising that concepts are partly determined by culture and habit and that concepts can mean different things across different Member States.

In general, semantic barriers arise when information or documents express the same or equivalent information in different ways. This may make it hard to:

- identify relevant information:
- accept it for administrative purposes;
- gauge its full meaning and reliability; and
- prevent downward pressure on quality and efficiency of service caused by excessive cost or adoption of 'least common denominator' standardised data models.

It can also foreclose an important back channel whereby public administrations can detect changes in the required information and other developments. These are not extensively discussed here because they have been the subject of detailed analysis and proposed solutions in more general settings such as the European Interoperability Framework (further: EIF) and ISA[2](Interoperability Solutions for European Public Administrations).

Specific manifestations of semantic barriers include:

- inconsistent definitions of data elements (sometimes anchored in specific national legislation);
- different data models;
- fragmentation and underuse that affect the development and acceptance of base repositories or registries[223]; and

- lack of clarity/willingness about who should pay for, own and control such repositories (even if this ownership does not extend to the data they contain).

D. Technological

One immediate consequence of OOP is the need to obtain information from other systems and to use it in a manner fully equivalent to information directly provided. This may not require a high level of technical interoperability, but barriers to interoperability will certainly dilute the benefits to be expected from OOP, provoke resistance from technical and support staff as well as policy makers and service providers and may distort the realisation of OOP itself. Again, these barriers have been extensively discussed elsewhere.

As a general rule, the technological barriers of greatest relevance to cross-border OOP involve local solutions that cannot easily meet OOP requirements but are so embedded that modification or replacement will be resisted, or that impose transitional or ongoing costs that cannot easily be justified[224]. They include:

- Legacy systems, which provide a 'sunk cost' barrier to the adoption of new common approaches or convergent modification of existing complex ICT architectures;
- Different approaches at local or national level for handling specific types of data or for providing specific services which may mean that some types of query cannot be handled or that a minimal[225] but complete set of information cannot easily be assembled;
- Imperfect incentives and lack of critical mass, which hinder adoption of technical solutions and organisational models that support data re-use; and
- Limited possibilities to develop common access tools for non-base repositories, access to distributed data sources and query-based (e.g. 'request filter') access to data.

The majority of national and business representatives considered that EU-wide OOP does not constitute a problem *per se* from the technological point of view; enabling technologies for some services are already in place[226]. There are also consistent trends to make services available through online portals and to use cloud computing technologies[227] to support service provision requiring data exchanges among Member States[228].

As perceived by individuals and businesses, the increasing availability of broadband connections, which allows public administration to provide and individuals and businesses to benefit from online services, creates an associated gap. The continuing inequality of broadband provision, especially across Member States, remains a significant technical gap affecting EU-wide OOP on both supply and demand sides. The supply of cross-border OOP depends on the digitisation of

services provided by public administrations and on the technological comparability and compatibility of the requesting and providing ends of cross-border exchanges. Demand for OOP is directly correlated with the accessibility to individuals and businesses of digital services both in terms of digital preparedness and in relation to connection infrastructures.

Leaving broadband aside, the most significant technical obstacle to EU-wide OOP implementation remains the heterogeneity of ICT systems and the lack of national interoperability. Nationally implemented technical approaches were reported to be highly heterogeneous as regards infrastructure architectures[229] and technical enablers[230]. The importance of heterogeneity and lack of mutual eID recognition was confirmed by business representatives although it is expected to disappear following the 18/09/2015 adoption of the eIDAS implementing acts.

E. Other

In addition to the above legal, organisational, semantic and technical issues, some other factors affecting the prospects for cross-border OOP should be considered.

Political Will

Interviewees identified *political will* as a necessary condition for OOP implementation: consensus is necessary to support initiatives, to agree specific conditions under which to implement them and to guarantee their sustainability. At national level, political is influenced by previous OOP experience demonstrating benefits for individuals, businesses and/or public administration[231] or by the need to comply with EU policies[232]. Note that the same spillover across levels can happen within countries; in Belgium, impatience with the progress of national OOP progress led Flanders to take its own initiative, which included some advanced features that are now being adopted more generally[233].

On the other hand, bottom-up cross-border OOP implementation can lead to localised disparities. According to the indications provided by the Finnish national representatives, collaboration among public administrations is typically more advanced among neighbour countries for which proximity may generate significant cross-border service demand and more positive attitudes toward cooperation and mutual exchange of information.

To illustrate the influence of EU policy on OOP implementation, Member States are already bound by EU Regulations dealing with specific key factors[234] and common certification or procedures at sectoral level[235]. Both types of Regulation represent significant incentives for Member States to realise EU-wide OOP, in the first case by establishing fundamental conditions for data re-use (associated with national eIDs)

and in the second by establishing a common structure for service provision under which information can be more easily exchanged cross-border. It should be noted that, where implementation of OOP enablers is solely driven by EU Regulatory strictures, 'ownership' and effectiveness of EU-wide initiatives may be limited and implementation protracted.

Quality and fitness for purpose assurance

Conventional documentation requirements assume that specific forms of document meet implicit quality and fitness for purpose requirements. These may be difficult to assess when using information or documentation from other administrations. In other words, there are both perceived and real difficulties in assuring that remotely obtained or certified data are as good as resubmitted data in terms of content, accuracy, reliability, proportionality, etc.

Asymmetric levels of maturity and compliance

Substantial barriers to OOP remain even within Member States and the level of maturity and compliance across Member States varies from "very advanced" to "not existing". To avoid discrimination, a pan-European cross-border OOP implementation may therefore be further hampered to the level of the weakest link or lowest common denominator. Related problems arise when trying to deal efficiently with different levels of readiness for cross-border sharing[236].

Beyond availability and quality of data provided or obtained cross-border, there costs and administrative burdens are likely to be asymmetrically distributed, leading to inefficient or damaging differences in the time needed to formulate and execute data requests and to check and comply with them. In consequence, the start-to-finish time for procedures may be extended for cross-border applicants.

Creeping inaccuracy

There may be longer-term problems of synchronisation and error-correction. In particular, creeping inaccuracy may arise in interconnected data interchange. For instance, suppose a record in country A is shared with countries B and C. If new data arrive in C, there may be no transaction to trigger correction in A and B. Over time, there may be many records about the same business or individual (which are not fully synchronised) and many derivative records (e.g. decisions to grant, withhold or fine-tune services) that embed these inaccuracies[237].

Specifically with regard to personal data, the GDPR attempts to mitigate this risk by placing the following requirements on data controllers[238] (note esp. subsection (d)):

"1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected

for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')."

The practical effect and proportionality of these requirements, especially in a cross border context, have yet to be clarified, and depend on the 'architecture' of OOP implementation; specifically on whether data referents who are natural persons have a unique 'data home'[239] with responsibility for maintaining complete and accurate information, updating these data with new information from authorities throughout the EU and notifying data controllers who have further processed these data under OOP of any changes.

Lack of convincing evidence

There is a further tricky consideration regarding commonly-cited 'reasons' for OOP such as administrative simplification, prevention of fraud, burden reduction, and service improvement. These reasons are not 'owned' by the EC and so cannot on their own provide an adequate case for action in the sense of the Better Regulation Guidelines. However, they may show up as impacts, and can therefore serve as 'drivers' *provided there is evidence that OOP will work to improve them*. As discussed in Section III, a formal Impact Assessment could only include them in the problem statement or as objectives if it could demonstrate that administrative complexity, administrative burdens and deficiencies in service quality:

- are *too high* i.e. could be reduced without any adverse consequences; and
- *would* be reduced by OOP.

But there is at present a lack of reliable evidence relating to either of these.

Of course, OOP *could* reduce burdens in general, but there are burdens associated with OOP implementation as well.

Burdens for public administrations

There are burdens for public administrations that may have to develop new systems to implement OOP and roll them out across their services. Costly elements include:

- Knowing what data exist; this entails creating and operating (or commissioning) search engines for use by service providers and/or data dictionary interfaces for use by 'home countries';
- Creating and running repositories[240] and other databases that can support e-enabled ingress, maintenance and egress/query operations;
- Legal and organisational costs in ensuring that data are unambiguously defined and held, e.g. by 'unique store' provisions or specific rules for identifying and mandating the use of 'authentic data';
- Transforming data to suitable formats (on one or both 'ends') and/or using alternative data sources and types;
- Getting and maintaining consents[241] and protecting personal data, privacy, security and IPR for data or data derivatives transferred to or obtained from other public administrations; and
- Making sure that data updates, erasure and corrections are synchronised across every copy and propagated to past users of those data in case this might trigger a change in decisions regarding eligibility, charging, etc.

Burdens for individuals and businesses

Even the direct beneficiaries of OOP may incur costs and other burdens, whose magnitude varies by circumstance and the implementation route chosen. Under some circumstances, they may outweigh the advantages (to those stakeholders) of having OOP in the first place. However, it is difficult to link cases of net harm or benefit from the kinds of objective factors that can be used to specify OOP policy. Therefore, such costs and burdens must be seen as an uncertain consequence rather than a problem to be addressed by a more selective implementation. They include the following.

- The need (possibly) to inform public authorities that data have already been submitted – and to whom.
- Costs and other burdens associated with checking accuracy, currency and access rights. These exist whenever data are held by data controllers, but become more important when data may be re-used, since resubmitted data can be more easily checked for currency and accuracy. These burdens have a passive form in respect of the need to 'curate' data that are held and might be further processed. They assume a more active and acute form for data that have been retrieved and used to pre-populate forms or automatically[242] used to drive a decision.

Data incompleteness or mismatch

OOP may not provide much net cost or burden reduction – or may even be disadvantageous - if the re-used data don't fully cover what is requested. There are fixed costs of providing data or opting in or out and variable costs of providing a bit more data, so asking for a bit less will not significantly reduce cost or save time. This can be ameliorated if public administrations can be encouraged to modularise their

data requests in order to minimise fixed costs, e.g. by expanding the scope of Base Registries.

Annex VII. OOP and the GDPR

This annex provides a more detailed discussion of the GDPR as it applies to OOP. This discussion is not intended as an authoritative legal analysis.

A. Processing of personal data under the GDPR

Article 6(1) GDPR sets out conditions for the lawful processing of personal data, which are broadly the same as those in the Data Protection Directive (DPD) [243]. It is useful to briefly review these, their relevance to OOP and the extent to which they differ from the conditions laid down in the DPD:

6(1)(a) – Consent of the data subject[244]. Compared to the DPD, GDPR is more restrictive; in particular it seeks to ensure that consent is specific to distinct purposes of processing. This may limit the implementation of OOP to the extent that the purposes for which data are further processed (see discussion of 'further processing below) differ from those for which the data were originally provided. More specifically, data controllers, including public authorities, must inform individuals as to how they will process the individual's data *before* the processing can take place. This obligation existed under the DPD, but more information must be provided, including:

- the legal basis for processing the data (often consent);
- the period for which the data shall be retained;
- the individual's right to complain to the Information Commissioner's Office;
- whether providing the data is required by statute or contract; and
- the consequences of not providing the data.

6(1)(b) – Necessity for performance of a contract with the data subject or steps preparatory to such a contract. This is the same as under the DPD, and may be useful for specific (contracted) services.

6(1)(c) – Necessity for compliance with a legal obligation. The DPD had a similar ground, but Article 6(3) and Recitals 41 and 45 make it clear that the legal obligation in question must be:

- an obligation of Member State or EU law to which the controller is subject; and
- "clear and precise" and its application foreseeable for those subject to it.

The recitals make it clear that the "legal obligation" need not be legislation; common law would be sufficient, if it met the "clear and precise" test. A legal obligation could cover several processing operations so it may not be necessary to establish specific legal obligations for each individual processing activity – but it will (probably) be necessary to apply the test to each data controller for OOP-based

further processing. This is relevant to OOP both in terms of the provision of services that the public authorities are obliged to provide (e.g. to establish eligibility or validate a claim) and in relation to the data controller's legal obligation (under GDPR) to take reasonable steps to ensure that data are accurate, etc.[245].

6(1)(d) – Necessity to protect the vital interests of the data subject or another person when the data subject cannot consent. Recital 46 indicates that where personal data are processed in the vital interests of a person other than the data subject, this ground should be relied on only where no other legal basis is available. This is relevant for OOP transfers that are linked to vital interests, although these are expected to be rare.

6(1)(e) – Necessity for performance of a task carried out in the public interest or the exercise of official authority vested in the controller. According to Article 6(3) and Recital 45, this only applies where the task or authority is laid down in Union law or Member State law to which the controller is subject. This is closely related to the 'legal obligation' justification in 6(1)(c).

6(1)(f) – Necessary for the purposes of legitimate interests[246]. This ground can no longer be relied on by public authorities processing personal data in the exercise of their functions – this considerably restricts the relevance of this justification for OOP purposes. Recitals 47-50 add more detail on what may be considered a "legitimate interest". Member States can introduce specific provisions to provide a basis under Articles 6(1)(c) and 6(1)(e) (legal obligation or performance of a task in the public interest or in the exercise of official authority) for other specific processing situations (e.g. journalism and research). This is likely to result in a degree of variation across the EU. (For further details see section on derogations and special conditions).

B. Consent

Consent is not the only legal basis for processing, but it is particularly important for OOP.

Article 7(1) of the GDPR requires controllers relying on consent to justify processing to be able to demonstrate valid consent by the data subject before the processing. Conditions for valid consent are as follows.

Article 7(2) – consent to processing contained in a written declaration produced by the controller must be distinguishable from other matters in that declaration, intelligible, easily accessible and be in clear and plain language. Recital 42 notes that consent is *informed* only when the data subject is aware of (at least) the identity of the controller and the intended purposes of processing.

Article 7(3) – data subjects must have the right to revoke consent at any time, and it must be as easy to withdraw consent as it is to give it. Withdrawal of consent does not retrospectively invalidate the processing, but the controller must inform data subjects of this before consent is initially given.

Article 7(4) notes that, in cases where the performance of a contract (*including provision of a service)* is conditional on consent to the processing of data that is not *necessary* for that performance, the consent will be presumed not to have been freely given. Recital 43 clarifies this and adds a further circumstance relevant to OOP by noting that consent is presumed not to have been freely given if (despite it being appropriate in the circumstances) there is no provision for separate consent to be given to different processing operations.

C. Further processing

Further processing (which covers most aspects of OOP as applied to personal data) entails the processing of previously submitted data beyond the circumstances governing its original processing. The assessment of the possibility of further processing may require consideration of whether the purpose of further processing is compatible with the purposes for which the data were originally collected. Article 6(4) of the GDPR sets out rules governing the factors a controller must take into account to assess this compatibility. Where processing is not based on consent or Union or Member State law relating to matters specified in Article 23 (e.g. protection of national security or criminal investigations), the following factors should be taken into account in order to determine compatibility:

- any link between the original and proposed new purposes;
- the context in which data were collected (in particular the relationship between subjects and the controller);
- the nature of the data (particularly whether they are sensitive or criminal data);
- possible consequences of the proposed processing; and
- existence of safeguards including encryption or pseudonymisation.

Recital 50 indicates that further processing for archiving in the public interest (as opposed to retention against future OOP requests), scientific and historical research or statistical purposes should be considered as compatible processing[247].

Note as well that if data controllers process (or control the processing of) data for various purposes (as will inevitably happen under OOP), they will need separate consents for each purpose. The GDPR also creates a presumption that bundling consents render them invalid.

Also important to OOP for individuals is the right to demand erasure (sometimes referred to as the Right to be Forgotten); this allows personal data subjects to require their data to be erased if the processing does not satisfy the requirements of the GDPR or if the individual withdraws consent. A public authority acting as data controller who receives such a request must notify anyone with whom the personal data has been shared unless it would be impossible to do so or require disproportionate effort.

D. Data access and portability

Data subjects have the right to know what data are being held that pertain to them. Compared to the DPD, the time limit under the GDPR to respond to subject access requests has been reduced from 40 days to one month. This may impose significant costs on data controller administrations, including the need for organisational changes.

Data controllers now also have to provide data subjects with supplemental information which includes:

- the purpose of the processing;
- the categories of data processed;
- the recipients of the data;
- the envisaged retention period;
- the individual's rights of rectification and erasure;
- the source of the data; and
- any regulated automated decisions made on the basis of the data.

The GDPR also introduces the concept of portability. Subject to various conditions, most notably that the data are processed by automated means, data subjects may request that their data be provided in a commonly used electronic form to enable them to port the data to another provider. This establishes a requirement on data controllers to be able to handle digital OOP requests.

E. Processing of sensitive data

One final point on the legalities of processing personal data concerns what the Article 9(1) of the GDPR calls "sensitive" personal data: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; data concerning health or sex life and sexual orientation; genetic data and biometric data where processed to uniquely identify a person[248]. OOP-relevant grounds for processing sensitive data are narrower[249]:

9(2)(a) - explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law;

9(2)(b) - Necessity for carrying out obligations under employment, social security or social protection law, or a collective agreement;

9(2)(c) – Necessity to protect the vital interests of a data subject who is physically or legally incapable of consent;

9(2)(e) - Data manifestly made public by the data subject;

9(2)(f) – Necessity for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;

9(2)(g) - Necessity for substantial public interest reasons on the basis of Union or Member State law, provided the processing is proportionate to the aim pursued and contains appropriate safeguarding measures;

9(2)(h) – Necessity for preventative or occupational medicine, assessing the working capacity of employees, medical diagnosis, provision of health or social care or treatment or management of health or social care *systems and services* on the basis of Union or Member State law or a contract with a health professional; and

9(2)(i) – Necessity for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.

As regards the latter two grounds, which cover e.g. sharing of health data with social care providers, additional confidentiality requirements are imposed.

There are two special cases that might potentially come within scope of OOP and where national differences are likely to persist. One involves sensitive data; under Article 9(4) Member States can maintain existing conditions or impose new ones (including limitations) on the processing of genetic, biometric or health data. By contrast, data on criminal convictions and offences are not regarded as sensitive under GDPR, though they currently are in some Member States (e.g. the UK's Data Protection Act). In this case, Article 10 of GDPR provides that that such data may only be processed under the control of official authority or where processing is authorised by Union law or Member State law that provides appropriate safeguards.

F. Other affirmative requirements

The GDPR requires public authorities actively to comply with all of its obligations. Among other things, public authorities acting as controllers of personal data must implement:

- data protection by design;
- staff training programmes;
- privacy impact assessments; and
- an audit of all personal data held.

Therefore, for the purposes of OOP for individuals, compliance with the GDPR implicitly delivers many of the necessary building blocks.

Annex VIII. European Interoperability Framework (EIF)

The revised EIF focuses on the delivery of European Public Services. It specifies 11 general interoperability principles[250] that should underlie any development of a European Public Service. Those of most direct relevance include:

- Subsidiarity and proportionality (see Section III);
- Reusability of solutions and information[251], which calls for the sharing to technological and organisational approaches as well as providing a general endorsement for the OOP;
- Openness and transparency, which implies that individuals should have access to and a measure of control over information about them stored by governments, and that individuals and businesses should have a voice in the improvement and design of public services;
- Technological neutrality, which means that any technological constraints or specificities should not be disproportionate or unnecessary for the service and that data should be portable between systems (subject to legal restrictions);
- User-centricity, which specifically calls for OOP
    - 'no wrong door' - multiple channels should be available (linked to the inclusion principle and a constraint on the administrative simplification principle)
    - 'one-stop shop' – points of single contact should be provided to protect users from internal administrative complexity (burden reduction)
    - user feedback should be collected and used to improve services
    - once-only – "As far as possible and in respect of applicable legislation, data should be provided by users only once, and administrations should be able to retrieve and share this data respecting data protection rules[252]"
    - data minimisation or 'relevant-Only' – individuals and businesses should only have to provide information that is necessary to obtain the public service;
- Inclusion and accessibility, which in particular imply that access to services should not be restricted or distorted by channel requirements, and thus relates to the transition from document-based to information-based government services;
- Security and privacy, which means that individuals and businesses should be able to trust public administrations, in particular to comply with any privacy and information security regulations;
- Multilingualism, which in the EIF refers primarily to the language(s) in which European Public Services are made available (rather than the languages in which data are stored and exchanged);
- Administrative simplification, which is connected (but not identical) to burden reduction and to digital-whenever-appropriate and digital-by-default concepts;

- Preservation of information, which means that information should retained for as long as necessary and legally authorised (subject to limits on data retention from privacy and information security regulations). The relevance here is that cross-border OOP means that data retention and access policies may need to be modified to ensure at least minimal alignment of national upper and lower limits[253]; and
- Effectiveness and efficiency, which means that a variety of technological and other approaches should be considered in the design of European Public Services.

Annex IX. Base registries and beyond

There has already been considerable progress in specifying and implementing a system of Base Registries to provide access to certain basic information held in broadly-accessible databases. More formally, the European Interoperability Framework 2.0 defines them as:

"reliable sources of basic information on items such as persons, companies, vehicles, licences, buildings, locations and roads" and "are authentic and authoritative and form, separately or in combination, the cornerstone of public services."

Most countries have systems of Base Registries whose contents, structure and function are clearly codified and often reinforced by law. These systems overlap with identified 'authentic sources' of data in many instances. However, as OOP implementation and eGovernment progress, new base repositories may need to be set up and other databases may need to be OOP-enabled even if they lack the standing of base repositories. Moreover, the often-distinct origins of base repositories have meant that their interconnection and interoperability involved additional costs.

Note, for example, that even in a fairly straightforward area like business registers there was considerable variation among Member States[254] in terms of:

- The structure of national registers - 18 Member States have a single central register, 7 have additional regional or local registers and 2 have only a network of interconnected regional or local registers, without a central register) – this is relevant to OOP in relation to the complexity of connecting multiple structures to provide full coverage, without which the benefits of OOP are diluted;
- The range of entities covered - 23 Member States keep track of entities other than limited liability companies[255], of which branches[256] and European Economic Interest Groupings are perhaps the most relevant to cross-border OOP;
- The information included – all business registers cover the basic information stipulated in Directive 2009/101/EC[257], but others collect additional information[258], which might be required for some public purposes in some countries;
- Forms of identifier – only 12 Member State business registries use unique identifiers, and of those, only 2 use them in the form specified in the Directive (see endnote 259 – and only 4 countries use their unique identifiers for cross-border purposes – which is relevant in view of the agreed importance of common and effectively unique identifiers to locate and gain access to reusable data; and

- Charging structures – most Member State business registries charge for most of the information they hold – which points up the importance of covering information-provision costs for those entities asked to supply information.

This problem is largely being addressed by action at the EU level in line with the implementation of Directive 2012/17/EU[259]. The Business Registers Interconnection System (BRIS[260]) will provide a system for interconnecting business registers at EU level. To understand the relation of the OOP in general in relation to Base Registries, and in particular the possibility of handling data supplied by citizens and businesses drawn in part from or via Base Registries, it is necessary to consider a range of factors applying to an existing or proposed data repository. These include the following[261].

Legal context

Base registries operate within a variety of legal constraints, covering (e.g.) their:

- Legal basis – including the legal standing of their contents and whether they serve as a unique point of storage or retrieval;
- Registry and data access - who is legally permitted: i) access to the registry to add, change, remove, process or export information and ii) who can consult the information in the registry;
- Data quality – in particular the checks that must be performed and the reliability of the data;
- Privacy and confidentiality – from the legal and regulatory perspective;
- Provision for legal review, appeals, etc.;
- Liability for accuracy, timely supply, etc.; and
- Barriers or possibilities regarding cross-border interoperability.

Organisational features

Important organisational aspects of registries include:

- Positioning - how the registry is positioned in relation to the public sector;
- Ownership and control – who operates the registries, who is responsible for and controls their structure and operation, and what objectives, constraints and requirements are placed on them, including whether ownership or control is vested in public bodies (singly or in collaboration), private sector bodies or a combination of the two;
- Organisation of the data within the repository;
- Operational roles and processes;
- Data flow - ingress, processing, modification and egress procedures and controls and monitoring and compliance arrangements (also related to security); and

- Processing – what analyses, syntheses, correlations and aggregations can be performed on the data within the repository, including any master data policy (also related to security).

Semantic aspects

- language(s) supported; and
- syntactic and semantic[262] interoperability.

Technical aspects

- reusability of components or registry software;
- user and system interconnection interface(s); and
- procedures for third party[263] authorisation and authentication.

Security aspects

- Security policy - and its governance;
- Access – who is able to add or modify data (and how is this reflected in metadata), who can make use of the data (directly, via queries or through attestation), who can delete or restrict access; and
- Protections – what measures and restrictions are in place, especially with regard to: collection and updating; track and trace to ensure consistency; privacy (including but not limited to personal data protection and/or data privacy); security (of the registry, its associated hardware, software, protocols and operations); and other rights to control the existence of, access to and uses of the data (e.g. to protect proprietary data, digital rights and industrial property).

Contents

- The data (including 'master' data and authentic sources[264]) they contain: and
- Meta-data, which may include such elements as format(s), provenance[265], consents given or other legal basis for processing[266], purposes for which they can be used (and by whom), reliability, legal standing and history of access, modification and other transactions.
- Coverage: typically, Base Registries do not hold a broad spectrum of data, but are specialised by data type[267] or purpose[268].

We note that the Base Registry metaphor covers a wide range of possible models, structures and procedures, and that it is not the only possible approach for obtaining reusable data without unduly burdening data referents. For instance, the same data can be maintained and supplied when needed by automated systems controlled by third parties or data referents themselves.

These characteristics must be considered together; for instance, the formal definition of a Base Registry refers explicitly to the concept of "authentic data," but does not in itself require a Base Registry to be the unique place where specific data

can be found, or from which data must be obtained in order to have legal standing equivalent to newly-submitted data. Note also that not all data requested by public administrations can be considered 'basic' or have the legal standing necessary for inclusion in Base Registries.

On the other hand, many of the data requested by public administrations in cross-border settings do not meet the conditions necessary for the creation of a Base Registry. Some are not basic data, but rather derivative products (such as the 'good conduct' certifications produced by services like the UK Disclosure and Barring Service[269]). Others involve a range of alternative data[270] with a variety of forms, formats, contents, levels of quality, etc. or may involve continuous or frequent additions and/or highly sensitive data[271]. In addition, some data cannot be properly used unless they are 'contextualised' with a range of other information, which works against the need for clear and unambiguous definitions, fairly simple access and inspection rules and clear responsibility for data quality, authenticity, integrity and other characteristics as provided by Base Registries. Therefore, some data are suitable for inclusion in Base Registries while other data can be held in repositories that adapt solutions and good practices developed for Base Registries or can use platforms and services provided for interconnected Base Registries.

Moving forward with a Base Registry Approach

The proactive encouragement option for OOP implementation involves the consolidation of a network of base Registries to provide authoritative 'data homes' for some kinds of data and to supply as a by-product, OOP-related infrastructures, models and services. Basic principles can be found in the Annex "Base Registry Approach".

This section lists basic principles that can be applied to construction of a suitable framework, concrete steps to set up the network and elements necessary to place it on a sound legal footing.

Note that the revised EIF describes the Base Register approach in detail and makes a series of specific recommendations consistent with those made here[272].

A. Basic principles

Each Member State will have a network of Base Registries, interconnected in conformity with the EIF:

- Each collects the information that it needs to use for its 'own' processes;
- Each excludes data that *must* be obtained from other registries (i.e. may not be collected again);

- Where necessary data are not (or are only partially) present in another Base Registry, supplemental data may be collected, but must be added to the data mapping or catalogue and placed (homed) in the single most appropriate register; and
- There should be a master data map showing authoritative sources, data model, quality, and responsibility for all data elements, available in all Base Registries – this will of necessity entail the catalogue of Base Registries specified for Option 2 (p. 28).

B. Concrete steps to establish the network

- A system of 'OOP services' should be established to:
    - Manage, interpret and fill requests;
    - Report changes or inaccuracies and to ensure that master records are updated;
    - Manage subscriptions by entities that run registries, contribute data, and/or seek access on a 'pull' (request or query) or 'push' (notification of changes) basis; and
    - Run mapping or data catalogue, translation and interoperability
        - OOP implies that data are re-used – it is vital for L.O.S.T. reasons that their meaning, quality, context of collection and use, access conditions, etc. are unambiguously and transparently established in a data model, fiche or catalogue. For cross-border situations, there may be different 'home' and 'local' versions, but the differences must be unambiguous and openly documented
        - A mapping system can be used to locate necessary data (including alternative sources of authentic information).
- The construction of a Base Registry network entails the following:
        - Existing registries should be used where appropriate, with minimal change to existing processes and organisation;
        - Existing registries can be used to define new Base Registries; and
        - When the context in which data are collected and managed differs from the data referent's context (service requested), the information layer and the service layer must be distinct and (for the case of personal data) aligned with the provisions on compatible purposes in Article 6(4) of the GDPR.
- Responsibilities (These requirements apply to business and personal data; for personal data some of these rights and responsibilities are laid down in the GDPR – see Annex III)
    - Data requestors and OOP service users are responsible for the suitability of the data they collect and use:

        - OOP service users need data catalogue, data quality and other OOP services to determine suitability;
        - within a given country, these are maintained by the data controller, but the data requestor is responsibility for their use and application; and
        - especially cross- border, unavailability of these services will not release them from liability for data that have been further processed, but will release them from their OOP obligations to reuse data unless the data referent authorises or knowingly consents after having been informed.
    - Data referents are responsible for the accuracy and currency of records held about them[273]:
        - they must have access to their data and ideally past access requests and contexts;
        - they also have the right to demand correction (where justified and authenticated); and
        - they may have rights of erasure and/or to opt out of OOP.
    - Data controllers (register controllers and operators) must
        - maintain and make available OOP services (possibly supplied by third parties);
        - maintain and make available data catalogues and mapping for their country's uses; and
        - Maintain and make available data catalogue/mapping services pertaining to other countries' holdings of data of similar content, context and application.

C. Place the base registries on a sound legal footing

Even though the *proactive support* option refers to action primarily at EU level, it cannot succeed without complementary legislative arrangements at Member State level. In particular, the construction and empowerment of the registry system requires legislation to:

- Define Base Registries for important domains;
- Establish each OOP registry in law;
- Define for each the legal basis, mandatory and optional data, responsibility, scope of data use, etc. (as discussed above); and
- Respect 12 principles[274]:
    1. Sound, complete and unambiguous legal basis,
    2. Responsibility of data referents/service claimants (citizen and business) to report inaccuracies,
    3. Use of available and appropriate data should be obligatory for the whole government,

4. Liabilities for data governance and those arising from further processing of data must be clear,
5. The financial basis for the system must be adequate, consistent with overall financial regulations and Departmental responsibilities and free of adverse incentives,
6. The content, purposes and scope of all data must be clear,
7. Explicit and public agreements and procedures should govern relations among register holders, suppliers and users of data,
8. Access to registers – including data sharing between Base Registers - must be controlled by clear procedures, with unambiguous roles and responsibilities and in conformity to relevant data protection and information security regulations,
9. Data quality should be explicitly defined and subject to strict rules and clear responsibility,
10. Decisions regarding the register require agreement or binding involvement of (national) data users,
11. The position of the register in the system and coherence with other registers should be clear and appropriate to the duties and competence of the register controller and
12. There should be an identified public administration entity in charge of each Base Register, and ministerial responsibility for implementation and functioning.

D. An example: Authentic Registers

A candidate set of principles and characteristics can be produced by adapting the structure specified in e.g. the Netherlands' Cadastre Act[275]. As applied to Base Register data, the relevant characteristics of 'authentic registers' are:

1) Transparent legislation
   a) The register is governed by law: The various registers, maps and auxiliary data products and services can be regulated by specific legislation, typically as an elaboration of the Civil Code in civil law countries.
   b) Users are obliged to notify the owner of the register of any errors or shortcomings – the legislation may requires that all changes to registers, maps and other 'public' documents are open to public inspection and appeal.
   c) Use of authentic registers is mandatory for the entire government apparatus: This is compulsory in many cases (for example by the notaries for their deeds, land consolidation projects, building permits, expropriation procedures).

d) Liability issues are rendered explicit: The Cadastre Act makes the Agency liable for mistakes.

2) Transparent finances
   a) The implementation and operations are subject to controls ensuring reasonable costs (i.e. not liable for prohibitively or disproportionately expensive provision of services to other jurisdictions or efforts to correct records and notify those who have used them in the past of changes)
   b) There should be explicit specifications of the apportionment of the costs including cost benefit bookkeeping and audit approval and public accountability through annual reports and annual accounts.
3) Explicit content and structure
   a) The content and scope of registers should be declared explicitly: the implementing legislation should define the exact purpose(s) and contents of registers and associated data products and services.
   b) Quality indicators may be left out of the legislation (being subject to negotiation and change) and instead developed by the responsible Agency within the quality management system under auspices of a User Council – which may include cross-border users.
4) Explicit responsibilities and procedures
   a) Exhaustive agreements and procedures should be drawn up for the owner(s) of register(s) and data suppliers and users of the data. They should include: terms under which registration takes place; how information is distributed; rights to determine use and governance for contents; etc. This should be (for avoidance of uncertainty) described in primary legislation and secondary regulations. In addition, all users of electronic services should sign contract covering technical specifications and user/use restrictions. Tailor-made products should always be provided under contract.
   b) Explicit procedures should be drawn up for access to (ingress, query, and egress) the authentic register and regulated in the primary legislation. In addition, the responsible Agency (and User Council) may develop and deploy innovative channels of distribution and derivative products.
   c) Stringent quality-assurance arrangements should be in place including (as relevant) ISO certification and quality management of annual planning and control cycles.

d) Specifications should require some form of involvement of data users in decision-making about the register.

5) Part of the system

a) Each authentic register should occupy an explicitly-described position within a system of authentic registers (to cope with ‘unique storage’ requirements and to allow suitable data collection (few-stop-shop) servicing of frequent or related requests for overlapping data).

b) Control of an authentic register rests with an administrative body under ministerial responsibility for implementation and operation: The Agency – which may be an 'independent public body' or ‘public corporation’ – will have administrative authority to control the register.

Annex X. OOP-related measures

A. EU Regulatory and legislative measures

Legislation offers the advantages of legal compulsion, clarity and elimination of ambiguity or inconsistency in interpretation. It also provides a strong signal of political will and intent and an implicit assurance of commitment, given the time and resources required to change or modify laws and the interdependence among all the laws of a country or region. Moreover, compared to other forms of intervention, legislation has invariably gone through a more extensive, detailed and transparent scrutiny process, combining stakeholder consultation and formal impact assessment with legal, technical and other forms of analysis.

The potential drawbacks of the legislative approach overlap with its advantages; it is difficult to reverse, even in the face of evidence that it should be redrafted[276]. Beyond that, the illegality of departures from mandatory provisions may serve to censor data relating to possible improvements. A further drawback, which is often noted in relation to ICT-specific laws, arises as an indirect consequence of the formal and slow nature of the legal process; laws may not accurately reflect technological or operational realities and as a result may not be future-proof or exhibit the right level and kind of technological or service neutrality. Finally, law enforcement sanctions do not always provide the right incentives and may be difficult credibly to enforce on public administrations.

Nonetheless, *formal law* has played an important role at Member State level. In the Belgian case, elements of OOP included in a range of federal laws did provoke or enable specific initiatives but did not induce adequate support and follow-up overall, which led the authorities to enact a dedicated 'Only Once' law[277] that (*inter alia*) mandated use of unique identification keys (or codes) for all services, simplification of (federal) mandatory government procedures and forms, and the equivalence for administrative purposes of documentary and electronic data and in doing so reinforced the use of authentic data sources.

Subsidiarity limits the power of the EU to impose conditions on Member State governments' processes for handling data associated with public services to individuals and businesses. This is discussed further in Section III.

Within the scope of legislative tools, we distinguish European *Regulation*, which takes direct effect across the EU in precisely the form adopted by Council and Parliament following a Proposal by the European Commission, and *Directives*, which are adopted in national law by different Member States in a manner consistent with national legislation following the adoption of the Commission's proposal by

Council and Parliament. If the case for common and consistent action is strong enough, then Regulation may be the appropriate course. Typically, it would involve delegation of monitoring and enforcement to a regulator; given that the overwhelming preponderance of service applicants are likely to come from within a country, this is likely to be a national regulatory agency (NRA). The specific choice of NRA will depend on the nature of the rule.

Regulation could be used in several ways, including:

- Mandating *interconnection*[278] of specific types of Base Registry or authoritative data source;
- Compelling Member State governments to implement and use (at least permissively) a common European electronic Identity interoperability platform (e.g. STORK);
- Imposing conditions under which documentary and electronic records are equivalent; or
- Defining a range of services and contexts for which Member States are obligated to first consult existing records before requiring individuals or businesses to submit data.

Alternatively, OOP provisions could be incorporated into existing sector- or service-specific European legislation that imposes information reporting requirements. This approach may be preferred in relation to existing Directives in case national implementation has led to differences in approach that create cross-border failures of OOP.

Absent specific EU-level provision of services, it does not seem likely that such Regulations could only be applied to cross-border requests, as opposed to being uniformly imposed regardless of country of origin or request. Therefore, they should be seen as enforcing OOP throughout Europe, and not just at cross-border level.

Of course, not all regulatory activity involves additional rules. Deregulation and regulatory forbearance are also possible tools associated with legislation. For example, a Regulatory requirement might be recast in functional terms in order to allow a variety of approaches, or to create a rebuttable presumption that a particular approach might be used. This has some potential limitations as a means of establishing a common EU-wide approach to OOP *practices* (since it allows greater scope for national difference – but does help to encourage innovation and the creation of a common evidence base on the effectiveness, efficiency, costs and benefits of different approaches.

Unlike pure pilot activities, this kind of compulsory experimentation is not subject to selection bias. By strengthening the evidence base and encouraging cross-border

experimentation, this approach may be seen as strengthening the prospects for OOP as a common principle even if common OOP practice is delayed or diluted.

Such forbearance (which does not mean revision of legislation) may be particularly useful in relation to 'wicked' problems like privacy and security, where existing Regulations may not function as expected[279]. Another variant of forbearance might be a Regulation - under the Better Regulation framework - requiring Member States to identify informational, filing and reporting requirements that are particularly burdensome to small and micro businesses and to exercise their mitigation powers by implementing OOP for such firms[280]. This would complementing the existing commitment to exempt such enterprises from regulation in general where this can be done without compromising the objectives of the regulation, and could be defended on the grounds that such businesses may be more sensitive to the burdens of repeated data provisions than larger corporations, especially in cross-border contexts.

On the other hand, some aspects of OOP may be better handled by European Directives, especially in light of existing national measures to address service provision, re-use of public data, authentic sources, etc., the existence of differentiated practices of Member State-level and below OOP implementation and the different levels of 'OOP-readiness' of the Member States. Identifying the full extent of such Directives and analysing the complex linkages between explicit OOP provisions and the objectives of the Directives is beyond the scope of this report, but it is worth drawing attention to the ways in which such modifications might be implemented, prospectively and retrospectively and at EU and Member State level. Note that these are not legislative measures per se but proposed changes to the mechanisms for assessing and adjusting legislative measures.

At EU level, the primary vehicle is the Commission's Better Regulation Programme[281]. This seeks to ensure that action at EU level is (among other things) open, transparent, participatory, necessary, appropriate, effective and efficient. To this end, it has developed a range of ex ante and ex post measures for assessing potential or existing activities. Retrospectively, this centres on the programme of Regulatory Fitness and Performance (REFIT) assessments[282], which seek to simplify and reduce the costs of regulation. These assessments are carried out (following an explicit roadmap) on an issue basis (i.e. all acts pertaining to a specific topic) rather than a measure by measure basis, which encourages consideration of duplications, overlaps and inconsistencies (potentially including duplicate requirements on regulated parties). In this context, OOP-readiness could be incorporated among the criteria used in REFIT assessments.

Prospectively. OOP considerations could be incorporated into the Better Regulation toolkit, which lays out the steps and procedures involved in conducting Impact Assessments. The toolkit already includes specific guidance[283] urging Commission staff to take information-related economic impacts on businesses and public administrations into account in several ways, e.g.:

- Operating costs – "Will it impose additional adjustment, compliance or transaction costs on businesses?"
- Administrative burdens on businesses – "Does it affect the nature of information obligations placed on businesses (for example, the type of data required, reporting frequency, and the complexity of submission process)?"
- Position of SMEs – "What is the impact of identified additional costs and burdens on the operation and competitiveness of SMEs and micro SMEs in particular?"
- Public authorities – "Does it bring additional governmental administrative burden?"

We note, in passing, that the Guidelines do not provide equal prominence to administrative burdens falling on individuals, except tacitly to the extent that they affect access to services[284]. From this, two suggestions follow:

- Administrative costs and other burdens to individuals stemming from information requirements should be explicitly incorporated among the economic impacts to be assessed, and considered in relation to societal impacts to the extent that they are likely to distort access to and use of public services;
- Information-related costs should be placed on an opportunity cost footing by taking into account the existence of other public administration databases containing the same or equivalent data.

Many Member States have analogous requirements for prospective Impact Assessments of significant measures[285], and some have independent bodies charged with scrutinising draft Impact Assessments. In view of the complementarity between EU-level (cross-border and pan-European) and Member State-level action on OOP (in particular, the importance of the latter for the feasibility of the former), consideration of the potential for OOP should be encouraged at Member State level as well, both via the EC Guidelines and through coordination among the scrutiny bodies[286]; holistic (issue- rather than measure-based) retrospective assessment is somewhat more haphazard, and probably does not (yet) provide a platform for enhancing the legal status of OOP at a fundamental level.

Another measure would potentially be a dedicated Directive that makes provision for delegated regulation to adapt or evolve the legal framework in the face of new technical, economic and service developments, or in relation to new information exchange linkages. This, however, would be a far-reaching proposal that is (based

on interviews with national representatives and domain experts) likely to encounter strong resistance.

B. Joint action and coordination measures

- Working and coordination groups
- Information and good practice exchange

C. Standards and frameworks

- Technical and operational standards
- Frameworks (interoperability, interconnection, access)

D. Direct interventions

There are a range of potential direct actions that could be undertaken at EC level. These include continuation and expansion of the existing pilot, structured natural experiments (e.g. using 'living lab' and/or CAPs methods). They also include demand-side measures such as incorporating OOP into public procurement procedures and more specifically in using 'innovation procurement' to obtain new OOP solutions and providing data users or data providers in public administrations (for whom the costs of OOP compliance are not compensated by a reduction in ongoing costs) with 'top-up' subsidies to cover certain costs. On the supply-side, measures can include direct OOP service provision (Option 4) and TTP or information brokerage. Finally, European institutions can work together to provide suitable evaluation tools, data collection and evidence and analyses of burden reduction associated with OOP.

E. Research and innovation support

R&I support measures may include technical explorations and empirical studies of the actual and potential impacts of OOP on the extent and consequences of cross-border service access and on the nature of within-country data use and service architectures.

F. Establishing shared or interconnected Base Registries for OOP purposes

Base registry data are already collected in clear and common formats and equipped with tools for curation, access, etc. As mentioned above, some instances of interconnection of Base Registries on a common platform are already well advanced (e.g. ECRIS, and EUCARIS) and more are foreseen (e.g. BRIS, scheduled to 'go live' in June 2017), especially under Action 1.2 of the ISA^2 programme[287]. There

is thus scope for extending and unifying these approaches. Table 15 summarises some existing projects or initiatives for federating Base Registries at EU level.

Table 15: Base Registry interconnection at EU level[288]

Subject	Initiatives	Remarks
Business registries	Business Registries Interconnection System (BRIS)	Combines Member State business registers, a service-based platform (European Central Platform) and portal (European e-Justice Portal) to allow for the cross-border search for company information via a unified multilingual interface. BRIS will also enable EU business registers to exchange information in relation to foreign branches and cross-border mergers of companies.
	Business Registry Interoperability Throughout Europe (BRITE)	A (completed) project funded by the EU under the 6th Framework Programme, which intended to set up an ICT service platform for register-to-register communications. The project ran from 2006 to 2009. It is cited as evidence of the long history of work in this area.
	European Business Register (EBR)	A network allowing searches across registers – this is a private sector initiative of multiple business registers, with a commercial orientation, that competes with other resellers of such data; we cite it purely as an example of a relevant, non-government initiative.

Subject	Initiatives	Remarks
Personal	Insolvency registries	The European e-Justice Portal provides access via a multilingual search facility to 7 interconnected insolvency registers (SI, CZ, NL, DE, AT, EE and RO) and unfederated access to the insolvency registers (where they exist) and records of the other Member States. Further to Regulation 2015/848 all Member States will have to interconnect their registers via the e-Justice Portal by 2019.
	European Civil Registry Network (ECRN)	Births, deaths, marriages, divorces; grew from a pilot project.
	European Criminal Records Information System (ECRIS)	AA secure network interconnecting the Member States' registries of criminal records (primarily convictions).).
	Information Service on European Residents (RISER)	Started as eTEN project; private company offering public clients access to names, addresses (and age) from electoral roles and official registers.
Land	European Land Registry Association (ELRA)	NFP offering legal support and follow-up to land registries – not directly OOP-relevant, though it does offer cross-border services.
	European Land Information Service (EuLIS)	Consortium of Member States selling land registry information to private clients. Currently has full live connection to registries in AT, ES, IE, LV, NL and SW; partial or no connection to 16 further member countries, partial connections to 2 non-members and 10 further countries. See http://eulis.eu/.

Subject	Initiatives	Remarks
	Land Registers Interconnection (LRI)_ system	A voluntary interconnection project, implemented by the Commission, aiming at the interconnection of Member State land information systems via the European e-Justice Portal.

Considering these different approaches, it is safe to say that the structured interconnection of existing Base Registries and the establishment of conditions for new ones to join are more prevalent than the formation of unified EU-level databases holding original data.

The reasons are many, and include the desire of Member States to retain control over their data, processes and procedures and the resulting clarity of lines of responsibility and accountability.

Looking to the future, it is possible that new Base Registries will be created or the types of data contained in them will change. From the OOP perspective, it is reasonable to regard Base Registries as a special case of public sector data repositories, bound by particular rules and served by a set of initiatives that facilitate OOP implementation by: providing examples of good practice, especially as regards cross-border access to publicly-operated data repositories; supplying platforms, applications and 'services' that can be directly used to interconnect or provide simplified access to other databases; and by providing a mechanism through which data can be shared. For the moment, we note that from the perspective of this project, a number of issues might arise that affect the willingness of Member States to participate in different ways. These, in turn, give rise to alternative approaches for 'joining up' Base Registries. The issues include the following.

- There may be national resistance to the transfer of control implied by transfer of data (even via 'mirroring') to an EC-controlled comprehensive database. Even if the costs of such transfers are minimised (e.g. by accepting data in native formats, contents, etc. there needs to be a strong justification for asking Member States to provide other Member States with access to data that the originating state does not control (except for public Base Registries).
- MS may not wish to bear the cost and time burdens of translating their stored data to common data format, access, organisation, etc. models.
- There may be potential liability e.g. if data from the originating Member State leads to claims in another for obtaining services for which the individual or business wasn't eligible (especially if the data model, data standards, purposes

for which the data are used or the conditions attached are not the same in the receiving state) or if the originating Member State is unable to verify third party compliance with its own data protection, security, etc. rules.

- Responsibility for accuracy, timeliness and notification of changes should lie with a designated controller of the authentic source of the data – in most cases, this will be the originating Member State. This can limit the risk of discrepancies between information provided on behalf of an individual or business (e.g. under the "Once-Only" principle) across borders and within the Member State. For some data this may be problematic if there is no transactional reason for the originating Member State to update the data. For example, an expat EU citizen may not be interacting with his native databases to record e.g. births and marriages[289]. For a business selling throughout Europe under the VAT MOSS rules, threshold rules may mean that the Member State where they sell need data that would not normally be recorded in their native country.
- For individuals and businesses with extensive cross-border activity, the data 'home' may not be easy to identify e.g. if an entity from one country generates new basic data while in another. In such cases, reconciling even the basic data may be costly, risky and separated from the service-request activities that normally lead to original records. The problem would of course be eased – but not eliminated - by the existence of a single European set of identifiers[290].

Among the measures that might favour the adoption of such a structure are the following.

- A common platform for use by all countries. This could be defined independently of data specifics – in other words, a platform providing a range of search, access, permission and other services to all Base Registries on the basis of declared and explicit data models. Alternatively, the platform could be defined in a manner specific to a particular type of data (e.g. business registry, insolvency, demographic/personal, geographic or transport-related data); this would be particularly appropriate where such platforms already exist or where the data are subject to particular constraints, legal rules or national or industry sensitivities.
- 'Pecking order' rules to establish priorities among different databases, with an associated subsidiarity[291] provision to ensure that the 'most authentic' data are provided in a transparent manner from the highest-priority database.
- A peer-to-peer model of connection between different platforms, with minimal standards to ensure interoperability, perhaps including agreement on a common interchange format specifying the data that can be requested and processes in each Member State for producing and responding to such requests.
- Legal provisions to enable public authorities to comply with data requests and to use responses in a manner equivalent to their own stored or user-supplied data.

- Adoption and exploitation of the semantic interoperability solutions being created by the ISA[2] programme[292] and other EC initiatives[293], possibly extended as far as the creation of a common semantic layer dedicated to exchanges of basic data among Member States.
- Multilingual and semantically-interoperable services that can be 'attached' to existing repositories and platforms or provided as a separable service.
- A *limited* mirror registry that collects and reconciles Base Registry data most likely to be of use in cross-border situations and where such transfers are justified by subsidiarity and proportionality (data that would result in a reduced burden and greater accuracy if obtained from the original Member State). The qualification has 3 reasons:
    - If Base Registry data cover part, but not much, of the data requested by the foreign government, there may be little savings in getting them from the home Member State, though this is offset by the ability to use authentic(ated) data;
    - If the number of requests is likely to be very small, the fixed costs may not be easy to justify; and
    - If the Member States involved have made little common progress in implementing the EIF (little progress or progress on different elements), the costs may outweigh the benefits.
- A *comprehensive* metadata catalogue[294] that collects or links information on the models and other aspects (see Annex X.F) of national Base Registries of specific data types in native formats, allowing foreign Member States to request the necessary data or certifications themselves on a bilateral basis.;
- A federating search and retrieval infrastructure under the EIF (in line with the EIF ambition of alignment of national and European IF's).

G. Establishing structures for sharing non-basic data

Some data of relevance for European OOP are *__not__* base data when first provided, but may become 'basic' for people or firms engaged in extensive cross-border activities. In much the same way, some services that are demanded or provided cross-border may become European Public Services as the level of demand or the sensitivities of recipients to costs and burdens increase.

This may be a matter of cost only –

- There is little justification for building a big data interface, negotiating and implementing sharing arrangements and adjusting protocols for data that are not going to be re-used often, or for which the aggregate savings to individuals or businesses falls short of new burdens to public administrations.
- A less laudable aspect and one that might in itself justify EU intervention, arises where OOP adoption reduces *overall* burden (aggregating over both foreign and native countries and the businesses or individuals concerned), but increases

specific burdens on one or two parties. Put simply, if OOP benefits Country A and cross-border beneficiaries, that may not be enough to induce country B do its part in implementation unless it is compensated e.g. by fees, or reciprocal benefits or EC subsidy (possibly in kind).

It may be a matter of functional convenience –

- Implementing a Base Registry structure and access provisions for a given set of data may make it easier or cheaper to adding more (if fixed costs exceed incremental costs);
- If the scale and scope of a database expand then enhancing privacy, security, processing, access, etc. controls becomes more efficient and practical; and
- If a database accumulates a useful *mix* of data or more coherent and useful access, search and mapping structures, public authorities might prefer to use that registry in place of other sources of (possibly different) data.
- Taking these into account, Options 3 and 4 could usefully focus on initial implementations and actions that help to 'build out' the OOP network into more services, more data types, etc. Along the way, some of the burdens can be eased:
    - For example, concrete measures taken to give effect to the GDPR's requirements for data protection by design and by default[295] may become clearer (e.g. as regards the operational meaning of "minimising the processing of personal data" in cross-border OOP settings) and more acceptable as the range of data and data access requirements evolves;
    - It may also happen that security, data protection and privacy can be addressed by the same solutions at system level

Finally, as the understanding, acceptance and implementation of OOP progress, some data, data types and/or functionalities may be removed from the scope of the principle – this means that some base data may become non-basic, rather than the other way round. This fits with data minimisation and purpose limitation principles, but goes beyond them in the direction of 'solving' the 'Nordic block' because it encourages public administrations to reconsider what data they collect and what purposes they use them for. A the moment, for example, lots of data are demanded that are not needed for the purpose, because a) they used to be necessary but the world has moved on (e.g. name and address, and phone number, when a unique identifier and/or personal IP address may be all that is needed) or b) they may be useful for some other purpose (this could be a defensible data mining or analytics purpose, or a fraud check that is no longer necessary, etc.)

In addition to implementing suitable search and data catalogue (or data dictionary) methodologies according to agreed definitions, there is scope, especially in relation to non-basic data and use for a variety of services to employ 'deep neural nets' and other forms of machine learning. This can reduce sensitive dependence and barriers

associated with the need to adopt a common ontology or to implement fixed 'translation services' that inhibit evolution towards better data use and exchange and may fail to recognise changing requirements and patterns of use and respond accordingly.

These measures are not limited to handling idiosyncratic or unstable data, or data of specialised interest. They also go beyond the Base Registry framework in involving:

- Different access forms e.g. to allow third parties to submit attestation queries rather than get data access, to modify or correct data and to ensure that such modifications are propagated to others who have used or will use these data;
- Mixed and variable forms of ownership, control and operation – including the possibility of multiple data sources and multiple service or functionality bundles; and
- Requirements to obligate public authorities to consider using different data (held by others) to achieve the same purpose.

H. Dynamic implementation

To each option is associated a 'glide path' or implementation trajectory in order to

- Set targets, learn from experience, and adjust so that costs and benefits are optimised
- Build communities of practice to build awareness and readiness, collect experiences, experiment with alternatives and mobilise support on a peer-to-peer basis
- Allow time and space for developing effective and efficient burden- cost- and responsibility-sharing arrangements
- Adapt to changing circumstances, by moving to or away from coercive, shared, interconnected etc. options as appropriate, knowing that both technological potential and societal need will continue to change;
- Spread disruptions and costs over time (this is essentially a 'real option' approach; if there is learning about OOP implementation, it makes sense to delay part of its implementation and to then expand, adjust, abandon or wait longer depending on how it plays out).

I. Infrastructural services and framework condition improvements

These measures include hosting and running Base Registries (in line with measures outlined in Annex X.F), hosting and running reference databases of non-base data (in line with measures outlines in Annex X.G), providing stand-alone data and query federation and search services, etc. and taking other steps to implement the

building blocks and improve the framework conditions identified in Annex VI Gaps and Barriers.

In principle, such databases could serve two useful functions:

- Providing legally acceptable proof of identity[296], including a link to a unique identifier or multiple identifiers needed to share data in Member State databases[297];
- Certifying services attesting to the presence or absence of the individual or business from one of a range of databases in order to establish their eligibility for specific benefits, services, jobs, etc.

An *identity database* could allow individuals or businesses to certify their identity without the difficulties created by rules requiring specific forms of documentary proof. Especially for persons, such databases are likely to be limited to national level in the medium term, with cross-border access provided through intergovernmental agreement. Proposals have been made for such databases based around e.g. biometric information[298]. They could provide a useful intermediary service to individuals or businesses seeking to authenticate themselves on eGovernment portals as well, even in the absence of a universal system of unique EU-level identifiers. More concretely, the eIDAS Regulation[299] laid the foundation for an EU wide eID system under which Member States:

- *May* 'notify' the European Commission of 'national' electronic identification scheme(s) used at home for access to public services;
- *Must* recognise and accept 'notified' eIDs of other Member States for cross-border access to its public services requiring e-identification;
- *Must* provide a capability for online free eID authentication;
- *Is liable* for unambiguous identification and authentication; and
- *May* allow the private sector to use 'notified' eIDs.

But the Regulation does *not* oblige Member States to have an eID scheme or to notify (and thus open up) the schemes that they have. The eID, even when 'notified' is not equivalent to an ID card and does not constitute a European eID except in the limited sense described above. The Regulation makes *no* provision for an EU database and its protections and conditions are only applicable to 'official' eIDs. Other elements remain to be finalised; technical standards, security arrangements, (multiple) quality levels, governance and international alignment.

Specifically as regards cross-border interactions, the Regulation does not oblige Member States to use identifiers linked to eID schemes in other Member States for internal purposes; therefore, cross-border individual or business service applicants might be obliged to obtain a 'local' eID, which would then be linked to their 'home'

identifier in order to ensure that use of the 'local' eID would provide access to information stored in the 'home' country.

Further proposals and a working instance have been provided by the two pilots of the Secure idenTity acrOss boRders linked (Stork) project[300], which emphasised interconnection of national eID infrastructures through common interfaces and stressed user control, explicit consent, transparency and privacy-awareness.

A (positive or negative) *certifying database or service* could be based on the structured interconnection of EU-level and Member State databases. Generally, EU-level databases are used to provide access to statistical data, information on rules and requirements and other information above the individual level of aggregation. But there are individual EU-level (purpose-limited) databases for a range of crime, migration and security data, such as:

- Individuals and property of interest to Schengen countries (SIS II)[301];
- Fingerprints of asylum seekers and irregular border-crossers (EURODAC);
- Visa applications by individuals seeking to enter the Schengen area (VIS); and
- An EU-level (centralised) adjunct to the federated criminal records system (ECRIS) for third-party nationals (ECRIS-TCN).
- Of course, such databases have entirely different legal bases compared to the standard service-access purposes envisaged for OOP implementation, but there are some overlaps. For instance, such databases are increasingly used to provide certification of eligibility for work and benefits[302], qualification to engage in specific business activities[303] or fitness to take employment involving working with children or adults[304]. Presence on databases maintained for these purposes certifies the absence of adverse records on law enforcement and related databases.
- This suggests that there may be a case for additional EU-level databases that could be used for general identification or certification purposes. However, the mere possibility that such data might be useful in a cross-border context does not justify the creation of such a database, especially as it gives rise to the risk that data in the central store might not be sufficiently authentic or authoritative for all purposes.
- At this level of generality, it is not obvious who would control and operate such databases; the ownership and control of the examples above mainly rests with DG Migration and Home Affairs and is underpinned by dedicated Regulations.

Annex XI. Terms of Reference for OOP Task force

To get the best from national and European OOP-related initiatives and optimise long term development, a Task Force should be set up that embraces the principles above and takes responsibility for aligning national and European level activities. It should be formed from relevant national authorities and agencies and consult 'lay representatives' from business and civil society to sustain 'ownership' by Member States and those affected by their activities.

The terms of reference of such a body should call on members to:

- Share experience and learn from practice;
- Coordinate future initiatives:
    - establishment of priorities and a road map for Member State and cross-border OOP implementation;
    - Identify legally reliable objectives for further and wider OOP implementation, which might include:
        - Reducing (cost, time and complexity) burdens on citizens and businesses;
        - Improving the cost-effectiveness of government services;
        - Fraud prevention;
        - Effective government; and
        - Efficient and equitable Single Market functioning (including jobs and growth).
    - Identify and agree a minimal sufficient set of platforms and organisation for interoperability;
    - define and implement a measurement or observatory exercise – in conjunction with Better Regulation – to track the costs, benefits and other impacts of OOP strategy
- Serve as a deliberative body to clarify issues arising.

As a starting point for the work of the task force, we offer the following two tasks:

First task of the Task Force: Set out principles for OOP implementation

It is important to clarify principles at the start, to ensure alignment and credibility. Based on our study findings we suggest to embrace the following key principles:

A. Embrace incremental federalism and prioritise business applications

The consensus view of government stakeholders is it may be best to work towards OOP in an incremental fashion, building on current experience and using explicit business case and business case development. This applies to both citizen- and business-facing OOP implementations, but the near-term priority lies with business applications, due to the existence of substantial common (hard and soft) infrastructure, the tangibility of benefits, the greater quantitative significance and lower service diversity of cross-border business-government interactions and the relatively lower hurdles in terms of privacy regulations. The path forward should aim at developing a framework that facilitates effective *federated* progress by providing suitable platforms and interoperability at all levels.

B. Ensure user-centrism as the norm

As noted above, building and sustaining momentum requires a shift from administrative to user-centred government and from a reliance on documentation to the information currently (and optionally) contained in those documents. User-centrism extends beyond the specification and delivery of services to include the design of 'user interfaces' that allow a business or individual to employ any single point of contact (the 'No wrong door' principle) to submit information needed for many functions (the 'Whole government' principle).

C. Move fully to information instead of document processing for administrative services

Most administrations have been moving towards data storing and sharing within their administrations, yet still today there is some legislation or administration rules that require documents rather than the information they contain. This is a major barrier that is mostly a remainder from old times than a necessity.

In addition to the three key principles above the following principles could be considered:

a. Businesses and individuals: All reusable data should have a data catalogue covering their contents, provenance, legal reliability, quality, validity and attached consents.
b. Businesses and individuals: Administrations providing European Public Services should only ask for information that was not previously submitted, has expired or lacks appropriate consents.

c. Businesses and individuals: Where possible, data should be taken from unique authentic authoritative sources.
d. Businesses and individuals: [Whole government principle] Especially where providing information may be burdensome (e.g. reporting deaths), government should proactively provide 'one-stop-shop' services to ensure that all relevant services and offices are informed and have taken appropriate action after they are first notified.
e. Individuals: must have the right to refuse to give information available from public administration sources, and to exercise all applicable data protection rights (e.g. access and correction) with respect to personal data obtained from government sources.
f. Individuals: To reinforce data protection rights, further processing (including query-based interrogation of databases and certification) should be recorded and used to ensure that data requestors are made aware of any significant changes.

Second task for the Task Force: Develop a Roadmap for Intervention

This can be approached from the perspective of specific elements of OOP implementation. An approach starting from pre-defined data elements is explicitly foreseen in the eGovernment Action Plan. In step 1 such elements would be collected and shared following the EIF. Step 2 would extend this to all data (again within EIF guidelines). Step 3 would use these data to populate forms or as a direct input into automated processes.

Depending on circumstances, the shared and automated aspect could use a 'light touch' process, supplemented by more detailed data as necessary, along the lines implemented in the Virtual Company Dossier and other 'pre-qualification' evidence, ideally in line with shifting from documents to data and negotiating the 'least common denominator' aspects of such forms.

More generally, implementation should be kept as non-specific and open as possible, to allow room for innovation and experimentation and to avoid ruling anything out or precluding alternatives that might be acceptable and beneficial or yield additional relevant data. Variants already available include pre-populated forms vs. forms where already available or unnecessary elements were greyed out.

Annex XII. Scenario impact analysis

All options must take account of critical uncertainties e.g. current state and trends of Member State OOP, critical framework conditions, requirements for and advantages of specific OOP options and the impact of Member State OOP experiences for other countries and at European level. To reflect these, we describe a limited number of possible futures ((future scenarios), based on two major uncertainties:

I. Macroeconomic impacts on supply of and demand for cross-border mobility.

This encompasses three possibilities:

- Favourable: mobility in search of new opportunities, realising comparative advantages[305], productivity gains and eventually[306] easing public service burden;
- Negative: mobility away from countries experiencing greatest difficulties and towards advanced Member States, increasing demand for support while reducing tax revenues, commercial margins and societal and economic cohesion within and between Member States; and
- [possibly] Structural change: Union cohesion gives way to regional blocs with internal but not interregional mobility.

II. Interaction between Member State and European OOP-related developments.

National OOP implementation can both hinder and facilitate European OOP. This underlies subsidiarity; whether the EU has competence to mandate or drive OOP. It depends in turn on how successful or disappointing national experiences affect the willingness of Member States to cooperate in different types of OOP: hierarchically structured vs. decentralised; general vs. sector- and functionality- specific; and localised vs. standardised in technical, semantic and legal terms. Two polar possibilities in this dimension are:

- Positive feedback: even different Member State OOP implementations create a common appreciation of benefits that justifies overcoming the resulting legal, organisational, semantic and technical barriers.
- Negative feedback: differentiated forms of OOP create interoperability barriers between countries and among services or public administrations.

Note that removing barriers to European OOP may not always be justified by the resulting form of European OOP or its contributions to Single Market objectives. If European OOP is *ipso facto* good or if its adverse effects can be compensated leaving a net gain, barriers should be removed, minimised or routed around. But a barrier is also a stimulus to further improvement.

For instance, if Member States collect very different information for a given purpose, barriers to OOP implementation may lead them to a minimal and common alternative that meets the needs of cross-border service provision. Moreover, European OOP may not be the only or the best way to achieve legitimate societal objectives. A 'light-touch' approach allowing small groups of Member States to agree OOP-like data interchange arrangements for the most-requested services may achieve greater cost and burden reduction or service improvement than a global approach[307].

The possibilities can be recapitulated as follows:

Table 16: Scenario Dimensions

Dimension	Alternatives
Macroeconomic outcomes	Favourable – mobility to positive opportunities; comparative advantage, productivity, eased public service burden. Negative – mobility from difficulties to advanced Member States; increased support demand, dwindling tax revenues, commercial margins, social and economic cohesion[308]. Structural change – formation of regional 'blocs' that share economic and societal flows, but resist cross-bloc interaction.
OOP development at Member State and European level	Positive feedback - different implementations create common appreciation that justifies overcoming LOST barriers. Crowding out (negative feedback) - differentiated OOP creates LOST barriers among countries, services, administrations.

Not all possibilities relevant or consistent. The policy options will play out in a future that is not fixed. Considering the most relevant combinations (scenarios) lets us check the robustness of the options and whether the choice of approach should be delayed until more information is available; it may need to change as the uncertainties are resolved or require complementary actions to hedge against risks.

The logic behind the selection of these scenarios is as follows. In a favourable macroeconomic climate, either positive feedback leading to broad acceptance of cross-border OOP (scenario I) or crowding-out leading to OOP in some Member States but weaknesses at European level (scenario II) are possible. Unfavourable macro conditions and austerity pressures may favour a common solution (scenario IIIa) or weakened cohesion (scenario IIIb). For present purposes, the differences between IIIb and II are minor; we do not further analyse IIIb. Under structural change, positive feedback is unlikely; there will not be enough financial and political resources and generalised austerity postures will themselves undermine convergence.

We regard the unshaded scenarios in Table 17 as logically consistent and relevant.

Table 17: Future Scenarios

Macroeconomic\ MS/EU	Positive feedback	Crowding-out
Favourable	I. *Growing together* better services, shrinking State burden, user-centred core standardised services	*II. Peaceful co-existence* services improve, burdens fall, efficiency and uniformity incentives are too weak for convergence
	Austerity Europe	
	IIIa. 'Lifeboat solidarity' Economic pressures drive cross-border activity	Economic pressure is too steep, OOP a limited option in the most necessary areas
Structural change	Structural change conditions will undermine positive feedback	*IV. Regional OOP* Formation of virtual blocs, asymmetric cross-border activity, OOP provided only to the most significant flows, reinforcing separation

Below we consider all 4 policy options against these 4 future scenarios. This discussion was used to provide the summary impacts depicted in Table 10.

A. Growing together scenario

The Growing Together scenario is shaped by a favourable macroeconomic outlook and a positive feedback between OOP developments at Member State and EU level. Personal and business mobility are likely to rise, leading to greater cross-border service demand on an equivalent footing to 'local' applicants. Due to the favourable economic climate, cross-border services are likely to be associated with productive mobility (where benefits outweigh (opportunity) costs for all parties). This enhances acceptability for OOP-related measures; home and destination countries are likely to see clearly the net benefits of mobility, which will be viewed as a way to improve the 'match' between specific individual and business requirements and capabilities and the comparative advantages offered by different countries and thereby increasing the effective scope and competitive health of the Single Market.

1. Baseline option

Overall, this option provides only moderate OOP development. Costs to government are likely to be lower than with other options and the current variability in provision across countries is likely to persist.

OOP development will favour business-orientated services, which are already being extended across data (e.g. establishment and insolvency data) and services (e.g. starting a business or branch, employment and payments and participation in public procurement). Progress will be greatest within national borders, due to the high priority attached to burden reduction that can convincingly be linked to economic growth. Cross border OOP for businesses will be slowed by existing differences especially in legal and organisational terms. Thanks to existing EU initiatives and the business focus of the pending large-scale OOP pilot, cross-border and pan-European progress for business will proceed together, with some existing bilateral solutions being diffused on a much wider basis.

Impacts for individuals will be muted in the near- to medium-term. Within national borders, progress will be retarded by: the high sensitivity (and lack of faith in government data stewardship) surrounding much potentially reusable personal data; document-orientated personal services; and the use of non-basic data. As a consequence, services will still require active participation by claimants, limiting cost and time savings. The same factors will restrain bilateral or cross-border progress; demand may increase, but the partial OOP provision available may not greatly reduce the costs or beginning-to-end time needed. On the other hand, EU level progress (e.g. CEF building blocks and associated DSIs) and the entry into force of the GDPR will help drive savings from pan-European provision (i.e. specific data and services addressed by EU action).

Impacts on government are mixed. The 'G1' entities in Table 10 must provide information to the 'G2' entities on behalf of individuals and businesses. They experience little direct return from the OOP agenda, except where they are already obliged to share information and benefit from streamlining processes[309]. There will be little impact for existing domestic exchanges and investment and operational costs and increased workload associated with cross-border and pan-European OOP requests. For requesting (G2) entities, burdens will be offset by cost savings, simplification, more accurate and reliable decisions and reduced fraud in proportion to volume: highest within country and lowest for full pan-European, since few countries will wish to institute measures automatically to collect data from all other MS rather than those from whom they experience significant demand and those countries at a corresponding or higher level of maturity.

2. Legislative approach option

Overall, this option offers the greatest uniformity of progress and (under the baseline scenario) convergence. Initial legislative delay will be followed by rapid implementation and reciprocal national progress. This is the most costly option, in view of legal costs and delay and the resulting uniformity, which may inhibit cost-saving derogation and variation as the world evolves.

Businesses and individuals are likely to find this option most attractive under the Growing Together scenario; greater legal certainty and uniformity will reduce mobility costs and allow those most in need of services to receive them in a timely and equitable fashion - within-country, bilaterally and across Europe. Compared to Option 0, the sound and comprehensive legal framework will be of greatest benefit to businesses seeking cross-border and especially pan-European opportunities; in the short run this will be driven by administrative burden reduction, but eventually distorting differences between business services and regulations will dwindle. In the same way, enhanced personal mobility will help harmonise services and government processes over the medium term.

Domestic (G1) government entities will experience net (transitional and ongoing) costs, especially as demand increases. This will be strongest at cross-border level for personal services; the increased variety of individual circumstances will complicate eligibility decisions, personalisation and service provision. Receiving (G2) entities are likely to see net benefits from accelerated acceptance of OOP[310].

Both types of public administration will have to adjust and align national legislation, and spend time and money on: familiarisation and creation of legally-required capacities and facilities; and on changes in procedure for controllers of master data, those who request and seek to use those data, arm's length 'OOP service' providers and other impacts of adjusting national legislation and service provision.

3. Proactive encouragement option

This provides slightly slower progress towards pan-European OOP than the legislative approach, since legal changes are more modest and the timetable is less prescribed, at least in the near term. Eventually, proactive encouragement may lead under the favourable conditions of this scenario (particularly positive feedback) to convergence to a more efficient and effective harmonised approach, with more national, data type and/or service differences. Compared to the legislative approach costs are likely to be lower, though reduced standardisation may add complexity or interoperability costs.

Businesses applying for multiple services within their home countries will see benefits equivalent to those under options 0 and 1; the primary differences concern cross-border interactions. There, business benefits are likely to lie between Options 0 and 1 due to the lack of consistent uniformity and full legal reliability and slower consolidation.

Individuals should find lower costs and faster processes. Difficulties will persist for lower-priority or unusual services, but should be modest assuming progress in implementing EU-level building blocks.

Lack of compulsion means that data suppliers (G1) will see little adverse cost or time impact (compared to other options, costs will be lower and offset by 'nudge' progress towards better evidence, common platforms, expanded critical mass and transition to low-cost, high-efficiency data-based government. Data requestors (G2) will see greater net benefits; this Option helps them streamline obligatory (public-facing) procedures (whereas the extra duties of G1 entities fall outside their current obligations). This is a direct result of the option's objectives to progress along lines of greatest benefit, improve evidence capture and use, stimulate voluntary and mutual OOP platform services and encourage convergence and transition to data-based government.

4. Responsive Assistance option

This provides the slowest, cheapest and least uniform OOP implementation. Like Option 2 it emphasises gradual search and convergence to an efficient, effective and appropriately-harmonised European approach, compared to the uniformity of Option 1 or the divergences of Option 0.

Businesses in their home jurisdictions are likely to see slightly lower burdens. These may fall short of benefits expected under Option 0; European engagement with this option is likely in the short run to focus on areas of greatest perceived need (individuals and cross-border businesses). Businesses operating in multiple countries will see costs and delays fall, but lack of short-run uniformity will raise familiarisation costs, especially compared Option 1. Sectors or business transactions prioritised by Member States will get greater and faster support, locking in existing asymmetries.

Individuals in their home countries will face a situation similar to proactive encouragement (option 2); both address issues of reconciling data protection with OOP within the competence and internal operations of Member State governments). Individuals will see little cross-border change; countries that attach high priority to specific cross-border requests will already have made progress. But

at pan-European level there is a risk (not a certainty) that EU-level support may crowd out some local action.

This is country-led; as with Option 2, there will be little impact on data suppliers (G1). Data requestors should face lower set-up costs for cross-border and (especially) pan-European OOP transactions.

B. Peaceful coexistence scenario

The most important difference between Growing Together and Peaceful Coexistence is the tension between the EU and Member States. EU-level action is more likely to crowd out than to supplement or align Member State measures. The most significant anticipated differences are discussed below.

1. Baseline option

There will be virtually no change for businesses. Individuals will see stagnation at pan-European level; limited local cross-border measures will be retained rather than extended. Governments will face difficulty in re-using or transposing EC-level measures if they compete with local measures; the resulting wider variety of requests may increase costs even for within-country OOP. On the other hand, costs of providing for pan-European OOP may fall relative to Growing Together if levels of demand fall and because pan-European development is constrained to build explicitly on what has gone before in the different Member States. However, these changes are mainly confined to the G1 side.

2. Legislative approach option

Without positive feedback between Member State and EU OOP initiatives, reductions in administrative burden will be lower across the board. This will partially reflect reduced cross-border demand, but also persistence of multiple systems and replacement of pre-filled forms with burdensome 'check and authorise' procedures. Governments (G1 and G2) may face a changed variety and volume of requests. Also, Member State legal measures (see page 197) may be different. The legislative approach option faces political conditions that sustain today's legal and organisational barriers. But it is difficult to assess the extent of such changes and the degree to which local differences will impose extra costs on G1 or G2 entities.

3. Proactive encouragement option

Option 2 depends for its effectiveness on willing cooperation among Member States and between the EC and the Member States. It may be less effective in the Peaceful Coexistence scenario, where government operational solidarity and

cohesion may be less extensive. This may in turn reduce business and individual benefits, especially at pan-European level, where it will still be necessary to become familiar with many processes in order to request services and in deciding how much, which kind and what format of information to provide and to whom. Data suppliers will be in the same position as under Growing Together, since building blocks already in place allow them to respond to requests from multiple Member States. The same is true of data requestors except for pan-European OOP; e.g. current arrangements allow individual Member States considerable leeway to decide whether to adopt eID, but oblige them to recognise notified and conformant schemes used by other countries.

4. Responsive Assistance option

Option 3 is relatively unaffected by weak feedback between Member State and EU OOP development. The main changes will come at pan-European level for individuals; countries may prioritise their own citizens and those of Member States with whom they have frequent and significant interactions. This may eliminate the crowding noted above, though data requestors will still have to manage multiple systems. On balance Peaceful Coexistence will be slightly better for individuals in respect of pan-European OOP and slightly worse OPEX for data requestors.

C. Lifeboat solidarity scenario

The defining feature of this scenario is an unfavourable macroeconomic climate that increases pressure on governments to save money, reduces perceived returns to public services for businesses and individuals from other Member States[311] and weakens Member State political will level for further progress on cross-border OOP.

1. Baseline option

Business under this scenario will have more need of cross-border OOP and thus greater benefits. Administrative burdens may not fall, but returns to foreign opportunities will rise. Increased focus on local interests will drive domestic OOP for citizens, but weaken conversion of EU building blocks into fully-interchangeable national systems; locational independence may also fall. Serving domestic requests is likely to become more costly as the shadow cost of government funds and demand both increase. But reduced pressure for pan-European OOP will produce some offsetting economies.

2. Legislative approach option

Austerity under lifeboat solidarity will reduce the priority attached by business to cross border OOP-enabling of services relative to other public assistance in meeting economic challenges. Benefits from Legislative approach measures will taper off,

though they will not disappear if businesses need to operate across more borders[312]. Individuals' benefits may dwindle further, reflecting changed needs for public services and the small additional cost of supplying needed information. For data suppliers the costs of servicing requests relating to individuals and businesses abroad are partially offset by the reduced need to provide analogous services at home and repatriated tax revenues, but compliance with legislative requirements may be seen as disproportionate in a climate of falling revenues, rising public expenditure demands and general administrative austerity.

3. Proactive encouragement option

For businesses, the ability to operate cross-border will become more important; the benefits of cross-border OOP will rise, further magnified by the increased frequency of such mobility. This will not extend to pan-European level; few businesses will respond to the economic situation by expanding to this scale and the 'co-regulatory' benefits of Proactive encouragement are unlikely to scale. The benefits pan-European service access for individuals will fall relative to other scenarios due to the infrequency, minor cost and time savings and lesser relevance of pan-European as compared to cross-border or within-country OOP. For G1 entities, the main impact is increased domestic demand, which is costly to address even without the higher opportunity cost of resources. For this scenario, Option 2 lacks the uniformity and reliability of Option 1, but is more constrained by EU intervention, which is likely to face considerable political and organisational resistance (especially for data requestors).

4. Responsive Assistance option

Businesses will feel the impact of this option's greater fragmentation and localisation in cross-border and pan-European contexts, where the benefits of matching local circumstances are more than outweighed by the need to deal with multiple 'burden-reducing' measures. Individuals will feel little domestic benefit from external good practices or common structures. There are, however, indirect benefits from the interaction of economic circumstances with the responsive EU policy stance via horizontal provision of 'OOP services' (see page 196). We do not expect significant impacts on government entities; this differentiates this option from alternatives involving more EU leadership.

D. Regional OOP scenario

The most important determinant of policy impacts under this scenario is the pattern of regional linkages that will evolve as the solidarity of the Single Market erodes. Of particular importance will be homophily (a tendency for similar countries to associate) and the kind of similarity involved. The State of Play assessment

suggests that economic proximity, legal structure, organisational culture, linguistic/semantic similarities and technological maturity and approach are especially important.

One might expect the most closely linked countries to share service demand characteristics, data coverage and quality and OOP maturity. However; reciprocity may arise among countries with highly asymmetric flows[313], given a mutual interest in reducing administrative burdens cross-border.

These linkages and cross-border demand patterns will strengthen in this scenario as regionalisation proceeds. Some specific costs may be higher for heterogeneous linkages (e.g. data requestors in countries with high OOP and data-driven eGovernment maturity may face higher cost and time burdens when implementing OOP with a data supplier counterparty in a less-mature country,

Finally, both for businesses and individuals, geography will play an important role. As with other transport costs, this may affect the attractiveness of moving or setting up a business in one or another region, but we do not expect this significantly to affect the decomposition into OOP-regions.

Thus, only the legislative approach will show OOP benefits at pan-European level in this scenario.

1. Baseline option

Regionalisation will obviously reduce the business benefits of OOP in all cross border contexts. Within a Member State, data suppliers may experience increased demand compared to the Growing Together scenario if regionalisation leads individuals and businesses to move to regional neighbours.

2. Legislative approach option

Devising and implementing legislative measures at EU level may be protracted, costly and ultimately less comprehensive in the presence of regional blocs aligned on OOP, especially true for individuals (if mutual trust is insufficient to produce EU-wide legal guarantees). Finally, governments requesting data from outside their 'regions' are likely to face increased delays and possibly costs.

3. Proactive encouragement option

Except for the reduced benefits for all parties at pan-European level, regionalisation is unlikely to change proactive encouragement impacts due to its permissive and non-coercive nature.

4. Responsive Assistance option

Under this option, EU support will follow regional agendas. Intraregional cross border interactions will benefit relative to the baseline, especially for individuals. The 'uplift' caused by good practice and knowledge transfer from regional neighbours should allow countries in advanced regions to help each other[314]; data requestors' investment and operational costs will fall even within-country.

Annex XIII. End notes

Please find below all notes to the report.

---

[1] "Conclusions of the European Council (24/25 October 2013)" at: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf, esp. Par. 9 on page 4.

[2] Data can be obtained in the following ways: Volunteered by subjects; Created through interactions; Linked from other sources; Elicited by targeted means (e.g. forms or dynamically-posed questions); Observed via surveillance; or: Derived from observations by analytics, modelling or other processing.

[3] Data are collected by Public administrations for a number of purposes: personalise services; determine eligibility; prevent fraud; feed predictive models (of the individual (e.g. taxes) or the population (e.g. demand forecasting for resourcing and business planning); provide evidence of service level, quality and other characteristics for accountability; support 'back-office' functions (settlement for cross-border services, SLA monitoring); identify and correct errors, inconsistency and out of date information; anticipate future service needs; target 'marketing' (outreach, information); analyse the population seeking services and relate it to the potentially-eligible pool to determine adverse selection, need, etc. (segmentation analysis); and provide appropriate continuity of service.

[4] Some cases can be found in the SWD and national analyses of the burden of fragmented VAT reporting rules.

[5] Consolidated version of the Treaty on the Functioning of the European Union, Article 26 – Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

[6] Administrative burden reduction is closely associated with the opportunities generated by digital tools. Implementation of online public administration portals and online identification tools, together with the growing digital literacy of governments, businesses and individuals alike provide baseline conditions that encourage tackling administrative burdens though digital strategies. Common approaches to reduce administrative burdens include: <1>Integration of eGovernment tools; <2> "Smart" use of information provided to public administration by individuals and businesses (i.e. individuals and business), and <3> Implementation of "Once-Only" data re-use principles for some data and functionalities.

[7] Some of the services within scope of this study are limited to citizens, but many are not, and the protections of the GDPR are not limited to EU citizens (indeed, the word does not appear in the Regulation). Therefore, we use the more inclusive term 'individual' where no confusion is likely to arise.

[8] Enormous amounts of data can now be collected, transferred, analysed and used with relative ease. Consequently, it is increasingly argued that in order to maximise the hidden potential of those data legislative burdens on those who control or process data should be lightened. This affects both individuals and businesses, but also administrations themselves. At the same time, and in particular relevant for individuals, the EU has remained steadfast in its insistence that an individual's right to control their own personal data must be preserved – in consequence, there is some tension between the goal of lightening legislative

and regulatory burdens on one side and preserving personal data protection in a changing world.

[9] generally according to standard procedures that treat all applicants the same way, including the proliferation (for some data) of different records, referring to the same person or business but held in different places and used for different purposes; and the evolution and deployment of systems for managing and using information that differ across administrations and countries, and which may not be fully homogeneous and interoperable across the EU.

[10] Note that the GDPR has replaced the DPD, but that many Member State laws and codes still reflect the earlier legislation. Some of the significant differences are discussed below in Section 2.

[11] This follow the European Interoperability Framework (EIF) classification; see e.g. "Security and data protection measures in the Context of Once-only and reuse of existing data approaches" EUPAN HRWG/IPSG Meeting, October 2015. Available at: http://www.eupan.eu/files/repository/20151021170531_(09)_Security_&_data_protection_measures_-_Joint_Session_-_Plenary_Session_-_EUPAN_HRWG_IPSG_Meeting_-_Luxembourg_-_2015.pdf.

[12] An interesting project to keep in mind is the ISA project titled Catalogue of Services. In this project a common data model was defined: the Core Public Service Vocabulary – Application Profile (CPSV-AP). This is a common way of describing services. The situation right now is that even within the MS, the public administrations offering public services have no idea which services are being offered by different administrations. That's why many are creating catalogues of services. However in order to be able to create such catalogues, you need a common way to describe these services. That's where the CPSV-AP comes in. This model can be adopted natively (as Estonia and Italy are doing) or be used to map between different data models. See https://joinup.ec.europa.eu/asset/cpsv-ap/description or http://ec.europa.eu/isa/actions/01-trusted-information-exchange/1-3action_en.htm.

[13] e.g. fair and lawful processing, purpose limitation, data adequacy and minimisation, responsibility for ensuring data accuracy, minimising data retention and maintaining subject rights. These rights include: access (what data are held and processed, who else has access, copies of data and sources, reasoning behind decisions based on the data, etc.); objecting to distressing or damaging processing (including further processing of data) or direct marketing (even by governments); correction; and compensation.

[14] The Whole Government and No Wrong Door principles are key eGovernment features in e.g. Canada (http://publications.gc.ca/collections/Collection/P4-1-2006E.pdf), the UK (esp. in the "Tell Us Once" service), Finland and the Netherlands (see e.g. OECD (2015), OECD Public Governance Reviews: Estonia and Finland: Fostering Strategic Capacity across Governments and Digital Services across Borders, OECD Public Governance Reviews, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264229334-en.

[15] As is the case in Estonia.

[16] This applies, for instance, to the UK's "Tell us once" service, which collects data relating to deaths from relatives (through a range of interfaces and offices). The responsible office ensures that the data are spread to and recorded by all concerned offices and that appropriate actions are taken.

[17] Study conducted for the Luxembourg Presidency of the European Council, available at: http://www.eupan.eu/files/repository/20151209104842_Presentation_-_CTIE_Study_'Security_and_data_protection_measures'_-_Luxembourg_Presidency_2015.pdf.

[18] *Subsidiarity* requires EU decisions to be taken as closely as possible to the affected parties. The EU should not act unless this would be more effective than action at national level. *Proportionality* limits EU actions to what is necessary to achieve agreed policy objectives; the EU should choose actions that leave the greatest possible freedom to Member States. Here, this means that EU action is justified for overcoming OOP-related differences that lead to discrimination and/or plausibly imperil the (Digital) Single Market.

[19] See endnote 17.

[20] "Better regulation for better results - An EU agenda" COM(2015) 215 at: http://ec.europa.eu/smart-regulation/better_regulation/documents/com_2015_215_en.pdf.

[21] "Ministerial Declaration on eGovernment" at: https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf.

[22] "EU eGovernment Action Plan 2016-2020: Accelerating the digital transformation of government" at: http://ec.europa.eu/isa/library/documents/eu-egovernment-action-plan-2016-2020_en.pdf.

[23] See endnote 1.

[24] For instance, the eGovernment Action Plan defines the OOP thus (emphasis added): "Once-Only principle: public administrations should ensure that citizens and businesses supply the same information only once to **a public administration**. Public administration offices take action if permitted to internally re-use this data, in due respect of data protection rules, so that no additional burden falls on citizens and businesses." Cross-border OOP involves multiple public administrations.

[25] For personal data the public authority acts as a data controller under the GDPR.

[26] Article 6(4) of the GDPR discusses compatible purposes.

[27] The discussion in Annex III expands these and considers the extent to which they differ from the conditions laid down in the DPD.

[28] See discussion in endnote 244.

[29] See esp. Annex VII.C.

[30] This includes: legal basis (often consent); retention period; right to complain; whether data provision is required by statute or contract; and consequences of not providing the data. See also endnote 36.

[31] A legal obligation could cover multiple processing operations; it may not be necessary to establish specific legal obligations for each operation but it is necessary to apply the test to each controller. This applies to services that public authorities must provide and to their legal obligation (under GDPR) to take reasonable steps to ensure that data are accurate, etc. See "Creeping inaccuracy" in Section VII.E.

[32] Or another person when the data subject cannot consent, but Recital 46 indicates that this ground for processing personal data in the vital interests of a person other than the data subject should be relied on only where no other legal basis is available. This may apply to health data, but see page 13.

[33] OOP-relevant examples include processing for fraud prevention (Recital 47) and transmission of personal data for internal administrative purposes, including client and employee data, but *this justification is not available to public authorities*.

[34] e.g. protection of national security or criminal investigations.

[35] Article 49(1) allows *data transfers* based on "compelling legitimate interests" that are *not repetitive*, relate to a limited number of data subjects and where the controller has assessed and ensured adequacy. However, this justification is ruled out for public authorities and can in any case only be used when the controller cannot rely on any other method of ensuring adequacy, including model clauses, BCRs, approved contracts and all derogations from Article 49(1)(a)-(f).The controller would also need to notify the supervisory authority that it was relying on this ground for transfer.

[36] The required information includes: the purpose of the processing; categories of data processed; recipients of the data; retention period; rights of rectification and erasure; data source; and any regulated automated decisions made on the basis of the data.

[37] Article 9(1) et. seq.

[38] Racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; data concerning health or sex life and sexual orientation; genetic data and biometric data where processed to uniquely identify a person. Interestingly, processing of photographs – which have previously been regarded as sensitive in some Member States – is not automatically 'caught' unless used for unique identification or authentication as a biometric.

[39] For an analysis, see: http://www.ippr.org/files/publications/pdf/self-employment-Europe_Jan2015.pdf?noredirect=1.

[40] Note in particular that under the GDPR, personal data expressly includes online identifiers, device identifiers, cookie IDs and IP addresses.

[41] Discrimination on the grounds of nationality has been illegal under EU law since the Union's founding treaty was signed in Rome in 1957. This has effect on bilateral intra-European arrangements that would favour individuals and businesses of one country above individuals and businesses of other EU Member States.

[42] Note that Directive 2012/17/EU mandates interconnection of business registers.

[43] Note that the CEF eID-based solution provides an EU-wide platform for this.

[44] See endnote 299.

[45] E.g. by ensuring – through legal, organisational, semantic and technical adjustments - that data and information – especially in electronic form – have the same legal status as documents.

[46] Meaning that data collected in real-time were analysed periodically or after specific incidents.

[47] Examples include enabling patients to: adjust their own dosages (under specified conditions); use the data when seeking advice from other providers or fellow patients; and to manage their engagement with providers to ensure appropriate continuity of care. A related (non-medical) example is the use of 'quantified self' monitoring data to enable workers to adjust their work patterns or negotiate with employers to reduce workplace stress and thus to mitigate its health and other consequences.

[48] No further action is literally impossible; extant policies and rules foresee periodic review and adjustment.

[49] For more information, see http://ec.europa.eu/isa/isa2/index_en.htm - see also Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.i

[50] GDPR will take full effect on 25 May 2018 after a two-year transition period for adaptation of existing national laws and practices. It may take more years to "settle" as technological possibilities and ways of using data change, as the DPD "bedded in" through the Art29 WP up to 20 years after entry into force. The eIDAS Regulation entered into force on June 2014; its trust services provisions applied directly in the Member States from July 2016 and mandatory recognition of eIDs will apply directly from September 2018.

[51] EC (2014) "Study on eGovernment and the reduction of administrative burdens", available at: https://ec.europa.eu/digital-single-market/en/news/final-report-study-egovernment-and-reduction-administrative-burden-smart-20120061

[52] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home.

[53] The five identified building blocks are: eDelivery, eSignature, eInvoicing, eID, eTranslation.

[54] The list of enablers reported in this paragraph corresponds to the one used in the D2 *State of the Art* in the chapter "OOP barriers and enablers".

[55] For example, some countries require data provided to governments to be stored in a single location, which affects the extent of re-use and the methods by which they can be shared.

[56] Existing initiatives (especially in 'lead countries' like Estonia, Finland, Belgium and the Netherlands) have already changed the control of data resources: increased interconnection and centralisation at national level; 'dashboard' facilities for data referents; and bilateral cross-border development and permissive use of common platforms and data models. Initiatives that combine the one-government principle with OOP have led the lead office to offer services subject to (paid) internal service level agreements.

[57] This encourages different public agencies to coordinate across boundaries to provide an integrated response to service management and delivery. Examples include the UK's Tell Us Once service (provided both to individuals and across Government Departments) and portal services for business registration.

[58] Especially under the EIF, but also including procurement reforms.

[59] This option takes as given the existence of data in multiple as well as centralised repositories and thus the need for interconnection and interoperability frameworks and measures.

[60] An 'opt-in' approach might be regarded as less burdensome, but might also limit the applicability of OOP and create additional administrative burdens.

[61] Note that the question of where to place responsibility for this meta-catalogue remains open.

[62] Note that the Connecting Europe Facility (CEF) has developed a range of Building Blocks, which provide basic capabilities that can be used by any European project to facilitate cross-border delivery of digital public services (including eID). The eIDAS Regulation now compels Member States to reuse eIDAS-compliant Digital Service Infrastructures created using these Building Blocks.

[63] Including e.g. Business Registry data, but also the areas addressed by IDA large scale pilots such as e-Health, e-Identification, e-Justice and e-Procurement.

[64] Further details on these requirements can be found in the revised EIF draft (see endnote 135).

[65] As detailed in the revised EIF draft.

[66] Optionally, this may involve pre-populated forms, tailored offerings or reduced information requests. These choices will affect impacts, but should probably be left to local discretion.

[67] See e.g. the UK's statutory data sharing code of practice: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf. A non-statutory alternative is provided in Option 2 below.

[68] As used here, proactive encouragement includes the softer end of the self- and co-regulation 'Beaufort scale' developed by Cave and Marsden (Cave, J., C. Marsden, and S. Simmons, (2008) Options for and Effectiveness of Internet Self- and Co-Regulation. RAND Europe. Retrieved at: http://ec.europa.eu/dg/information_society/evaluation/data/pdf/studies/2006_05/phase2.pdf). See also Senden, L. A. (2005). Soft law, self-regulation and co-regulation in European law: where do they meet? Available at SSRN 943063.

[69] For personal data, the GDPR provides for industry-led approved codes of conduct and certification. Enforcement of EU data protection rules is undertaken by national data protection supervisory authorities, and (for the EU institutions) by the EDPS. We use 'codes' in a general sense that may include 'non-governmental' arrangements that limit the need for further processing by public authority while retaining the operational and substantive advantages of OOP (e.g. data in privately-owned business registries).

[70] See endnote 135 for revised EIF reference and general recommendations; even more specific recommendations in different areas dealing with base registries and data exchange in can be found in ISA Actions such as Access to Base Registries (e.g. Good Practices) or SEMIC. Existing tools suitable for reuse include e.g. the Core Vocabularies.

[71] Seven Member States will notify by the end of 2016, a further 6 intend to do so by the end of 2017 or later, 6 more have signalled their intent to notify but have not set a date and a further 3 are considering whether to notify their schemes. Between 29/9/2015 and 28/9/2018, cross-border recognition of notified schemes is voluntary, after which it will become mandatory.

[72] COM(2016)288: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0288

[73] COM(2016)288, p. 11.

[74] These are discussed in more detail in D2 and D3; they include e.g. the X-Road platform in Estonia and Finland for businesses and the UK's "Tell Us Once" service for individuals.

[75] Higher compliance with local initiatives reflects greater 'ownership' and alignment; it also helps to clarify and provide evidence for beneficial impacts and complementary adaptations.

[76] The greater flexibility and organisational proximity of the stakeholders in this option make it easier to discover and negotiate mutually beneficial changes compared to formal and harmonised approaches, and allow cost- and responsibility-sharing arrangements to eliminate barriers in one place that are – in aggregate - offset by benefits elsewhere. See e.g. Atkinson, M., Wilkin, A., Stott, A., Doherty, P. and Kinder, K., 2001. Multi-agency working: A detailed study. Local Government Association.

[77] Where formal limits on reuse of solutions developed at local level are not maintained (due to agency costs or in order to foster innovation), the scope of the activity may be extended beyond the domain for which it was originally designed without revisiting the case for action.

[78] The subject matter and the bodies could be chosen in line with guidelines for evaluating and implementing self- and co-regulatory solutions. See e.g. the Better Regulation Guidelines or Cave, J., C. Marsden, and S. Simmons. Phase 3 (Final) Report Options for and Effectiveness of Internet Self-and Co-Regulation. TR-566, RAND Corp: Santa Monica, CA, 2008.

[79] Covering semantic, technical and organisational interoperability, interconnection, federation (see footnote 6), data management, etc.

[80] e.g. registers of information, databases of OOP implementation and monitoring data covering performance at country level and especially cross-border as needed to verify compliance and (informally) discourage non-compliant behaviour.

[81] In other words, adherence to applicable codes and standards for information exchange and registry interconnection should be stipulated in all EU initiatives (including e.g. procurement) that involve potential reuse of previously submitted information. This magnifies the 'pull' aspect of a requirement to re-use existing data by tying it to specific common or transferable features.

[82] This can easily be done for demand-side measures (see Section IV.A.4); code or standards compliance could be included in the requirement and/or the qualification conditions for tenders. The Procurement Directives allow standards to be used in this way ('equivalent performance' in lieu can encourage innovation and avoid unfair exclusion). The comply/explain/prove mechanism could provide leverage through conditionality to EC support for Member State initiatives or access to Commission services or by using it to let Member States show compliance with relevant Directives or EIF maturity (this is not subsumed in the legislative approach because other evidence could be substituted).

[83] The benefits of a completely uniform approach may not be compelling, and the EC may lack the *vires* to impose harmonisation at all levels. Interoperability, to take an example, is

fine in itself, but does not create a case for requiring common processes at all levels (which is sufficient but certainly not necessary for interoperability). Determining what forms of localisation are most appropriate is a matter that should involve the local level and should be a continuing process as circumstances change. These circumstances are not limited to the technology and legal basis of e-Government *per se*, but also include the structure of services and service needs. Moreover, compliance, adoption (by public authorities) and acceptance by service claimants may be strongly influenced by perceptions of ownership, control and flexibility.

[84] e.g. hosting and running Base Registries, reference databases of non-base data, platforms, data and query, federation and search services.

[85] For example, the Belgian law of 5 May 2014 was sparked by the central government's dissatisfaction with the slow progress of regional OOP implementation despite endorsement at federal level.

[86] See endnote 77.

[87] EU support could violate additionality or crowd out action better adapted to local conditions.

[88] This could in principle be used to underwrite Member State costs of OOP implementation to the extent that these could be directly attributed to cross-border activities. This may be particularly useful for Member States facing the most severe public expenditure constraints, which are often most likely to receive requests for previously-submitted personal information or to benefit from the ability to obtain reliable and comprehensive business information from other countries.

[89] This schema is no longer part of the revised EIF, but the scenarios remain valid.

[90] These include: Starting a business; participating in public procurement; registering patents, trademarks, designs; and demonstrating compliance with rules on consumer protection, labelling, packaging, etc.; registering for and filing corporate and personal tax returns, making payments, and qualifying for and claiming benefits; making excise and shipping declarations; registering and obtaining certification of (some) qualifications, diplomas and professional standing; job, commercial partnership and investment search; providing information to regulators; and making customs declarations and payments.

[91] Certification and notification of births, marriages and deaths; driving and vehicle licenses; passports and visas; residence and work permits; educational application and enrolment; study grants and loans; tax and business registration (and providing other data for these purposes); VAT payments; social security enrolment and other information (e.g. eligibility, contribution history); eligibility and claim/payment history for unemployment benefits, child allowances, pensions and public health insurance; and origin-destination settlements and certification that EU-wide customs obligations have been met.

[92] e.g. ECRIS, SIS-II.

[93] including competition, data protection, communications and sectoral regulators

[94] Including e.g. practitioners of regulated professions and service providers and also owners, subsidiaries and partners of national or cross-border enterprises.

[95] For instance, in the cross-border business context, a foreseeable consequence of reduced costs and other burdens is an increase in the level of cross-border activity. This can be

expected to lead to: greater competition; improved consumer outcomes (at least in the foreign country, but possibly throughout the Single Market); faster innovation; reduced margins for businesses in the foreign country (at least initially); increasing demands for input markets; changes in international competitiveness; and possibly increased specialisation across Member States (in obedience to the principle of comparative advantage).

[96] E.g. biometric and criminal data – see discussion on page 12.

[97] e.g. implementation of consent mechanisms

[98] These are not well-matched to the different requirements of service request procedures.

[99] e.g. fragmentation of base repositories

[100] Barriers always inhibit OOP implementation, but gaps can also provide incentives or drivers

[101] Repositories containing data not suitable for base repositories, esp. those that are: not of wide applicability; subject to frequent change; sensitive or restricted; etc. See Annex IX.

[102] As used here, this could mean a single EU eID or a system for mutual recognition of national eIDs.

[103] Extensive work to improve semantic and technical interoperability has been carried on at European level (e.g. by ISA^2 and Large Scale Pilot projects), leading to solutions at EU level; current and future semantic and technical interoperability initiatives should cease to obstruct EU-wide OOP implementation. By contrast, legal interoperability issues are more problematic, as shown by limited success of efforts to harmonise national frameworks. Because data and information re-use at national level remains a Member State competence, changes in laws/regulations to favour interoperability (and OOP) could be very difficult.

[104] A range of good practices for access to base registries have been developed by Deloitte for the ISA programme; they are available from: http://ec.europa.eu/isa/documents/final-report_en.pdf.

[105] e.g. Register Centre's Nordic Moving Service.

[106] e.g. X-Road or BRIS, which provides legal interoperability and organisational and semantic agreements with the MS.

[107] This shows a classic positive network externality which symmetric or widespread cross-border demand would produce a 'tipping equilibrium' in which one approach (not necessarily the best) would dominate throughout Europe, and in which innovations and improvements away from that architecture would struggle for acceptance. On the other hand, given present asymmetries in cross-border activity, a likely baseline outcome is the formation of distinct 'interoperability clusters' with low intracluster barriers but high intercluster barriers. This shows a classic positive network externality which symmetric or widespread cross-border demand would produce a 'tipping equilibrium' in which one approach (not necessarily the best) would dominate throughout Europe, and in which innovations and improvements away from that architecture would struggle for acceptance. On the other hand, given present asymmetries in cross-border activity, a likely baseline outcome is the formation of distinct 'interoperability clusters' with low intracluster barriers but high intercluster barriers.

[108] One key point here is the difference between the responsibilities of public data controllers to their individuals and their responsibilities to non-individuals; these same issues form part of the current development of the EU-US Privacy Shield and the data protection aspects of TTIP. The recent decision in the Microsoft case provides a clear indication that this topic is not yet fully resolved.

[109] Assessment of administrative burdens sustained by individuals and businesses of all Member States for all public services to which OOP might be applicable is out of the scope of this project. Chapter 6 of D3 provides an initial attempt to assess administrative burdens for each of a selection of use cases, but this is difficult to extend to the level at which policy decisions are taken. Interviews with national public administration representatives of the ten selected countries did not provide any information on cost of implementation and maintenance of the current OOP scenario and impact data provided by selected Member States in the 2 June public event demonstrated the difficulty of measuring more and a fraction of the cost impacts or of producing robust and generaliseable results even at national level let alone for cross-border activity..

[110] Member States prosper in different ways using common economic, legal, organisational, service and technical infrastructures

[111] There may be transitional demands for e.g. education and start-up business support.

[112] "The good is the enemy of the best" or *vice versa*

[113] Specifically, the balance of cost savings and benefits to the parties under this scenario will be adversely affected; cross border activity will tend to involve entities with higher needs for public services and the returns to the destination country in terms of economic productivity, etc. are likely to be lower than under the favourable alternative.

[114] See e.g. discussion of the implications of GDPR for public authority data controllers in endnote 279.

[115] In addition to the widely varying definitions of OOP, contents, access models and formats in different countries and for different data types documented above an in previous Deliverables, the specifics of the legal framework can both facilitate and impair OOP. For instance, the requirement that data held by public authorities must not be stored in multiple databases certainly forces administrations to re-use data or to request them but not store them and thus reinforces the reality of authentic sources. However, it does not directly compel OOP. Indeed, it has been seen by national representatives interviewed for this project as an impediment to data re-use and to the creation of data structures efficiently adapted to the informational requirements of specific services, in which case multiple copies of 'non-base' data or data for which no single authentic source has been specified.

[116] Continuing the previous example, countries with 'single point of storage' rules may face difficulties when citizen or business cross-border activity generates new data that must be stored in both countries; while there is no essential bar to interpreting such laws as applying only to the country where they are passed (and not to data of that country's individuals of businesses in the European context), the rationale behind such laws (whether to prevent fraud and error or to strengthen incentives for OOP) remains valid and the objectives of the relevant single point of storage law may be weakened by cross border transfers.

[117] Incompatibility in this case may refer to legal, organisational, semantic and technological differences or to cultural barriers to wider information sharing or to the adoption of a solution developed elsewhere.

[118] It should be noted that ISA has developed a model to measure service maturity as related to interoperability – see http://ec.europa.eu/isa/ready-to-use-solutions/imm_en.htm. This approach could, in principle, be adapted to measure OOP maturity of strategies, systems or services.

[119] These considerations apply both to 'top down' and to 'bottom up' options. To illustrate the 'top down' aspect, consider the case of legislative measures at EU level (Option 1). Account must be taken of the proportionality and effectiveness of the proposed legislation. Roughly speaking, the implementation cost is proportionate to the degree to which the Member State is already in compliance; those for whom compliance is easiest will be those who have adopted common methods or solutions most consistent with the proposal; those who have not made any substantial progress (in some cases because the benefits are expected to be modest) will face a net excess of costs over benefits; those who have sophisticated and advanced OOP elements (because the benefits were seen to outweigh the costs at national or bilateral cross-border level) may face additional costs in 'retrofitting' their systems to meet the new top-down requirements.

For bottom-up options (esp. Option 3), progress towards OOP can be seen as a networked decision. The different status of the various Member States means that some links are more likely to form and lead to mutual progress than others; the more consistent and widespread the network, the more uniform the associated standards, solutions and cross-border arrangements are likely to be. This does not mean that the interacting counties should be at the same level of maturity, have the same definition of OOP and related principles, or have the same set of priority areas. Indeed, a degree of complementarity may be useful to ensure that fundamental elements are thoroughly explored (obviating the 'lock-in' or first mover advantage that bedevils so many ICT-intensive areas) and that significant cross-border activities are accommodated even if specific flows may be very asymmetric (e.g. if country A receives a lot of University applicants from other Member States, but sends very few of its own student abroad).

[120] Some, like GDPR, are too recent to come within scope of REFIT.

[121] Ranging from cost- and responsibility sharing arrangements to semantic interoperability frameworks.

[122] Source: interviews with national representatives and published indicative computations.

[123] core expansion limited by subsidiarity

[124] expanded sets of OOP-enabled public services and re-useable data

[125] By addressing the most urgent and quantitatively significant motives for OOP without the need for cross-border data transfers and by creating a set of different approaches that are not easy to interconnect or link.

[126] By providing proof of concept and (eventually) evidence, and by providing reusable solutions and expandable platforms.

[127] See Section V.A and Annex X.

[128] User-centric means reconfiguration of services to meet citizen and business needs *as experienced by beneficiaries* (e.g. 'life events' interfaces and service access points). It can also imply greater user participation in setting policies, including OOP and complementary data management, cost recovery etc.

[129] In effect, the home jurisdiction provides acceptable assurance of a cross-border applicant's eligibility.

[130] E.g. in differences between Member States in terms of the time-frame for free mobility of workers from new Member States, eligibility for specific benefits or business support measures and credit for contributions to social insurance programmes.

[131] Concentrates on areas of greatest immediate payoff, in particular business applications.

[132] Aligned to the needs of businesses and individuals rather than those of administrations.

[133] E.g. provisions under GDPR Articles 6(1)(c) (compliance with a legal obligation) or 6(1)(e) (necessity for performance of a task carried out in the public interest or exercise of the controller's official authority).

[134] For application of the GDPR, OOP transmissions should be treated as further processing.

[135] Unless otherwise indicated, definitions are taken from Sec 6.2 of the consultation draft of the revised European Interoperability Framework: SC152_D04 02 03_ Third Intermediate EIF Version_v1.00.pdf, which is the draft circulated for use in the public consultation exercise (now withdrawn).

[136] https://joinup.ec.europa.eu/

[137] GDPR Article 4(1) – similar definition is given in Article 7(a) of the DPD.

[138] GDPR Art. 4(1).

[139] Official definition from European Data Protection Supervisor glossary at: https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Glossary/pid/74.

[140] Technopopedia: see https://www.techopedia.com/definition/29059/data-ownership.

[141] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, Official Journal No. L 77 27 March 1996, p. 20-28: http://www.europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=31996L0009&model=guichett.

[142] Article 2 (b) of Regulation (EC) No 45/2001: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/DataProt/Legislation/Reg_45-2001_EN.pdf. Note that this applies to processing of *personal* data.

[143] Article 2 (e) of Regulation (EC) No 45/2001: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/DataProt/Legislation/Reg_45-2001_EN.pdf.

[144] Note that this differs slightly from the GDPR definition of a 'recipient' in a way that is relevant for OOP. The GDPR (Art. 4(1)) defines a recipient as "a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. *However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not*

be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing." GDPR Art. 4(1).

[145] Directive 95/46/EC at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[146] Author's own definition.

[147] https://ec.europa.eu/digital-agenda/en/digital-single-market.

[148] MOREQ specifications: http://ec.europa.eu/transparency/archivalpolicy/moreq/doc/moreq2 spec.pdf.

[149] Author's definition.

[150] Author's definition.

[151] MOREQ specifications: http://ec.europa.eu/transparency/archivalpolicy/moreq/doc/moreq2 spec.pdf.

[152] Author's definition.

[153] "Interoperability governance" is the background context in the form of relevant policies, strategies, guidelines, etc., for any interoperability activity.

[154] *http://ec.europa.eulisaldocumentslisa_2proposal_en.pdf*: also DECISION No 922/2009/EC.

[155] http://www.opensource.org/docs/osd.

[156] See http://www.g nu.org/philosophy/free-sw.html for a definition.

[157] GDPR, Article 4(1).

[158] See Article 8 of the Services Directive — OJ L376 of 27.12.2006.

[159] GDPR, Article 4(1).

[160] The use of the term "cross-border data processing" is drawn from the GDPR; the definition here thus modifies that given in the revised EIF, which applies as well to non-personal data.

[161] http://www.oasis-open.org/committees/download.php/19679/soa-rm-cs.pdf.

[162] The principles underlying this are: i) Speed – the time taken to deliver a service should be the shortest possible for both the customer and the agency while still ensuring outcomes are delivered right the first time; ii) Engagement– the way in which services are delivered should be seen as citizen-centric; iii) Responsive – there should be an intelligent mechanism in place to address any variation in meeting service levels and drive any changes required; iv) Value – the customer needs to believe that the One-Stop Shop is cost effective, and value is driven by customer outcomes, not agency or department processes; v) Integration – a One-Stop Shop should be seamlessly integrated, there should be no 'wrong door' policy for the customer; vi) Choice– there should be multiple channels for service delivery, so that customers can have 'channels of choice', depending on specific needs at specific times; and vii) Experience – personalisation of service is necessary to ensure that customers' experiences are on a par with what they are receiving in the private sector. See PWC (2012), Transforming the citizen experience One stop shop for public services, pwc.au.com.

.[163] When first implemented, these served as providers of reliable public information, but gradually began to deliver various services (e.g. licenses, permits, certificates).

[164] All Member States have these in compliance with the Services Directive (Directive 2006/123/EC).

[165] One of these is specifically discussed in the body of this report: starting a business branch in another country. The other three (requesting a licence for transport of goods; participating in a public procurement exercise for construction; and establishing a new association are reported in annexes.

[166] The main body of this report discusses one of the two investigated use cases: enrolling in a Masters' degree course: the case of registration as a self-employed individual is reported in annex.

[167] EC, *Future-proofing eGovernment for a Digital Single Market, Final Insight Report*, June 2015

[168] Reported in the eGovernment Benchmarking framework raw data and – by consequence- available for all Member State and for all functionalities in analysis.

[169] According to the eGovernment Benchmark Background Report 2015.

[170] Information taken from the eGovernment Benchmark Framework 2012-2015, Method paper July 2012 (pp.76 and following)

[171] Note that the business register may not always be a government organisation. In most EU Member States they are run by the government, but e.g. in Estonia and Denmark they are operated by the Court of Justice; in Italy and the Netherlands they are run by the Chamber of Commerce and in Luxembourg the registry is operated by a public-private partnership. See http://www.corporateregistersforum.org/wp-content/uploads/2015-international-business-registers-report-reprint.pdf. more information about EU business registers is also available on the e-Justice portal https://e-justice.europa.eu/content_business_registers_in_member_states-106-en.do

[172] This does not eliminate all presence requirements; even when cyber-notary certification is accepted the original certificate often requires in-person verification of identity.

[173] In 2014, 98% of company formation documents were submitted electronically and 73% of annual returns were submitted electronically.

[174] See https://www.epnuffic.NI/en/diploma-recognition/recognition-of-your-profession-in-the-Netherlands.

[175] See http://ec.europa.eu/growth/single-market/services/free-movement-professionals/policy/european-professional-card/index_en.htm.

[176] This will include formal signature validation and registration of branch names if they differ from that of the parent company.

[177] If he intends to use this as a trade mark, he will also need to register it with the Benelux Office for Intellectual Property.

[178] In 2014, 98% of company formation documents were submitted electronically and 73% of annual returns were submitted electronically.

[179] The application document is available for download at https://www.yrityssuomi.fi/en/lomake?docid=5621

[180] http://ec.europa.eu/growth/single-market/public-procurement/rules-implementation/index_en.htm; details on EU-level enforcement activities to date available from http://ec.europa.eu/growth/single-market/public-procurement/infringements/index_en.htm

[181] This became applicable from April 2016, but both electronic and paper versions may exist until April 2018 – see http://ec.europa.eu/growth/single-market/public-procurement/e-procurement/espd/index_en.htm

[182] Available to registered users at: https://joinup.ec.europa.eu/catalogue/asset_release/vcd-virtual-company-dossier.

[183] The service was revamped with the entry into force of new public procurement directives in April 2016: https://ec.europa.eu/growth/tools-databases/ecertis/

[184] Described at: https://ec.europa.eu/growth/single-market/public-procurement/e-procurement/espd_en.

[185] This account reflects the revised timetable at: http://ec.europa.eu/DocsRoom/documents/16332/attachments/1/translations.

[186] http://ec.europa.eu/DocsRoom/documents/16332/attachments/1/translations.

[187] See e.g. https://www.turn2us.org.uk/Benefit-guides/Self-employment-and-benefits/Can-I-get-self-employed-tax-credits#guide-content or https://www.individualsadvice.org.uk/work/self-employed-or-looking-for-work/self-employment-checklist/.

[188] Public Information Act (2000) – Available at: https://www.riigiteataja.ee/en/eli/518012016001/consolide#para43b3

[189] *General Part of the Economic Activities Code Act* (Passed 23.02.2011, Entry into force 01.01.2014) – available at: https://www.riigiteataja.ee/en/eli/530102013062/consolide

[190] Loi du 5 mai 2014 portant assentiment à la Convention concernant la compétence, la loi applicable, la reconnaissance, l'exécution et la coopération en matière de responsabilité parentale et de mesures de protection des enfants, faite à La Haye le 19 octobre 1996.

[191] These include Chapter 26, Part 2 on "streamlined company registration procedures," Part 3 on public sector procurement, Part 7 on Companies' Transparency (esp. registers of persons with significant control|). Of particular significance is Part 8 about company filing requirements, which replaces annual returns with confirmation statements referring to data already provided on an ongoing basis and Schedule 5, which provides an "Option to keep information on central register." See full text at: http://www.legislation.gov.uk/ukpga/2015/26/contents/enacted.

[192] Some versions of purpose limitation allow re-use provided consent is obtained, but this may be difficult or cumbersome to verify and may not be practicable when information is collected from third parties.

[193] The Finnish interviewees estimated more than 500 laws would need to be modified accordingly.

[194] Such as the UK's "Business Impact Target" (BIT) in the SBEE 2015 Act (see footnote 9).

[195] Enrolling in higher education; Applying for student grants; obtaining financial aid for starting up as self-employed; Registering for unemployment benefits; Ensuring continuity of pension payments.

[196] Register company name; Register domicile of business; Register a company or a branch of a company in a business register; Receive formal validation of signatures of representatives of the business; Register with Social Security Office; Register with compulsory healthcare; Be compliant with social security obligations; Be compliant with obligations related to work place security; Be compliant with tax related obligations; Register employee before first work day.

[197] Maria Sangder and Arto Smolander, Talent Vectia Oy (2015), "Exploratory study on cross-border information exchange and digital services between governments"

[198] https://joinup.ec.europa.eu/asset/core_vocabularies/description.

[199] http://ec.europa.eu/isa/actions/01-trusted-information-exchange/1-2action_en.htm

[200] At the moment in which the report was elaborated the initiative was in a pilot phase and SPID credential could be used to access services in pilot regions (eg. Tuscany, Friuli Venezia Giulia and Emilia Romagna) and pilot agencies (eg. INPS, INAIL).

[201] PAe webpage: https://www.administracionelectronica.gob.es

[202] Government Gateway: https://www.gov.uk/

[203] Indeed, a national legal context can directly impede OOP implementation; in the case of Finland, the national public administration representative pointed out the strong legal emphasis laid on 'purpose limitation - that data and information should only be used for the purpose for which they were originally collected. This directly inhibits realising the enormous potential of re-using data and information available or already provided. In principle, this could be overcome by suitable consent provisions, but the burden associated with the need to provide purpose-specific consents reduces the advantages – to the end-user – of OOP. There are alternatives; in the UK, for instance, data provided to some authorities are deemed to be reusable and consent is obtained when the data are first provided. But this is likely to end shortly with the entry into force of the GDPR and even now is not effectively transferrable across national boundaries.

[204] The GDPR gives personal data subjects access rights to their data in commonly-used electronic formats for the purposes of automated processing.

[205] Directive 2006/123/EC on services in the internal market

[206] Directive 2006/123/EC, 2006 – Art. 5 "Where Member States require a provider or recipient to supply a certificate, attestation or any other document proving that a requirement has been satisfied, they shall accept any document from another Member State which serves an equivalent purpose or from which it is clear that the requirement in question has been satisfied." – Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0123&from=EN

[207] Directive 2006/123/EC - Art. 34 "The Commission, in cooperation with Member States, shall establish an electronic system for the exchange of information between Member States, taking into account existing information systems."

[208] Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport.

[209] Partially governed by the Services Directive, which requires Member States to set up Points of Single Contact for this purpose.

[210] Directive 2011/24/EU on the application of patients' rights in cross-border healthcare.

[211] http://ec.europa.eu/justice/criminal/european-e-justice/ecris/index_en.htm

[212] Restricted to authorised law enforcement officers, for whom use of ECRIS data is compulsory.

[213] Informally, purpose limitation means that data can only be used for the purposes for which they were originally collected. However, in practice it means that data can only be processed fairly and lawfully and for explicitly enumerated purposes, and that they must not be further processed in a manner *incompatible with* (rather than different from) those purposes. The tricky parts here are compatibility and the role of consent in validating repurposing.

[214] For example, see https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/.

[215] We note that this is related to but distinct from the lack of equivalence among different forms, contents, purposes, controllers and vintages of essentially the same information. In many ways, this is a desired 'side effect' of or complement to OOP, but like the 'whole government' principle it goes far beyond OOP.

[216] Article 1 states "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data" - see Directive 95/46/EC at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[217] This is the case in Italy where data access and use is supposed to be regulated by *ad-hoc* framework agreements among the public administrations involved, which can be implemented only on approval by the Italian data protection Authority.

[218] i.e. base registers, data exchange infrastructures, interoperable components

[219] E.g. the UK, where the driver and vehicle parts of the DVLA's database structure do not share data.

[220] This 'federated interconnection' approach was used when building e.g. ECRIS and SIS II.

[221] This may be a permanent feature; see discussion of the 'No wrong door' principle on page 150.

[222] e.g. in Belgium for marriage procedures any birth certificates issued in other languages, even within the country, need to be translated and certified for an approximated cost of 100 EUR

[223] This includes a clear and agreed separation of 'permanent' (or 'base') data from data that change frequently or should not be widely shared, etc.

[224] For example, costs to the 'original country' are not offset by direct benefits and are not generally aligned with organisational mandates restricted to delivering services to qualified claimants (rather than facilitating individuals' or businesses' access to services elsewhere.

[225] In other words, a set of data that meet the needs of the data requestor but do not go further, in obedience to the principle of data minimisation cannot easily be assembled by the original data controller. This would likely result in a response that is incomplete from the perspective of the data requestor, who would then have to

[226] E.g. through Large Scale Pilots of identification for registering domicile and business tax declarations (STORK), registering for legal aid (e-CODEX) and registering new legal entities (SPOCS)

[227] As reported by the Spanish national representatives.

[228] e.g. business real estate transactions, paying social contributions, reporting termination of employment or submitting a tender in public procurement. See EC (2013), "Study on analysis of the needs for cross-border services and assessment of the legal organisational, semantic and technical barriers" at: https://ec.europa.eu/digital-single-market/en/news/final-report-study-analysis-needs-cross-border-services-and-assessment-organisational-legal

[229] i.e. base registries versus distributed data exchange protocols.

[230] E.g. eSignatures and eID. For example, while eID uses similar identification numbers in Estonia and Finland the number is defined according to different criteria; in consequence the Finnish ID number is recognised for obtaining some services in Estonia, but not conversely.

[231] as mentioned by the Estonian and UK national representatives. For instance, the benefits experienced in Estonia thanks to the implementation of the X-Road infrastructure for data exchange at national level induced the decision makers to improve their commitment to realise initiatives for cross-border data and information exchange. In consequence, Estonia included in its Digital Agenda 2020 policy objectives 1) increasing the number of Nordic countries with which to jointly develop basic infrastructures (from 1 to 3) and 2) developing cross-border public services with 7 countries. Digital Agenda 2020 for Estonia – page 31/53 "*2. Number of Nordic (or other) countries with whom Estonia has jointly developed basic infrastructure components Starting level: 0 → target level 3 (2020) [Source: Estonian Information System's Authority] - 3. Number of countries with whom Estonia has developed cross-border public services based on the Estonian basic infrastructure (e.g. X-Road or eID) Starting point: 0 (2013) → target level: 7 (2020) [Source: Estonian Information System's Authority]*" – Available at: https://e-estonia.com/wp-content/uploads/2014/04/Digital-Agenda2020_Estonia_ENG.pdf

[232] as mentioned by the Hungarian national representative.

[233] Source: presentation of the Belgian national representative at the EU Presidency session on OOP, Amsterdam, 2 June 2015.

[234] E.g. Regulation 2014/910/UE on electronic identification, authentication and signature (eIDAS).

[235] E.g. Regulation 1072/2009 on common rules for access to the international road haulage market.

[236] For example, if country X needs data from 27 other countries and needs to provide data to 27 other countries, at what point (inbound or outbound) are things standardised? If

country X has only 'OOP-enabled' some services or data (or even none at all), how can resulting asymmetry of treatment (in terms of access to services) be managed?

[237] The decisions will typically not be revised when data in another country change, but are themselves data.

[238] GDPR, Chapter 2, Article 5, Par. 1.

[239] Analogous to the concept of the 'home data centre' concept proposed under the US Nebula option of the Future Internet Architecture project – see http://www.cs.stevens.edu/~nicolosi/papers/nebula-wp-10.pdf.

[240] Most countries have made some progress already, especially as regards base repositories whose contents, structure and function are clearly codified and often reinforced by law.

[241] For personal data, Article 6(1) of the GDPR establishes several grounds for further processing, at least one of which must be satisfied. These include: consent of the data subject (specific

[242] Individuals have a right under GDPR to demand human processing, but exercising this right imposes costs on data subjects, controllers and processors that limit the benefits of OOP. A full impact assessment of a specific option will have to assess the proportion of cases where this right is exercised and the attendant costs.

[243] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[244] Article 7(1) of the GDPR requires that controllers relying on consent to justify processing should be able to demonstrate that consent was given by the data subject to the processing. Conditions for valid consent are: 7(2) - consent to processing contained in a written declaration produced by the controller must be distinguishable from other matters in that declaration, intelligible, easily accessible and be in clear and plain language - Recital 42 notes that consent is *informed* only when the data subject is aware of (at least) the identity of the controller and the intended purposes of processing; 7(3) – data subjects must have the right to revoke consent at any time, and it must be as easy to withdraw consent as it is to give it - withdrawal of consent does not retrospectively make the processing Unlawful, but the controller must inform data subjects of this before consent is initially given; 7(4) notes that, in cases where the performance of a contract (*including provision of a service)* is conditional on consent to the processing of data that is not *necessary* for that performance, the consent will be presumed not to have been freely given. Recital 43 clarifies this and adds a further circumstance relevant to OOP by noting that consent is presumed not to have been freely given if (despite it being appropriate in the circumstances), there is no provision for separate consent to be given to different processing operations.

[245] The obligations are discussed in the paragraph on "Creeping inaccuracy" in Section VII.E.

[246] Potentially OOP-relevant examples include: processing for fraud prevention (Recital 47); and transmission of personal data within a group of undertakings for internal administrative purposes, including client and employee data (note international transfer requirements still apply. But this justification is not available to public authorities. Note, too, that Recital 47 also encourages controllers to consider the expectations of data subjects when assessing whether the controllers' legitimate interests are outweighed by the interests of data

subjects. The interests and fundamental rights of data subjects "could in particular override" the controller's where data subjects "do not reasonably expect further processing."

[247] In the particular case of *data transfers* as a type of further processing, Article 49(1) allows transfers based on "compelling legitimate interests" where they are *not repetitive*, relate to only a limited number of data subjects and where the controller has assessed and ensured adequacy. However, this justification would seem to be ruled out for public authorities and can in any case only be used when the controller cannot rely on any other method of ensuring adequacy, including model clauses, BCRs, approved contracts and all derogations from Article 49(1)(a)-(f).The controller would also need to notify the supervisory authority that it was relying on this ground for transfer.

[248] Interestingly, processing of photographs – which have previously been regarded as sensitive in some Member States – is not automatically 'caught' unless used for unique identification or authentication as a biometric.

[249] Compare 6(1)(a-f) as discussed above.

[250] Revised EIF, Chapter 2.

[251] The consultation version of the revised EIF expresses this as: "Public administrations are encouraged to reuse and share information and data that are already stored by public administrations, unless certain restrictions apply." Revised EIF, Recommendation 3, p. 11.

[252] This reference is strengthened in relation to the general discussion of further processing of data: "public administrations already store large amounts of information with the potential for reuse. Examples of existing information with high potential for further processing include master data coming from base registries as authoritative data used by multiple applications and systems; open data published by public organisations which can be used under open use licences; other types of authoritative data validated and managed under the responsibility of public authorities. Reuse of information avoids the burden of requesting the same information multiple times, increases information quality and decreases costs." Revised EIF, p. 20.

[253] "For information sources owned and managed by national administrations, preservation is a purely national matter. For information that is not purely national, preservation becomes a European issue, as preservation policies might be different per Member State. These differences require an appropriate preservation policy as public administrations might operate under different jurisdictions which might elicit other requirements." Consultation draft of revised EIF, p. 12.

[254] Please note these data are on 27 Member States, not including Croatia that joined the European Union on 1 July 2013 as 28th Member State. Talaban, M. (2013) "Business registers interconnection system (BRIS)" presentation at ECRF Conference, Bucharest June 2013 at: http://www.ecrforum.org/wp-content/uploads/2013/2013%20Romania/Presentations/1-BRIS-Mrs-Magda-Talaban-EU.pptx.

[255] E.g. sole traders, partnerships, social enterprises, European Economic Interest Groupings, cooperatives, consortia, branches, associations, insurance societies and foundations.

[256] Note that, while 25 Member States register branches, only 1 uses an identifier that links the branch to the parent company.

[257] Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:258:0011:0019:EN:PDF.

[258] 19 Member States publish such additional material e.g. mergers and acquisitions, company dissolution, shareholder lists, financial structure and instruments, and prohibitions.

[259] Directive 2012/17/EU of the European Parliament and of the Council of 13 June 2012 amending Council Directive 89/666/EEC and Directives 2005/56/EC and 2009/101/EC of the European Parliament and of the Council as regards the interconnection of central, commercial and companies registers

[260] See e.g. https://e-justice.europa.eu/content_business_registers_at_european_level-105--maximize-en.do and http://www.ecrforum.org/wp-content/uploads/2013/2013%20Romania/Presentations/1-BRIS-Mrs-Magda-Talaban-EU.pptx.

[261] Based in part on elements of the ISA Action 1.2 documentation, e.g. the inventory template: http://ec.europa.eu/isa/actions/documents/isa_1.2_d1.0.1_template_for_the_inventory.pdf.

[262] Including semantic interoperability agreements and the existence of base registry taxonomies and data dictionaries.

[263] Including the case of interconnected base registries.

[264] These are data that are uniquely held in the registry in question, which must therefore be shared with other base registries and data users, as well as 'authentic data' that may not be uniquely held but which have pre-eminence over any other record.

[265] including means and sources of collection and subsequent processing

[266] See discussion in 0.

[267] E.g. Cadastral, Criminal, Business, Census data.

[268] The purpose may be described in functional terms e.g. identification, attestation or certification of standing, qualification or eligibility, etc. Alternatively, they may be described in terms of the functionality (ies) and/or services for which they are used. See D2 for definitions and examples of functionalities and services.

[269] This has recently implemented a pilot scheme for EU-wide background checks; while this is currently limited to criminal records, it does provide a single point of entry for public administrations, businesses and individuals seeking assurance on the fitness of prospective employees. See http://www.cbscreening.co.uk/news/post/the-dbs-launches-a-new-eu-check-pilot.aspx.

[270] E.g. certification of professional competence or educational attainment.

[271] E.g. health records.

[272] Specifically, Recommendation 20 calls on states holding data to "make authoritative sources of information available to others while implementing access and control mechanisms to ensure security and privacy in accordance with the relevant legislation." Recommendation 21 deals with interfaces and meta-data: "Public administrations, when working to establish European Public Services, should develop interfaces to base registries and authoritative sources of information, and expose the semantic and technical data needed for others to connect and reuse the information. These data should be aligned whenever possible." Recommendation 22 expands on this to call for what we have called a data catalogue: "Each base registry should be accompanied by description of its content, service assurance and responsibilities, type of master data it keeps, conditions of access, terminology, glossary, as well as which master data it consumes from other Base Registries (if any)." Recommendation 23 deals with data quality: "Public administrations should create data quality assurance plans for base registries and related master data, execute them regularly and keep them updated.

[273] That does not remove the responsibilities of data controllers to maintain and use accurate and up-to-date records, but the responsibility for notifying data controllers of the need for corrections rests with data referents.

[274] Adapted from the principles used by the Netherlands.

[275] See https://www.fig.net/resources/proceedings/fig_proceedings/cairo/papers/ts_01/ts01_04_vandermolen.pdf

[276] This potential weakness can be minimised by e.g. sunset provisions.

[277] The Act of 5 May 2014 enshrining the principle of one-time data collection in the operation of departments and bodies that are part of or carry out tasks for government and on simplification and equivalence of electronic and paper forms, published in the Belgian Official Journal on 4 June 2014.

[278] Note that Directive 2012/17/EU mandates interconnection of business registers.

[279] Some of this is already built in, for instance Art. 82 of the GDPR allows Member States to enact specific laws for processing personal data in the employment context. Other provisions are less comforting; it has been argued, for example, that the GDPR's sanctions regime, which mandates step fines for non-compliant controllers (or joint controllers) may produce unforeseen consequences when applied to e.g. small and micro industries that cooperate with public sector OOP bodies. The situation as regards public administrations who act as controllers or processors is less clear, especially if OOP transfers create joint controller links. By the same token the data minimisation requirements may inhibit OOP development.

[280] This may also be appropriate for consideration at EU level, to ensure a focus on the availability to government of necessary information rather than the specific actions required of firms to make such information available.

[281] See http://ec.europa.eu/info/strategy/better-regulation-why-and-how_en.

[282] See http://ec.europa.eu/smart-regulation/refit/index_en.htm.

[283] See http://ec.europa.eu/smart-regulation/guidelines/tool_16_en.htm.

[284] Under Societal Impacts, the toolkit does draw attention to access to and effects on social protection, health and educational systems, by asking staff to consider "Does the option have an impact on services in terms of quality/access for all?" – see tool 16 (endnote 283).

[285] This is widely regarded as good practice and has been strongly encouraged by the EC, but as Renda (2015) notes "While some national governments have started to adopt sophisticated better regulation tools many years before the European Commission (in particular, the United Kingdom), and other have made significant steps in the development of methods for the assessment of regulatory costs (the Netherlands, Germany, and increasingly Sweden and the Czech Republic), in most Member States, despite the official adoption of better regulation tools, implementation remains poor or non-existent." Renda, A., 2015. Too Good to Be True? A Quick Assessment of the European Commission's New Better Regulation Package. A Quick Assessment of the European Commission's New Better Regulation Package (May 21, 2015). CEPS Special Report, 108.

[286] The active party here could be RegWatch Europe, an organisation of independent regulatory scrutiny bodies from Austria, Czech Republic, Netherlands, Sweden, the UK and latterly Norway and Finland.

[287] The ISA^2 actions are not limited to semantic interoperability, but extend to other levels as well. See http://ec.europa.eu/isa/isa2/index_en.htm. The actions include revisions to the European Interoperability Framework (EIF) and the European Interoperability Strategy (EIS), development of a European Interoperability Reference Architecture (EIRA) and a map of solutions in the shape of the European Interoperability Cartography (EIC). For an overview of the themes and actions, see http://ec.europa.eu/isa/library/documents/isa2-work-programme-2016-summary_en.pdf.

[288] Adapted from ISA Work program Access to base registries, final Report, Feb. 2014 at: http://ec.europa.eu/isa/documents/final-report_en.pdf.

[289] Note that individuals living abroad are *not* generally required to report data to 'their' home countries. Consider registration of births; UK rules say:

> *"You must register your child's birth according to the regulations in the country where the child was born. They'll give you a local birth certificate. This local birth certificate should be accepted in the UK, e.g. when you apply for a passport or register with a school or doctor. You might need to have it translated and certified if it isn't in English. Once you've registered locally you may also be able to register the birth with the UK authorities. You can only do this if the child was born on or after 1 January 1983. You don't need to register with the UK authorities but it means:*
>
> - the birth will be recorded with the General Register Offices or at the National Records Office of Scotland
> - you can order a consular birth registration certificate
> - You can still apply for a UK passport for your child even if you don't register the birth in the UK."
>
> *So the creation of a master record in the home country is at the discretion of the data referent (or its parent). This may limit the savings from OOP, because public authorities in other countries may face a 'paper chase' trying*

to find reusable data or have to ask the individual or business where the records are, which limits administrative burden time or effort savings.

[290] A unique identifier could be used by repositories to search across interoperable repositories for new data that should be incorporated into their records, but this might fall foul of 'single point of storage' rules and force interconnection at the identifier level rather than interconnection at the repository level. Moreover, the assignment of identifiers may itself need to be interconnected or cross-linked in order to keep track of e.g. business branch formation or partnerships, marriages and divorces, etc.

[291] The approach followed within OOP-enabled countries for federating national and local data, etc. It is regarded as a limited solution for cross-border contexts where priority may not be easy to establish.

[292] See endnote 287.

[293] Examples of the use of semantic interoperability tools (not just for connecting base registries or exchanging data at the level of individual individuals or businesses) include: the use of the Core Business vocabulary in the DG JUST Business Registers Interconnection System (BRIS); the DCAT-AP specification in the DG CNECT pan-European Open Data Portal (part of the Connecting Europe Facility's Digital Service Infrastructures); Core Vocabularies for the DG COMP State Aid Notification system; and the Core Public Service Vocabulary-AP in Estonia and Italy. For more details, see Annex I (detailed action descriptions) of the ISA^2 Action Plan at: http://ec.europa.eu/isa/library/documents/isa2-work-programme-2016-detailed-action-descriptions_en.pdf.

[294] In essence, a metadata registry that provides an overview of *all* data available for EU-wide use by administrations.

[295] Par 78 of the preamble to the GDPR says "the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features."

[296] This applies both to personal and business identities. Note, however, that progress towards a consistent system that supports unique identification is more advanced for businesses, including – for some purposes – unique identifiers at EU level. The distinction between unique identification and identifiers is made in recognition of the fact that many legacy identifiers exist, which can provide unique identification at EU level provided they can be located and used to gain access to associated data. For example, once BRIS is live, a European Unique Identifier (EUID) will be used for the identification of limited liabilities registered in the Member States.

[297] Before the eIDAS Regulation (910/2014/EU) was passed, virtually all Member States had some form of electronic ID (eID). However, despite the fact that approximately 2.6% of Europeans work in another member State and Europe's 23 million SMEs include 1.84 million who sell in other Member States and 1.15 that have or are foreign subsidiaries, virtually none of the existing eIDs work cross-border.

[298] See discussion in Annex VII.E regarding the treatment of biometric information for identification purposes under the GDPR.

[299] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[300] See https://www.eid-stork.e and https://www.eid-stork2.eu/.

[301] Note that SIS II directly addresses the issue of legal standing by including among its data copies of European Arrest Warrants (EAW) that have the same legal value as the originals.

[302] There have been proposals for EU-level databases on e.g. social insurance contributions and rights of movement, abode or work within the EU.

[303] In addition to absence from insolvency registers, this may involve certification that the business and the persons involved have not been and are not subject to criminal proceedings and other matters Unlikely to be reliably and widely available from Member State sources.

[304] E.g. the UK Disclosure and Barring Service maintains its own database of individuals who have been (or were about to have been) discharged or transferred to another post: because they harmed someone or might have harmed someone while working in a regulated activity. It provides certification based on these data and on data drawn from other databases including the above-mentioned EU-wide databases.

[305] Member States prosper in different ways using common economic, legal, organisational, service and technical infrastructures

[306] There may be transitional demands for e.g. education and start-up business support.

[307] "The good is the enemy of the best" or *vice versa*

[308] Specifically, the balance of cost savings and benefits to the parties under this scenario will be adversely affected; cross border activity will tend to involve entities with higher needs for public services and the returns to the destination country in terms of economic productivity, etc. are likely to be lower than under the favourable alternative.

[309] This could happen as a result of the use of common data models and simplified query procedures and the establishment of reciprocal or even outsourced arrangements to manage retained data and ensure their quality and coverage.

[310] In particular, the G2 entities are likely to receive more 'credit' from individuals and businesses than the G1 entities, since it is the G2 entities that impose the administrative burdens that OOP seeks to reduce.

[311] Nationalism tends to increase as a consequence of adverse economic outcomes at home due to austerity attitudes and policies; it also tends to increase after shared economic reverses due to 'adverse selection' perceptions that businesses and individuals arriving in the teeth of a downturn are less productive than in better times. See e.g. Drache, D. and LeMesurier, A., 2015. "Global Change and Uncertainty: The Paradox of Our Time: A Research Report on Sovereignty and the Magnetic Power of Interdependency" Available at SSRN 2581154.

[312] This will depend on how the macroeconomic picture affects Single Market solidarity.

[313] For example, exchanges of data between countries that are net suppliers and net demanders of education, or labour, or financial services might be expected to give rise to sustained linkages, with compensation coming from other forms of interaction or direct subsidy. The basis for this is the recognition that the G1 entity experiences more cost than direct benefit, while the reverse is true for the G2 entity. If the two countries have similar levels of G1 and G2 entities facing each other, the costs and benefits balance out; otherwise, it may be necessary for the G2 country to assist the G1 country in making the necessary CAPEX and OPEX expenditures.

[314] An example is provided by Estonia's transfer of the X-Road approach to Finland.

European Commission

Once-Only Principle for citizens and businesses: Policy options and their impacts

Luxembourg, Publications Office of the European Union

273 pages

ISBN 978-92-79-65335-3

doi:10.2759/393169

KK-04-17-066-EN-N

doi:10.2759/393169 ISBN 978-92-79-65335-3