Project acronym: CLARITY
Project title: Champion eGovernment applications to increase trust, accountability and transparency in public services
Grant number: 693881
Programme: Horizon 2020
Objective: NSO-1-2015 ICT-enabled open government
Contract type: Co-ordination and Support Action
Start date of project: 01 March 2016
Duration: 24 months

**Deliverable D2.2:**
Preliminary needs analysis for the up-take of eGovernment services in Europe

Author(s): Tom Demeyer, Ivonne Jansen-Dings (Waag Society), Thordis Sveinsdottir, Rachel Finn, Kush Wadhwa (Trilateral Research) Akrivi Vivian Kiousi (Intrasoft) Serdar Temiz, Mattias Axell, Viktoria Ratz, Toni Mickiewicz (Open Knowledge Sweden) Gustav Ulander, Eva Karlberg, Hugo Hedlund, Marie Larsson and Ingrid Thylin (Skellefteå Municipality), Oscar Corcho (Universidad Politecnica de Madrid), Maria Jesus Fernandez Ruiz and Victor Morlan Plo (City of Zaragoza).

Dissemination level: Public
Deliverable type: Final
Version: 1
Submission date: Due 31 August 2016
Table of Contents

Executive summary

1 Introduction ................................................................. 5
1.1 Public value .................................................................. 5
1.2 Methodology ................................................................ 6

2 Societal Needs ................................................................ 8
2.1 Introduction .................................................................. 8
2.2 User-centered design .................................................... 9
2.3 Engagement & Initiatives ............................................. 9
2.4 Challenges: privacy, ethics & accountability .................. 10
2.5 Good practice Cases .................................................... 11

3 Legal, Social and Ethical issues in open eGovernment .......... 16
3.1 Introduction .................................................................. 16
3.2 Legal, Social and Ethical issues in open eGovernment .... 16
3.3 Ethics in data practices ................................................. 19
3.4 Social issues and needs of citizens ............................... 20
3.5 Good practice cases ..................................................... 24

4 Public Sector Needs ........................................................ 27
4.1 The changing role of the public sector ......................... 27
4.2 From national guidelines to local priorities ................. 28
4.3 Skills and expertise shape the design of eGovernment services .. 29
4.4 Authenticity of An accountable and auditable eGovernment ...... 30
4.5 Data and reliability of digital services ........................ 30

5 Industry and Market needs .............................................. 32
5.1 Introduction .................................................................. 32
5.2 Setting the scene .......................................................... 32
5.3 The view from industry ................................................ 33
5.4 Overarching industry needs ..................................... 34
5.5 E-procurement ........................................................... 34
5.6 Certification of ICT skills and eligibility ................... 35
5.7 E-invoicing ................................................................. 37
5.8 Good practices in e-Invoicing .................................... 38
5.9 e-Identification (eID) .................................................. 39
5.10 Good practices in eID for businesses ....................... 40

6 Conclusions .................................................................. 41
EXECUTIVE SUMMARY

This is deliverable report D2.2 Preliminary needs analysis for the up-take of eGovernment services in Europe for the European Commission funded project CLARITY. It presents the work of the project consortium on the analysis of societal, industry and public sector needs, with regard to the provision of open eGovernment services in Europe. Building on D1.1 Stakeholder Taxonomy and D2.1 Drivers of change in open eGovernment we look at the needs and needs assessment methods required for a successful continued transition towards open eGovernment. This document presents the preliminary findings of a desk based research, which will be validated and updated in foresight focus groups and presented in a subsequent deliverable D2.3 Considerations for the up-take of eGovernment services in Europe.

Societal changes and technology developments offer a huge potential for innovation in government and the democratic process. There are however also plenty of opportunities for mistakes if needs are not fully explored, and technology supply and innovation are left to steer the course of open eGovernment application design, development and implementation. The CLARITY partners conducted desk based research and reviewed policy, academic and grey literature to ascertain the key needs of societal actors, industry and public authorities.

We found that with regard to societal needs, user-friendly and accessible services that citizens can trust is presented as the most prominent cluster of needs that drive the up-take of open eGovernment services. We also found that local services need to be seen as relevant to citizens and have root in their communities. Strong user communities around eGovernment services is also a benefit that drives uptake. The issue of user-centred design should be stressed in the provision of public services, and accessibility for disabled, marginalised and older people should be considered at all times. There is also a need to keep other lines of communication with public authorities open, to compliment services provided online. Trust in services also needs to be raised through committed approach to privacy and data protection and explicit statements of how citizen data is used. Responsibility in data analytics and use is also paramount, to avoid any adverse effects on sections of the population.

The public sector needs are complex as we found that many public service providers are in a transitional phase, attempting to meet the demand for high quality personalised services at a lower cost. The needs also vary between the local and national level of service provision, as local government looks to the national government for direction, policy emphasis and funding for open eGovernment initiatives. The key needs of local services are regarding dedicated funding and staff with skills in digital service design, development and provision so that high quality services can be provided. As it stands, skills are lacking and public authority staff struggle with the new demands placed on their roles and technical uptake is slow. Many public authorities also have a need for guidance on legal, ethical and digital issues overall. On the national level, political awareness and urgency and support regarding eGovernance is lacking and a holistic vision missing in many countries. Knowledge building and retention regarding ICTs is an ongoing issue the public sector. Finally, procurement of all operational systems needs to be eGovernment and open data aware to make an eGovernment financially sustainable.

The single digital market is the main driver for industry in general and for the ICT sector especially. Transparent and modular (e)-procurement, open standards, independence of proprietary solutions will support a level playing field for suppliers big and small. Facilitating cross-border business with regulated e-identity and e-invoicing systems as well as certification
policies should also be implemented to assist industry in easing procurement across Europe. There is also a need for a more open and transparent procurement system across Europe and some steps have been taken in that direction and we present good practice examples in section 5.
Overall we found there to be a strong interest in open eGovernment services among all stakeholder groups, and there are a multitude of interesting developments and applications that are being used within the Member States, a small example of which are described in the document. Following the identification of needs of the three key groups (citizens, industry and public authorities) the CLARITY partners will take stock of available applications and then identify, by using a gap analysis, where innovation and further development is needed in open eGovernment services.
1 INTRODUCTION

In the development of Open eGovernment throughout Europe the focus of governments has been to support administrative processes, improve the quality of the services and increases internal public sector efficiency. Digital public services potentially reduce administrative burden on businesses and citizens by making their interactions with public administrations faster and efficient, more convenient and transparent, less costly and can unlock further economic and social benefits for society as a whole.\(^1\)

With the EU eGovernment Action Plan 2016-2020 the European Commission aims to provide a dynamic and flexible approach for member states to pursue their own strategies and activities, while at the same time be able to join up efforts and prevent further fragmentation in the delivery of digital public services. The core vision of the Action Plan is as follows:

By 2020, public administrations and public institutions in the European Union should be open, efficient and inclusive, providing borderless, personalised, user-friendly, end-to-end digital public services to all citizens and businesses in the EU. **Innovative approaches are used to design and deliver better services in line with the needs and demands of citizens and businesses.** Public administrations use the opportunities offered by the new digital environment to facilitate their interactions with stakeholders and with each other.\(^2\)

In order to create a better understanding of the needs and demands of citizens, businesses and governments themselves better in relation to digital public services, we will investigate in this document the way society, public sector and industry are finding out about the different needs (current and future) that exist in relation to Open eGovernment. We will look at currently used methodologies and newly formed collaborations in order to successfully identify the needs of different stakeholders and the way that these findings are being translated into actual services that fit the user’s needs.

1.1 PUBLIC VALUE

Open eGovernment can be defined as a government open to the contribution of citizens and society to create **public value** and engaged to respect three main principles: ensure full **transparency** of its actions, its processes and its data, enable **participation** of citizens to its decisions and processes, promote and accept the **collaboration** of citizens to the production of its services.\(^3\)

For many governments **transparency** is a high priority policy objective, however the equally important **participation** and **collaboration** have been underrated in the past. When designing digital government services all of these aspects should be considered as it will help government transition from traditional service provider to being open and flexible partners for citizens and business.

It is key we keep **public value** as a guide in the development of Open eGovernment. “Public services are services offered to the general public and/or in the public interest with the main

---

2 Ibid., p.3.
purpose of developing public value. Public value is the total societal value that cannot be monopolized by individuals, but is shared by all actors in society and is the outcome of all resource allocation decisions.4

In the process of transitioning to an Open eGovernment public authorities need to find the tools and methods that help them reach transparency, participation and collaboration in order to create true public value. This will to some extent mean redefining their role in the digital services infrastructure, as many services will be created and maintained outside of government itself.

Big companies like Google and Apple are already providing many public services like cartography, mobility and healthcare information. But also smaller and local businesses play into this need, with applications to interpret service (open) data like garbage pickup times, or with services around for instance health or childcare. And even citizen (communities) are finding ways to become their own service provider for their own local needs.

By adhering to the principles of open eGovernment public bodies can harness all of these developments and integrate them into their own policy making process. It is crucial that the creation of public value is at the core of this process and that open access to these services it protected, whether they be infrastructure (i.e. Internet of Things or connectivity) or processes (i.e. decision making or participation).

1.2 METHODOLOGY
Understanding the needs of the different stakeholders in the Open eGovernment field can help public bodies identify effective measures that fill the discrepancy between the current condition and wanted condition, either through improving performance or by correcting a deficiency, for instance. Tools that help identify needs can clarify problems and identify appropriate interventions or solutions. They can help improve the quality of policy or program decisions and help guide subsequent decisions. We do assume, however, that needs are not assessed ‘from a distance’ but this assessment is itself part of a User-Centered Design process. Also, needs are not static entities; priorities change, and needs may be met through other means than policy changes or eGovernment practices.

In creating this document, we have investigated the Open eGovernment domain in two ways. First by reviewing relevant literature on open government, eGovernment services and innovation. We focused mainly on recent academic and policy literature that specifically addresses the changing relationship between the different stakeholders in the ecosystem. Second by investigating successful applications of Open eGovernment services, specifically looking at the tools and methods used to become one of the innovators of government digital services.

This needs assessment focusses on societal, public sector and industry needs concerning the provision of eGovernment. First we will focus on societal needs, with the following chapter zooming in on the legal, social and ethical issues with eGovernment provision. This will lead into a closer look at the public, i.e. governmental, needs surrounding this topic. After that we focus on the needs of the private sector. Throughout the document cases are presented to show

---

D2.2 Preliminary needs analysis for the uptake of eGovernment services in Europe

how needs are identified in practice, specifically on the topics: general practice health, local government services, small business and self-employed and disability.
2 SOCIETAL NEEDS

2.1 INTRODUCTION
When discussing Open eGovernment the discourse mostly discusses government as a service provider, and the various stakeholders as receivers of these services. eGovernment however should be seen as a dialog between stakeholders and government(s). The services that government provides stem from or are enabled by stakeholders themselves; government is in this sense a mediator in service provisioning. The digital transition will make this much more explicit and operationally effective.

When we talk about stakeholder needs, we find it helpful to see eGovernment as a partnership between government(s) and societal stakeholder groups (or ‘roles’), and not strictly as a service provider.

On the European level, however, the perceived (or real) distance between local and national interests and the European bureaucracy makes the perspective of government as a dialog between (ideally equal) partners a challenging one. This is exactly where eGovernment with its related technologies could make a difference. Well provisioned, and addressing the right subjects and issues, eGovernment technologies are able to cross boundaries of distance, language, culture and scale that more traditional forms of government do not so easily handle.

Instrumental service provisioning remains an important aspect of eGovernment, and on the European level the CEF building blocks\(^\text{6}\) may grow to be a valuable ecosystem that will enable many services.

To find out which of these services are needed, and to find out whether they function and address the right needs requires a dynamic dialog. The same is needed for the design and building of these services. Methods of user-centered design, co-creation and design thinking provide an indispensable contribution that is lacking, to an extent, in current public service delivery\(^\text{7}\). It may also provide for shared ownership and establish a stake in successful deployment and use for all engaged stakeholders.

The field of eDemocracy and that of eGovernment are of course closely related; we could see the latter as an executive branch of the former. Successful eGovernment needs, at least in the longer term, a successful eDemocracy, as the cycle of design, use, evaluate and feedback never stops. One can see eDemocracy as a constituent part of eGovernment, insofar as democratic mechanisms are organized and facilitated by the government, and the government itself, in turn, is a result of those mechanisms and processes.

In this respect we look at methods of eDemocracy as a means to discover and establish the needs and priorities for Open eGovernment.

If the mechanisms of eDemocracy have begun to prove themselves, it is at the local level. To bring them to Europe needs work, to say the least. First, the needs and priorities of eDemocracy, in turn, need to be established, albeit on a higher, more abstract level.

---


\(^6\) The CEF Building Blocks, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home

We mention three critical aspects:
- Trust
- Community
- Usability

**Trust** is paramount; without it there can be no thought of democratic engagement. Trust depends on both **security** and **privacy protection**, but to a very large extend also on communication, design and governance of the processes and tools.

**Communities** run through all stakeholder groups. They form around a theme, an issue or an interest. They may be composed of people or organizations in very different societal roles, public officials, citizens, scientists, SMEs or corporate interests. Without a means to build and address these communities there can be no meaningful deliberation or decision making.

**Usability** is key in eGovernment. The current CEF building blocks go a long way towards providing a rich enough set to provide basic capabilities for eDemocracy tools that can provide for a European-wide participation and deliberation ecosystem, with the exception of the communities’ aspect, which may need to be addressed at a higher level. Implementation of the various building blocks will determine their ultimate usability in this context (anonymous authentication, voting, auditability). We do need to recognize that much work has already been done on eDemocracy tools\(^8\), which would provide for a running start; recognizing common issues and successfully addressing communities across European borders will remain a formidable challenge, but will also provide many opportunities.

Tools which are obscure or hard to use are very quickly abandoned, or not even considered. Despite being almost a cliché, **user-centered design** is not commonplace at all in the systems and tools developed through or for the European bureaucracy. However, this practice does help identifying needs in an early stage of development.

### 2.2 USER-CENTERED DESIGN

“User-centered design (UCD) is a design philosophy where the end-user’s needs, wants and limitations are a focus at all stages within the design process and development lifecycle. Products developed using the UCD methodology are optimized for end-users and emphasis is placed on how the end-users need or want to use a product instead of forcing the end user to change their behavior to use the product.”\(^9\)

Putting the user at the center when designing services and processes seems evident, but is hard, and often neglected in practice. There may be focus groups or test panels, but these are only part of the process; it begins with questioning the question. There is no specific management approach implied by UCD, but the process is iterative and the end users are involved throughout the design and development of the service, process or product. UCD is needed in order to create a good user experience, which increases performance and satisfaction, and avoids many of the pitfalls that make services (or software) fail, make them hard to use, or difficult to ‘take up’.\(^10\)

### 2.3 ENGAGEMENT & INITIATIVES

---

\(^8\) D-Cent Tools, [http://dcentproject.eu](http://dcentproject.eu)

\(^9\) Definition from: [http://www.webopedia.com/Term/U/user_centered_design.html](http://www.webopedia.com/Term/U/user_centered_design.html)

“We, citizens of all cities, take the fate of the places we live in into our own hands. We care about the buildings and the parks, the shops, the schools, the roads and the trees. But above all, we care about the quality of the life we live in our cities. Quality that arises from the casual interactions, uncalled for encounters, the craze and the booze and the loves we lost and found. We know that our lives are interconnected, and what we do here will impact the outcomes over there. While we can never predict the eventual effect of our actions, we take full responsibility to make this world a better place.”

The above quote comes from *A Manifesto for Smart Citizens*, by Waag Society. Unlike many collaborative statements created about citizen engagement this document puts the citizen front and center. It shows that citizens are willing to use the knowledge, ambition and skills they have in order to take responsibility of their own environment and create solutions that fit their own (local) needs. Many everyday challenges and needs of citizens are currently not being addressed by government services, either because adoption rates of new technologies by government agencies tend to be slow or because certain specific needs of (small groups of citizens) are low on the list of the cities priorities.

Citizen led initiatives can be defined as: “Collective activities initiated by citizens aimed at providing local ‘public goods or services’ (e.g. regarding the liveability and safety) in their street, neighbourhood or town, in which citizens decide themselves both about the aims and means of their project and in which local authorities have a supporting or facilitating role.”

The opportunities for these citizens to self-organize and design and implement local solutions is of clear value to government agencies and should be nurtured as part of the Open eGovernment ecosystem. For government this form of co-production may be additive - adding more user and community support to professional interventions - or substitutive, replacing government efforts with resources from users and communities.

It creates opportunities for government to take a facilitating role in regard to service provisioning, either by network structuration (by helping communities understand domain specific rules and regulations, for instance) or by process management, like trust building, interpersonal contacts, shared understanding and commitment.

It also creates opportunities for government to enter into dialog with citizens on issues related, but outside the scope of the current project, in order to discover further needs and establish priorities.

### 2.4 CHALLENGES: PRIVACY, ETHICS & ACCOUNTABILITY

Rather than just rolling out services using (IC) technology, the ubiquitous use of ICT changes government, as it changes society. Where ‘eGovernment’ suggests the use of tools to better and more efficiently govern; it also initiates changes and provides the means for a transition to an ‘iGovernment’, an “information government”\(^{13}\). The reasons for using ICT change from efficiency and productivity considerations also to management, care and control, the existential core of government, which is a cause for concern because control and functioning of the technology used is not subject to the democratic process on the one hand, and is rarely fully appreciated in its consequences on the other.

---

Technology is not a neutral force; when used as a simple tool this is less relevant, when used in a decision-making, care or control process it is a different matter. The availability and marketing of a particular system in itself is already a political choice. The decision to use a particular system is made by consultants with interests not necessarily aligned with the public cause, the expertise needed for deploying and running the systems is left to the supplier and the precise functioning a proprietary black box, in some cases. A government run by systems it does not control or even understand cannot be accountable; one of the core values of a democratic society.

In a ‘big data’ iGovernment, bodies operating in very different domains will increasingly make use of shared pools of information from varying sources which are no longer any one’s particular responsibility. No one knows precisely who is responsible for much of the information (or its accuracy), and no one has a comprehensive overview of its sources, and thus of the implications that particular use-cases may have, for instance in regards to citizens’ privacy.

Data is frequently imperfect; it becomes very hard, or impossible, to assess these data in terms of inclusiveness, or in terms of bias. The choice of data labels is subjective, the decision to include or exclude research or data, and many other choices can no longer be judged in their original context, and usage of the data becomes contentious. “Unthinking reliance on data mining can deny historically disadvantaged and vulnerable groups full participation in society. Worse still, because the resulting discrimination is almost always an unintentional emergent property of the algorithm’s use rather than a conscious choice by its programmers, it can be unusually hard to identify the source of the problem or to explain it to a court.”

2.5 Good Practice Cases

By showing a couple of cases of eGovernment on the subjects of general practice health, local government services, small business and self-employed and disability, we want to identify a few examples of how needs are assessed in practice.

Smart Citizens Lab

---


In the Smart Citizens Lab, citizen-lead communities explore tools and applications to map and measure the world around them. Along with experts, scientists, and designers they deal with themes ranging from air quality to the conditions of swimming water to noise pollution. Building and using simple sensor and toolkits, and interpreting and visualizing the results, participants are better equipped to engage in dialogue about their living environment and better express their needs and concerns. A set of tools, methodologies and best practices for orchestration of bottom-up citizen science and data sense making will be developed, through which needs and priorities can be assessed and issues can be put on the agenda.

CitySDK / Issue Reporting

CitySDK is an EU CIP project which dealt with harmonizing the IT interfaces to public administration across Europe in three domains: tourism, participation and mobility. It researched and implemented systems and API’s in order to facilitate third party service providers across Europe. Small-scale IT providers (app builders, SMEs) can write eGovernment apps and services that work in different countries and cities, making the potential market a much bigger one and development economically more feasible.

By concentrating on a limited domain and functionality, as well as adopting emerging (global) standards, inroads can be made in what otherwise can be a very hard nut to crack. Also, selecting eGovernment services where the link with internal operational systems is narrow and well defined, like open-311, makes adoption by administrations cheaper and thus a lot easier. The Issue reporting API enables:
- Submission of issue reports via third-party apps and services

---

- A standardized reporting protocol with service-request categories defined by each city
- Sending of media and location details along with issue reports
- Searching and follow-up of submitted reports and their status

The need for a streamlined interface to local issue reporting is driven from both the side of the local government and from the citizen perspective. A multi-channel interface to the city, through various apps, as well as through web-site of a local paper helps people to easily find the service. A single interface makes sure the issues reach the right department, and that feedback on follow-up is possible.

*Datalab Amsterdam*

![Datalab Amsterdam logo](image)

Datalab Amsterdam is a workspace, knowledge center and partner in data-centered innovation in Amsterdam.\(^{18}\) It provides advice, data (where possible) and helps build innovative solutions for the city. It is fully funded by the city of Amsterdam.

The approach taken by the DataLab is that implementing and demonstrating fixes for relatively small-scale problems, with a short lead time, has two effects. Firstly, the problem is addressed, of course. Secondly, it is demonstrated that short, agile and pragmatic ways of addressing issues can actually lead to workable solutions. The desired effect is a change in culture as regards to ICT-based projects, which historically have been big, costly and hard to manage. Also, external consultants and IT suppliers are replaced by an internal, agile, problem-solving oriented group of developers. This is very much inspired by the methods and goals of the code-for movement\(^ {19}\).

The challenges (as they are called) taken up by the datalab, the needs that will be addressed, are solicited actively amongst local neighbourhood coordinators (civil servants), local NGOs, retail, SMEs and other societal actors. Then follows a challenge intake assessment checklist to prioritize the issues taken on.

---

\(^{18}\) Datalab Amsterdam, [https://www.datalabamsterdam.nl](https://www.datalabamsterdam.nl)

\(^{19}\) Code for America, [https://www.codeforamerica.org](https://www.codeforamerica.org); Code for NL, [http://codefornl.github.io](http://codefornl.github.io)
The GoOV APP is an app on a smartphone for anyone who has trouble traveling independently, such as people with intellectual disabilities, cognitive disorder, or seniors. GoOV helps them travel safely and with confidence using regular public transport. This obviates the need for special transport solutions; people learn to be more independent, and they are saving a considerable percentage of their care budget.

Using a list of pre-prepared locations, the app guides the user from door to door using simple and intuitive instructions. Walking routes are made available and real-time transit information enables accurate instructions on where and when to get on or off public transport. When the user gets ‘stuck’ there is an emergency button which connects to a help line that can help the passenger to get on their way again.

The needs from an eGovernment perspective are twofold. The care budgets are under pressure, and specialized transport accounts for a large chunk of the personal budgets. First, looking at IT supported solutions that help alleviate budgetary concerns and improve life for those concerned, the responsible local councils and care institutions need an open mind and willingness to experiment and adapt ‘standard operating procedure’ to facilitate new developments. Secondly, provisioning standardized real-time transit information is now part of the procurement process and contract with transport companies in the Netherlands and other EU countries.

---

20 GoOV, http://www.go-ov.nl
The Whitebox\textsuperscript{21} is a small box in the practice of a GP, which allows for one-on-one access to a personal health care file by another health care provider. This caregiver can retrieve data directly, without going through a central system. The GP can, for instance, give a focused access to a pharmacist, or a specialist, and to nobody else. At the basis is the understanding that the GP is best custodian of the patient’s health care records. The White Box allows for very selective sharing of information, which remains in the GP’s regular administrative systems. The white box is a proxy to those regular systems. It can generate specific, encoded URL’s (which may also be printed, to be given to the patient), that allow limited access to particular information, for particular professionals. In the Netherlands there is no central registry for patient records. A proposal for a central connecting hub was rejected by parliament because of privacy concerns. A solid, secure and privacy preserving way to share health record information is seen as beneficial for health care practice by both health care professionals and patients.

\textsuperscript{21} Whitebox, https://hka-pilot.nl/
D2.2 Preliminary needs analysis for the uptake of eGovernment services in Europe

3 LEGAL, SOCIAL AND ETHICAL ISSUES IN OPEN EGOVERNMENT

3.1 INTRODUCTION
For the ongoing development, provision and uptake of open eGovernment services it is imperative that social, legal and ethical issues are considered. When EU citizens were surveyed on the reasons for not using online channels for submitting official forms, the following picture emerges, which demonstrates that to some extent there is a lack of open eGovernment services, but more clearly that issues pertaining to social, legal and ethical dimensions are very important.22

![fig. 3.1 Reasons for not using online channels when submitting official forms (Source: Digital Agenda Scoreboard 2014)](image)

As can be seen, the key reason is that citizens do prefer a personal contact and a visit to submitting forms online. Furthermore, trust emerges as a strong reason in different ways, e.g., more trust in submission by paper than by electronic means and concerns about data protection and security. Last but not least and important barrier of lack of skills and knowledge is mentioned by almost 15% of users.

This section will specifically look at legal, ethical and social issues regarding the provision and uptake of open eGovernment services, with a focus on citizen’s needs and will conclude with a number of good practice examples that can serve as assistance to public authorities who are faced with some of the barriers detailed in this report.

3.2 LEGAL, SOCIAL AND ETHICAL ISSUES IN OPEN EGOVERNMENT

“Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.”23

Societal needs regarding the legality and ethical conduct in open eGovernment provision and development are the focus of this chapter. The fundamental principles laid out in the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union will be used as guidance to cover citizen needs regarding open eGovernment services.

As much of open eGovernment initiatives rely on data to provide personalized services, to fulfil the “once only” principle and operating between institutions and across borders, this section will focus specifically on the legal, social and ethical issues regarding privacy and data protection relevant to open eGovernment services. Data protection and privacy of citizens is the subject of a wider legislation at both European and Member State levels, e.g. UK Data Protection Act 1998, Charter of Fundamental Rights of the European Union (article 8), as well as the newly established General Data Protection Regulation.

Regarding data protection, the Oxford Internet Institute states:

“data protection rules do not, in principle, prohibit the use of personal data but they offer a legal framework to allow data processing – provided specific requirements are met and special rights are granted to data subjects. The major principles encompassed by such rules are: respect of the purposes of data processing announced at the time of data collection; proportionality (balance between the interest of processing data and the data subjects’ interests); and transparency.”

Considering how vital data is to the provision of open eGovernment services, it is clear that data protection and privacy regulation could be considered a difficult barrier for the ongoing development of the field. In May 2017, the General Data Protection Regulation will be implemented across Europe. Its broad significance is that it will create stronger data protection laws, with the aim of making the region the safest worldwide, in terms of data protection. The regulation has exemption clause for Member States and allows them some discretion when processing data is considered to affect ‘public interest’. This could apply to the provision of open eGovernment services as governments “may restrict the scope of the obligations and rights, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure”.

Governments collect and share data to an increasing degree in order to e.g., personalize services, fulfil the ‘once only’ registration principle and ensuring interoperability of data within and across borders. For citizens it is thus increasingly necessary, for the purpose of accessing open eGovernment services, to submit their personal data. Research has shown that new ICTs have greatly impacted on citizens’ concerns for their privacy and their trust towards data collection and storage by organizations. High profile data losses and a perceived lack of control over their data fuels citizens unease, which can result

---


25 Ibid.


in lack of trust in e services and products and consequent lack of take-up. For example, in the UK, the National Health Service has repeatedly been fined by the Information Commissioner’s Office (ICO) for losing hardware with patient data, sending patient data out to third parties and making mistakes in handling patient email addresses when sending out mass communication.28

Personal data is valuable and increasingly at the risk of theft. Public authorities, at all levels, now hold large quantities of data on the individuals and their practices within their remit, this can range from non-personal data, (e.g., parking and bin collections), to highly sensitive data on health, social circumstances, and financial data, such as bank details.

In addition to concerns over data theft, there are also concerns regarding the data practices of public authorities, whether data is anonymized, encrypted, shared, published and used. Enhancing citizen trust is imperative for furthering the take-up and development of open eGovernment services, as these rely on user data to operate fully. Lack of trust in how the government manage citizen data, and concerns about lack of data protection, and privacy safeguards, can discourage citizens from using electronic services.30 The EU eGovernment Action Plan 2016-2020 stipulates that in order to increase trust in and take-up of digital services,

“All initiatives should go beyond the mere compliance with the legal framework on personal data protection and privacy, and IT security, by integrating those elements in the design phase.”31

For this purpose, it is imperative for open eGovernment service providers to know and understand user needs regarding privacy and data protection and operate according to law and ethical principles regarding collection of data on individuals. According to a report from the Information Commissioners office in the UK the recurring themes, emerging throughout the research literature, of what citizen’s want and need from data protection, are:

- ‘Control over their personal data;
- Transparency – they want to know what organisations will do with their personal data;
- To understand the different purposes and benefits of data sharing;
- Security of their personal data; and
- Specific rights of access, deletion and portable personal data.’32

Control and access to their personal data for citizens is imperative to increasing trust in data collection, storage and analytical practices of eGovernment. Research by ScienceWise in the

---

28 NHS tops the list for serious data breaches last year, Margi Murphy, 9 April 2015 for ComputerWorldUK: http://www.computerworlduk.com/security/nhs-tops-list-for-serious-data-breaches-last-year-3607138/
UK found that the public is particularly concerned about losing control of their personal data. Access and control allows citizens to make better informed decisions regarding services, and allows them to correct or remove incorrect information or sensitive data from their records. It also allows citizens to withdraw sensitive data or data they are not willing to share. With open eGovernment services specifically, citizen access and ownership of their data would fuel trust and allow for increased cooperation and shared responsibility of open eGovernment programmes, e.g., health, welfare and education. In health and disability services, this is increasingly important as the drive for personalisation, giving patients increased responsibility, empowerment and a voice in how their services are designed and developed. Evidence gathered by the RCGP demonstrated that access to electronic health records by the patient encouraged good record keeping practices by staff and allows patients to improve the accuracy of their record, and take increased responsibility for their health.

Increasing transparency in government is an on-going mission within the EU and the Member states, whereby governments attempt to open up their processes for legislation, regulation and overall decision making, as well as open up government data. Government transparency about their data practices is important when increasing citizen trust. When citizens submit their data, they need to know how and for what purpose their data is collected, and whether this data will be shared with other government departments, or third parties. Citizens should also be made aware of “mission creep”, when data is used for purposes other than their primary function. Transparency in data protection procedures, as well as information on how open eGovernment services intend to safeguard their users’ data and privacy need to be clearly presented and accessible for citizens to scrutinise.

When it comes to their data, citizens need know what measures are being taken to keep data safe, as well as who has access to their data. Access to data should be kept to a strict “need to know basis” and access controls should be used to enforce this rule. All those handling confidential data should also be aware of their responsibilities with regard to confidentiality, privacy and data protection. This is specifically important with regard to sensitive data, e.g. health data. Citizens should also be aware of data sharing within organisations and whether their data is being linked to other data about them in different departments or sections public service. In the UK, patients have the right to request that their health information is not used beyond their own care and deny the extension of access to parties outside of their main healthcare team.

3.3 ETHICS IN DATA PRACTICES

“In today’s digital environment, adherence to the law is not enough; we have to consider the ethical dimension of data processing.”

37 Ibid.
Ethics in data practices have become prominent with the rise of big data analytics and data mining. Governments now use their citizen data with the aim of improving service delivery and cutting costs by targeting services where they are needed. The ethical conduct of data analysis is derived mostly from research ethics and touches on the principle that research should not result in damage to or discrimination of individuals or groups.

With the rise of big data mining, whereby public and private organisations examine large data bases with the aim of creating new information and services, concerns have been raised that data practices may contribute to discrimination and assumptions about individuals and groups within society, based on weak links between variables. Seifert, (2004) cited in Bean, et al (2009)39

“1) A dependence on data patterns and relationships determinations by analysts, 2) varying competencies and deficient analytic skills of specialists interpreting the data for knowledge management (KM), 3) falsely identifying relationships between variables that do not necessarily equate with causation, 4) misunderstanding information awareness issues of data quality and integrity, 5) mission creep (or the use of data beyond its primary collection), 6) privacy of data, 7) inadequate security of data (based on the interoperability needs of several organizations and user groups and the complexity of the distribution), 8) ethical breaches of users and suppliers of information, and inadequate attention to laws and insufficient policies”

The analysis of datasets has great potential for open eGovernment so that services can be developed and adjusted according to the needs of citizens. This also has the potential of great cost savings for service providers. However, it is imperative that data is analysed correctly and ethically and that findings are not used to discriminate, track and identify individuals and groups within society. Care should be taken that data analytics does not further stigmatisation and exclusion of populations and geographical regions. An example of this would be analysis of health data to map out geographical spread of stigmatising diseases (e.g., HIV) and linking this further to ethnicity, although carried out for the purpose of targeting care, can further the stigmatisation of groups of patients, causing stress and damage to individuals. Same can be said for mapping socio-economic issues such as poverty, deprivation, and crime data, and linking to variable such as gender, ethnicity, race and sexuality. Furthermore, data should not be used in ways that citizens find objectionable, for example data collected from users of a specific services with the aim of improving said service, should not later be used to justify closure of the service as the data was not gathered for that purpose. Access to open eGovernment services should be enabled, not hindered by data analytics and citizens should never be discriminated against on the basis of government data and use of services. For this purpose, it is imperative that public authorities adhere to ethical data practices and ethical conduct of both research and data analytics carried out within their remit.

3.4 SOCIAL ISSUES AND NEEDS OF CITIZENS
“Providing services that are digital by default may exclude those on the wrong side of the ’digital divide’, i.e. those in society who do not have easy access to the internet because of poverty, physical handicaps, age, limited digital literacy or residence in areas such as rural communities with little or no access to broadband connections.”

Social and ethical issues pertaining the provision of eGovernment services are discrimination against those who do not have access, ability or skill to use ICTs to access public services. The digital divide is still present in Europe today and should be taken into account in open eGovernment service provision. The digital by default principle, as outlined in the EU eGovernment action plan 2016-2020 states that public administrations, while aiming to deliver more services digitally, should keep “other channels open for those who are disconnected by choice or necessity. In addition, public services should be delivered through a single contact point or a one-stop-shop and via different channels.”

The strategy thus recognises that not all citizens have the ICT means to use open eGovernment services. The below chart from Eurostat shows the percentage of individuals in European countries using the internet to interact with public authorities in 2009 and 2014. As is evident, the percentage has increased in all countries.

It is clear that Europe is a “mixed bag” when it comes to using the internet to use public services, consequently continuing the maintenance of other communication channels, e.g., face-to-face or telephone service desks, is necessary to help protect citizens against social exclusion and a lack of access to public services. The digital divide, which appears along the lines of income, age, digital skills, or geographical location, means that some citizens have a limited ability to participate using open eGovernment services while others may feel much more at ease, e.g., people who have grown up with access to ICTs.

---


Technical approaches (e.g., improving broadband access) are only one way of ensuring that excluded populations use open eGovernment services. Public authorities will also need to support digital skills training to ensure that all citizens can use open eGovernment services. Training of staff and officials is also necessary so they can better adapt to providing, advising and supporting online services.

Other factors that can lead to exclusion stemming from provision of open eGovernment services are lack of accessibility for the disabled and people who speak different languages. Open eGovernment services should be provided in accessible written text of various sizes, and audio transcription would assist those with visual impairment and services in accessible forms. Possibilities to engage with eGovernment services by other means than using a mouse should also be implemented. Government services should also take care to translate their service applications to a number of other languages that correspond with the demographics of the population served at any given time.

A number of standards and web accessibility certificates are now available for governments to consult so that they can provide the most accessible open eGovernment services for their citizens. These are listed in the good practices section towards the end of this document.

To summarise social needs of citizens, a list of recommendations from the Oxford Institutes on how to mitigate digital divide and accessibility barriers to eGovernment services is a useful list that demonstrates well the current needs, and how public administrations should respond to them:

Digital divides and choices

- Acknowledge that there is no single, simple ‘digital divide’ between those with and those without access to the Internet. Instead, there is a segmented citizenry with distinctively different eGovernment needs.

- Recognize the importance of the need to motivate choices among citizens to take-up eGovernment once they have access, as well as ensuring that access and the competencies to use that access are widely available.

- Target eGovernment to satisfy the requirements of citizens with different needs. For instance, the most ardent Internet users should be able to access everything possible online, as that is where they will expect to deal with government. Other Internet users need to be persuaded that eGovernment can provide the same benefits as e-commerce or e-banking. And non-users need to be given practical motivations to want to try digital Public Services.

- Develop multiple channels where appropriate (e.g. print or telephone call centres as well as online services). In addition, many non-Internet users know someone or an organization who can use the Internet for them if they need it. Government should therefore identify the relevant trusted intermediaries for particular groups and provide support for them in eGovernment initiatives.

- Offer easy-to-understand ‘meta-data’ guides to help navigation through information, websites and other eGovernment services.
D2.2 Preliminary needs analysis for the uptake of eGovernment services in Europe

- Create multilingual online support where needed.
- Provide documents in formats that can be easily accessed by a wide range of potential users.\(^{42}\)

Summary table for social, legal and ethical needs of citizens regarding provision of open eGovernment services.

<table>
<thead>
<tr>
<th>Social needs</th>
<th>Legal/Ethical needs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessibility for disabled people</td>
<td>Protection of personal data</td>
</tr>
<tr>
<td>Multiple channels of communication</td>
<td>Access to and control over their own data</td>
</tr>
<tr>
<td>Digital skills training</td>
<td>Transparency of data collection</td>
</tr>
<tr>
<td>Multilingual services</td>
<td>Transparent data practices</td>
</tr>
<tr>
<td>Access to the internet</td>
<td>Data access control for public servants</td>
</tr>
<tr>
<td>Access to internet enabled devices</td>
<td>Ethical data practices (collection, analysis, sharing, linking)</td>
</tr>
<tr>
<td>Providing as many open eGovernment services as possible</td>
<td></td>
</tr>
</tbody>
</table>

\(^{42}\) Oxford Internet Institute, op cit, p.150-151
3.5 **Good practice cases**

*Data collection, use, protection and privacy:*

The following screenshot is from the **Manchester City Council** in the UK\(^\text{13}\). It outlines step by step how the council collect and use citizen data. The page also includes a link to the full Data Protection Policy of the Council and a link to the Information Commissioner’s Office, which is the Data Protection Authority for the UK.

![Manchester City Council Data Protection page](https://ico.org.uk/for-organisations/guide-to-data-protection/)

**The Information Commissioner’s Office** in the UK provides a detailed and easily accessible guide to data protection in 8 principles\(^\text{44}\).

1. Data must be processed fairly and lawfully
2. Personal data must be processed for a specified purpose
3. The amount of personal data held must be adequate and not excessive in relation to the purpose for which it is processed
4. Personal data must be kept accurate and up to date
5. Personal data must be retained no longer than necessary
6. Individuals have rights in respect to their personal data
7. Personal data must be kept secure

---

\(^\text{13}\) Manchester City Council, *How we use your information*, no date. http://www.manchester.gov.uk/info/200031/data_protection_and_freedom_of_information/6845/how_we_use_your_information

8. Personal data should not be transferred outside of the EEA unless adequate protection for the rights and freedoms and data subjects is ensured. The General Data Protection Regulation\(^{45}\) (GDPR) in detail stipulates the measures necessary to safeguard personal data.

**Mydex**\(^{46}\) is a service that aims to empower individuals through ‘convenient, trustworthy access and control of their personal data and how it is used by them an others. Mydex offers services to public authorities by offering them access to citizen data (managed and kept up to date by citizens themselves). Councils can then request information if needed by sending an electronic request for data straight to the citizen’s digital letterbox.

![fig 3.4 Screenshot from the Mydex website](image)

**ISO/IEC 27001 Standard on Information security management**\(^{47}\)

This family of standards helps organisations to keep information assets safe, e.g., financial information, client data etc. ISO 27001 can help towards compliance with the newly established General Data Protection Regulation.

---


\(^{46}\) Mydex, no date. [https://mydex.org/](https://mydex.org/)

Accessibility:

The Campaign for Plain English has since 1979 “Crystal Mark” approved over 22000 documents worldwide. The Campaign offer accreditation services that award a seal of excellence for general documents for clarity of language. They now provide an Internet Crystal Mark for Websites after examining language, accessibility, navigation, design and layout of the site.

fig 3.5 Internet Crystal Mark from the Plain English Campaign

European Commission – Digital Single Market – Web Accessibility
Momentum for web accessibility is provided by the adoption of Web Content Accessibility Guidelines 2.0 (WCAG 2.0) and the adoption of a new European standard (EN 301 549) on accessibility requirements for public procurement of ICT products and services.

W3C Web Content Accessibility Guidelines
From January 2010 all new EUROPA websites have to be created in compliance with the Web Content Accessibility Guidelines 2.0 level AA. WCAG 2.0 is a technical standard, which included 12 guidelines that are organised under 4 principles: perceivable, operable, understandable and robust.

fig. 3.6 WCAG 2.0 seal awarded to accessible websites

Standard for Accessible ICT – EN 301 549
The European Standard EN 301 549 a European Standard for accessible ICT. It is intended in particular for use by public authorities and other public sector bodies during procurement, to ensure that websites, software and digital devices are more accessible for persons with a wide range of abilities. The standard documents provide a framework for developing a wide range of applications that will make ICT products and services more accessible for the 80 million Europeans who are living with various types of disability.

European Commission – 10 golden rules in accessible Web design
The EU Internet Handbook provides 10 golden rules for developing accessible websites in the form of a checklist. The EC claims that applying these 10 golden rules will solve 80% of accessibility barriers.

49 Web Accessibility Initiative (W3C), Web Content Accessibility Guidelines (WCAG) overview, https://www.w3.org/WAI/intro/wcag.php
51 http://ec.europa.eu/ipg/standards/accessibility/10_rules/index_en.htm
4 PUBLIC SECTOR NEEDS

The public sector is changing roles from the service provider into the facilitator role. In this chapter we will focus on these changes and how different challenges, such as local vs. national, government expertise and accountability, influence the needs of the public sector.

4.1 THE CHANGING ROLE OF THE PUBLIC SECTOR

Nobody can predict what changes lie ahead in the long term, for the public sector, but currently two of the main drivers reshaping the role of the public sector are changing demographics and budget cuts, as established in section 2.1 Drivers of Change in Open eGovernment. Changing demographics, with an ageing population, requires that a smaller tax base provides higher quality services to a larger population.

A digital public service approach fosters creation and implementation of new and improved processes, products and services. Opening up public data facilitates collaboration for the design, production and delivery of public services, across public bodies, and can result in cost reduction as well.

‘Digital by default’, ‘Once only' and 'whole of government’ are some of the three approaches that help digital government in terms of removing burden in government services and reducing cost52. ‘Digital by default’ is the approach where digital services are considered first, traditional service provisioning is secondary. ‘Once only' is related to the registering of data, where registering at one public body is enough to access the same data from all public bodies. Its complementary, a 'whole of government' approach, is the approach where related government services could be provided in coordination, as an integrated service. For example, provisioning of a death certificate triggers a change in the tax administration.

Open public data should be central to development plans and procurement by public bodies, and become an integral part of the governments operational context. In this way future technical changes, and thus extra cost, can be avoided.

Trends of individualisation and globalisation require that services may be customized to a larger extent and delivered in new ways. Governments need to create reliability and authenticity in an individualised world. Environmental factors need to be considered in all decision making. Mobility is another aspect, EU report on Citizenship states that EU citizens associate “moving and living freely within the EU” as a right with their EU citizenship, where public sector bodies are forced to coordinate within EU to deliver services to their citizens in the way (language, need) they require53.

The boundaries between public and private service providers are being distorted through digitalization. One example is an on-going initiative where Skellefteå municipality is addressing issues of the ageing population and the fact that parts of Skellefteå are sparsely populated. An international consortium of cities, universities and private companies are working on the use of ICT and digital eGovernment services as a way to make older inhabitants more socially active, improving their health and quality of life. Also, their access to, among

others, eGovernment services is being looked at. It does not only help municipality to improve its service but also SMEs that work with open data and public services can contribute and help economic growth, creating new jobs, greater innovation, and other improvements. An early conclusion is that the challenges, while similar in nature, differ between the different countries. In rural Ireland, for example, broadband connectivity is absent in many areas, while in Sweden, where broadband connectivity penetration is high, the services using these connections are seen to be lacking.

We need to add that the public sector is very slow to adopt and adapt to new technologies. According to van der Meulen, to establish an eGovernment model is just a first step on a journey to become a mature services organization. Historically the public sector created formation places to address issues, increasing the bureaucracy and also keeping unemployment down. Now, the shift is toward hiring consultancy companies and outsourcing technical work. This results in higher costs and poor continuity. More modern ways of looking at government and digital services are making headway, though, but the process is very slow.

4.2 FROM NATIONAL GUIDELINES TO LOCAL PRIORITIES

National guidelines implementation across EU are different depending on the character of the country. In some countries, local authorities and municipalities have more autonomy and relatively independent economy where they can partly decide their agenda on their projects and budget. In some countries, central government decides the most. When we look at Sweden, government is decentralised with its authorities and public bodies are very autonomous in comparison to many other countries. This has caused Open Government Principles and the legal implementation such as the PSI law (based on PSI directive), the Principle of Public Access (Freedom of Information) to be implemented differently from country to country. Data disclosure decision in different countries of course also vary with the type and context of data.

D2.2 Preliminary needs analysis for the uptake of eGovernment services in Europe

Implementation of PSI Directive had three different paths in EU member countries:

<table>
<thead>
<tr>
<th>Category 1</th>
<th>Category 2</th>
<th>Category 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Belgium</td>
<td>Austria</td>
<td>Bulgaria</td>
</tr>
<tr>
<td>Cyprus</td>
<td>Denmark</td>
<td>Croatia</td>
</tr>
<tr>
<td>Germany</td>
<td>Slovenia</td>
<td>Czech Republic</td>
</tr>
<tr>
<td>Greece</td>
<td></td>
<td>Estonia</td>
</tr>
<tr>
<td>Hungary</td>
<td></td>
<td>Finland</td>
</tr>
<tr>
<td>Ireland</td>
<td></td>
<td>France</td>
</tr>
<tr>
<td>Italy</td>
<td></td>
<td>Latvia</td>
</tr>
<tr>
<td>Luxembourg</td>
<td></td>
<td>Lithuania</td>
</tr>
<tr>
<td>Malta</td>
<td></td>
<td>Netherlands</td>
</tr>
<tr>
<td>Romania</td>
<td></td>
<td>Poland</td>
</tr>
<tr>
<td>Spain</td>
<td></td>
<td>Portugal</td>
</tr>
<tr>
<td>Sweden</td>
<td></td>
<td>Slovak Republic</td>
</tr>
<tr>
<td>United Kingdom</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In Category 1, 13 Member States have adopted specific PSI re-use measures. In category 2, 3 Member States have used a combination of new measures specifically addressing re-use and legislation predating the Directive, in Category 3, 9 Member States have adapted their legislative framework for access to documents to include re-use of PSI.\(^{59}\)

The EU eGovernment Action Plan 2011-2015 focused on technological enablers that facilitate access to and use of public services. The new eGovernment Action Plan 2016-2020 has goals:

- "to modernise public administration,
- to achieve the digital internal market, and
- to engage more with citizens and businesses to deliver high quality services."\(^{60}\)

Both e-government Action Plans 2010-2015 and 2016-2020 do not have a dedicated budget or funding instruments, except coordinating funding resources via EU programmes. One thing to note is that if there is no dedicated budget, public authorities are not likely to prioritize it.

4.3 **SKILLS AND EXPERTISE SHAPE THE DESIGN OF eGOVERNMENT SERVICES**

Elected representatives, in general, are lacking in necessary skills and expertise in to give shape to open eGovernment services. Municipal officials are also lacking these skills and expertise and rely on industry, mostly, to formulate needs and prioritize digitization and eGovernment. Reasons for this lack of expertise are the inability to change bureaucratic mind-sets and a lack of interesting positions for people with the right skills.

---

\(^{59}\) Implementation of the Public Sector Information Directive Accessed August 2016

The overall organization, however, requires more fundamental legal and digital awareness. An illustrative example is home care staff utilizing private text messaging services to exchange knowledge about patients. This serves an intrinsic need that the staff has. However, its utilisation is openly unlawful and contains risks for patient security. Complications such as these are bound to increase in the future.

The ability to formulate new needs and requirements towards vendors of ICT services needs to be strengthened in order be able to support new user requirements and an increase in service demand. National vendors, however, in general have monopolistic market positions and are not accustomed to responding adequately to the process change needed to adequately meet the new needs. Verhulst & Young (2016) state that a key challenge for the impact of open data is unresponsiveness to citizens’ needs.

The municipality requires more education and develop more skills in facilitating user participation and user-centered design in public e-service development. The reuse and sharing of available information are also areas of development. Managerial roles are also transformed through eGovernment developments.

Countries and municipalities that have an active ecosystem around open government are naturally the ones that are furthest on the road towards an Open eGovernment. Horizon 2020 and the EU are encouraging initiatives that help to improve skills and expertise in the local/national governments to make Open Data and Open eGovernment usable and accessible for everyone. Good examples are the 8 Diplohacks all over the world. Aims of these events was to facilitate Open eGovernment services that increase transparency in the European Union through the use of EU open data, as well as building a network and start a dialog between Diplomats and local hackers/designers across Europe.

4.4 AUTHENTICITY OF AN ACCOUNTABLE AND AUDITABLE eGOVERNMENT

By following the Administration & Service Law, the constitution, and Public Sector Information law properly, with new and radically inclusive methods for citizen involvement, the government could become a platform and facilitator trusted by society. Currently, the legal restrictions added to the 250-year-old constitutional Freedom of Information act work rather against innovation and transformation. The lack of a true and practical interpretation of this act may lead to mistrust of, or disinterest in, public services and open public government in EU countries.

4.5 DATA AND RELIABILITY OF DIGITAL SERVICES

In order to let public bodies to ensure correct and reliable digital services, the data used should be authentic, reliable and complete. Only authorized officers at public bodies should have the right to create, add, delete and modify the data in order to guarantee authenticity. The data should be provided from trusted resource. Enhancements and annotations to existing data datasets should be explicitly indicated as such; provenance should be clear at all times.

64 Diplohack, http://www.diplohack.org/
Data management policies and procedures that clearly state the rules for creation, use, and deletion of the data should be in place, and enforced. Digital assurance tools and procedures could help to fulfil this request.

Another challenge is the metrics of success. Financing and maintenance of open public data and related services becomes a contentious issue, since the cost is local, where the benefits are global, in many cases. Furthermore, when the goal is not to reduce cost but rather to improve the service quality or citizen satisfaction, measures of success of eGovernment services become hard to establish.

Governments should also establish a safe infrastructure (authentication, storage, standards) to prevent or resist cyber-attacks, corruption of information, and leakage of information. Also, a process or certification (quality control) of Open Data, in order for an industry relying on the quality and sustainability of the data to be able to build their services, may help. The Helsinki Region Infoshare aims to make information (urban and regional data) easy to access, free open to use for everyone. By focusing on four operational areas, production, opening, sharing and use of the data, have created in a more reliable data sources. HRI connects the data user and data owner in. In this way they have created in a more reliable data sources.

Also, choosing Free Software and Open Source in the technical implementation for the backbone of eGovernment infrastructure may not only increase trust in government applications, save tax payers money and reduce incompatibility from proprietary non-standards, it can also engage and motivate the largely digitally mature open source software community in co-creating and contributing voluntarily to the eGovernment services functionality. Open source reinforces strong security practices by involving many people that expose bugs quickly, and offers side-effects that provide customers and the community with concrete examples of reusable, secure, and working code. Flexibility and scalability of ICT systems is an important part of public sector need. Digital service infrastructure should be so flexible and should be able to address changing demands from public bodies as well as citizens in terms of content, use and development.
5 INDUSTRY AND MARKET NEEDS

5.1 INTRODUCTION
This section will focus specifically on the relationship between public authorities and the ICT industry with regard to provisions of open eGovernment services. In the first instance it will give a brief overview of the current policy landscape within which the provision of open eGovernment services exist.

The focus is on the development of a European framework for e-Commerce and the needs of businesses for increased clarity and seamlessness when trading across borders, within the Single Digital Market. This section will outline the 4 interlinked policy and practice areas that are currently under development to assist industry in this quest, i.e. e-procurement, e-certification of skills, e-invoicing and e-ID. Meeting industry needs within these four domains will allow for untold benefits to ICT firms, as well as other industries.

5.2 SETTING THE SCENE
E-enabled provisioning of public services to external customers has four main interactions: government-to-citizen (G2C), government-to-business (G2B), government-to-government (G2G), and government-to-employee (G2E). Streamlining these interactions as a service is a user-oriented process at the heart of an open eGovernment strategy. Evaluation results of the past eGovernment Action Plan 2011-2015 recognise that the Action Plan had a positive impact on the development of eGovernment at the European and Member State level, and this has paved the way for the subsequent 2016-2020 action plan.

Furthermore, the new eGovernment Action Plan is influenced by the creation of a single global online marketplace, The Digital Single Market, as an integrated standardisation priority plan with a focus on ICT technologies operating under a common European interoperability framework.

The Digital Single Market Strategy is built on three pillars:

- Increasing capability: Ensure the necessary ICT skills and resources are available to meet the current and future ICT needs of the Public Service.
- Improving access for consumers and businesses to online goods and services across Europe – this requires the rapid removal of key differences between the online and offline worlds to break down barriers to cross-border online activity.
- Creating the right conditions for digital networks and services to flourish – this requires high-speed, secure and trustworthy infrastructures and content services, supported by the right regulatory conditions for innovation, investment, fair competition and a level playing field.
- Maximising the growth potential of our European Digital Economy – this requires investment in ICT infrastructures and technologies such as Cloud computing and Big Data, and research and innovation to boost industrial competitiveness as well as better public services, inclusiveness and skills.\(^{67}\)

Overall during the last years, Information and Communications Technology (ICT) became the foundation of all modern innovative economic systems leading to a rapidly growing digital global economy. EU recognises the need for investment in ICT infrastructure, technology,

research and innovation that will result in services for e-government and, for instance, e-justice, e-health, e-energy or e-transport, which should also be interlinked and multi-lingual to complement and enhance development efforts.

Enabling cross-border mobility with interoperable digital public services is one of the basic targets of the new action plan. Administrations are expected to have a facilitating role that should help businesses operate online across borders within the Single Market, simplifying access to information under EU business and company laws and enabling businesses to easily start doing business, and expand and operate in other Member States. This will have to be achieved through end-to-end public e-services and in this new context. Although Europe has the capabilities to lead in the global digital economy, it is not currently progressing as expected.

The Commission supports an inclusive Digital Single Market and is setting the necessary framework for citizens and businesses to acquire the necessary skills and benefit from innovative solutions or services. In order to achieve this vision, the Action Plan identifies three policy priorities:

- Modernising public administrations using Key Digital Enablers (for example technical building blocks such as CEF DSIs like eID, eSignature, eDelivery, etc.),
- Enabling mobility of citizens and businesses through cross-border interoperability,
- Facilitating digital interaction between administrations and citizens/businesses for high-quality public services.

Within these policy priorities, the eGovernment Action Plan identifies 20 concrete actions that support national level strategies that set out to ensure momentum with ICT promoting action. In this light, the Public Service ICT National Strategies set out a high-level vision to reinforce ICT’s role in supporting Public Service Reform and transformation. At the heart of this reform agenda is a focus on specific commitments to changes such: as radically reducing costs in order to derive better value for money; placing customer service at the core of every action; maximising new and innovative service delivery channels; leading, organising and working in new ways; and building solutions with a strong focus on implementation and delivery.

5.3 THE VIEW FROM INDUSTRY

From the other side of the economic playing field, the industry perceives the public sector as the main engine to bridge the digital divide at a national level and boost development opportunities. In this light, industry stakeholders suggest that public agencies could start acting as model users of ICT and be catalysts for others to follow, aiming at maximising the growth potential of the European Digital Economy.

A good start would be to improve Governance ensuring that the ICT strategy is aligned, directed and monitored across all public bodies that support the specific goals and objectives at a holistic government level, emphasizing shared commitment. This can be achieved by digitisation of key transactional services and increased use of ICT to deliver improved efficiency within the public infrastructure, providing new digital services to citizens, businesses and public servants. The concept of “Build to Share” has been more frequently expressed, the last years, and creating ICT shared services to support integration across the wider Public Service infrastructure, is driving requirements such as efficiency, standardisation, consolidation, reduction in duplication as well as to controlling costs. Since online public services are crucial to increasing cost-efficiency and quality of the services provided to citizens and companies, the end result would be better public services.
In addition to that, the scope is extended to achieve inclusiveness by improving participation, opening up opportunities and enhancing skills (i.e. technological) as well as boosting industrial competitiveness. This then leads to increasing customer centricity for public services, which in turn will increase online take-up, especially when services are transformed into new accessible and usable solutions. New services, applications and content would create new markets and provide the means to increase productivity and hence growth and employment throughout the economy.\textsuperscript{68}

5.4 OVERARCHING INDUSTRY NEEDS

One of the reasons why consumers and smaller companies do not engage to a greater extent in cross-border e-commerce is due to complex and opaque rules that apply to business transactions between the Member States. Having 28 different national consumer protection and contract laws discourages companies from cross-border trading and prevents consumers from benefitting from the most competitive offers and from the full range of online offers\textsuperscript{69}. Overall, transparency and clarity with regard to procurement, regulation, invoicing and identification across borders would assist the ICT industry in contributing to a greater degree to the development and uptake of open eGovernment services.

5.5 E-PROCUREMENT

Electronic Procurement is a web-based, collaborative technology that aims to facilitate the full lifecycle of a tendering process and contract management activities related to the process and defined by the procurement initiator. This technology is meant to assist both buyers and suppliers, offering a secure, dynamic and collaborative interactive environment for allowing procurements of any nature, complexity or value concerning public sector organisations’ use of electronic means to purchase goods and services or to tender public works.

e-Procurement involves the following stages of a process:

1. electronic publication of notices announcing public procurement tenders (“e-notification”);
2. publication of public procurement documentation, such as terms of reference on the web (“e-access to procurement documents”);
3. and electronic submission of tenders by companies when responding to a call for tender (“e-submission”).\textsuperscript{70}

Currently, e-procurement is recognised as one of the key drivers towards the implementation of the “once-only” principle in public administrations\textsuperscript{71} such as the prequalification of economic operators (ESPD and e-Certis) and e-invoicing. The EU therefore considers procurement and standardisation as an important mechanism for the public sector to encourage innovation and entrepreneurship. It is also considered as important to improve the conditions for reuse of public information from government agencies for both commercial and non-profit purposes. In this light companies insist that the transition to electronic procurement should be sped up. Improved coordination of central government, municipal and county council procurement of ICT can promote this development. From experience and discussions with industrial representatives, e-Procurement is considered by procurers to be a powerful

mechanism, generating recognised best practices and enabling geographically dispersed groups of stakeholders to participate. It opens up business opportunities and increases transparency of public spending. As a recommendation companies state that creative flexibility within the laws is what is required; appropriate rules and regulations need to be established for the public benefit.

Many domestic governments wish to adopt sound public procurement rules around the world but the direction should be established by the EU. The digital transformation to e-procurement involves initiatives developed by the European Commission and EU countries. These initiatives aim to reform aspects of the public procurement process and are driving the transition into other broader Commission initiatives such as e-government and the reduction of administrative burdens. In addition, the Commission set up the Multi-Stakeholder Expert Group on e-Procurement (EXEP). This group gathers a variety of stakeholders whose work in their countries and within EXEP is vital for a successful transition to e-procurement. Nowadays many examples start making their way in ICT. A good example is Open e-PRIOR, (electronic Procurement, Invoicing and Ordering) which has been published as open source by the Directorate General for Informatics (DIGIT) of the European Commission.

Good practices in eProcurement

The European Single Procurement Document (ESPD) is a self-declaration form used in public procurement procedures by contracting authorities and businesses in the EU. Before the introduction of the ESPD, companies were required to submit various documents to prove that they fulfil the exclusion and selection criteria of a tender; for example, show to have paid taxes and have not been convicted of criminal activity. With the ESPD however, companies will be able to meet these obligations with a single ESPD self-declaration form. The actual documents will only have to be provided by the winner of the tender.

The Multi-Stakeholder Expert Group on eProcurement (EXEP) is based on the Commission communication on ‘End-to-end e-procurement to modernise public administration’. The group’s work focuses on the core issues necessary for a successful transition to e-procurement and is organised along three axes: regulation, governance and technical (solutions and interoperability) issues. EXEP aims to provide guidelines for developing e-procurement systems and build on existing resources such as the Golden Book of e-procurement practices.

5.6 Certification of ICT Skills and Eligibility

Effective performance of a job requires both continuous improvement and a strong innovation aspect (not only in ICT). It’s a common stance that in order to develop professionalism in i.e. ICT certification of skills in a personal or company level has become essential. ISO 9001(2008) is an example of such a normative document which defines general requirements and quality criteria to maintain certification schemes.

---

76 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3142
The EC boosted the activity for the formation of a mapping tool that would be used to identify and compare certificates requested in public procurement procedures across the EU in order to add value to the procurement procedure, boost competition and ensure a higher level of quality bidders. Before the introduction of the ESPD, companies were required to submit various documents to prove that they fulfil the exclusion and selection criteria of a tender, for example have paid taxes and have not been convicted of criminal activity. Now, companies are able to meet these obligations with a single ESPD self-declaration form.

**European Single Procurement Document (ESPD) and e-CERTIS**

The ESPD (European Single Procurement Document)\(^80\) and e-CERTIS\(^81\) play a crucial role in the digital transformation of public procurement. They contribute to EU countries’ transition to full e-procurement, significantly by:

- reducing administrative burden
- simplifying access to cross-border tendering opportunities
- driving companies to acquire proof and documentation that proves that their business fulfils the tender criteria (e-CERTIS)

e-CERTIS is a multilingual web service that helps tenderers and bidders identify certificates and offers:

- Free online guide of certificates needed for public procurement
- Data is verified and updated by national ministries in charge
- Appreciated both by buyers and bidders proving their eligibility.

**e-Certis is applicable for:**

- First-time bidders, new to procurement procedures (even in the same country as the contracting authority), e-Certis offers a handy reference system on the types of documents you’ll usually have to submit, and their contents.
- cross-border tendering – you may be asked for certificates that don’t exist in exactly the same form in your country, or for familiar information in a different format.
- contracting authorities – you need to be sure the documents you receive, possibly from several countries, meet the requirements in the terms of reference as regards content and the authority of the issuer.\(^82\)

The full potential of the eESPD will be reached when tenderers will provide links to repositories, which hold data proving their compliance with the exclusion and selection criteria.

Industry stakeholders are strongly supporting developments towards frameworks which motivate the availability of a common language to exchange information about offerings and bids, but also allow more space for new players to be involved in the EU government market.

Overall the tendency expressed by the latest developments in EU legislative and offerings level, we see a strive from the side of the companies to consider the EU as a potential customer and under this light comprehend eESPD as a “business passport” for tenders anywhere in the EU.


\(^{82}\) Ibid.
The European e-Competence Framework\(^\text{83}\) (e-CF) provides a reference of 40 competences as required and applied at the Information and Communication Technology (ICT) workplace, using a common language for competences, skills and proficiency levels that can be understood across Europe.

### 5.7 E-INVOICING

In recent years, throughout the EU, a process of clarification and simplification of the rules around e-invoicing and e-archiving has been taking place but in a rather slow manner. For example, in 2010 in Belgium, national legislation was simplified to enable companies to choose the technical means on how they could exchange and archive electronic invoices but at the same time no specific methods were recommended by the national VAT administration.

E-invoicing is a known technology with unrivalled benefits linked to boosting cash flow and driving business performance. Whereas many European countries are already considerably advanced in this field, a vast majority of organisations have not yet decided on the adoption of a single unique system or service to be used across countries that could support invoice issuers and recipients wishing to replace expensive paper-based invoice management. A high number of providers offer solutions and services for this matter. Compared to paper invoices, e-invoices are easier to process, they reach the customer faster and can be stored centrally at very low cost.

The European Commission lists the benefits of and barriers to e-Invoicing as:

- faster retrieval of money from customers by reducing the time an invoice or payment is in the post
- reduced printing and postage costs
- quicker and cheaper processing as the information in electronic invoices can be fed directly into a company's payment and accounting systems
- lower storage costs
- reduced training and system development costs.

At the same time however, e-invoicing faces obstacles such as:

- e-invoices are produced in a wide range of formats and according to many different standards. This hinders the smooth transfer of an e-invoice from one place to another, and prevents the realisation of the full benefits and cost savings of e-invoicing
- variation in national rules which govern the validity and acceptability of e-invoices in legal, financial and administrative terms. This makes their use in cross-border transactions within the EU difficult
- many potential users have concerns about the security of e-invoicing systems and the potential for misrepresentation in fraud.\(^\text{84}\)

When there are significant and compelling cost savings to derive from a new technology or practice, it’s only a matter of time before adoption rates rise. Finally, with digitally optimized electronic invoicing, it seems that now is that time.\(^\text{85}\) A global study published earlier this year says that the volume of e-invoices and e-bills in 2014 will approach 40 billion worldwide, with annual growth rates of 20 per cent.\(^\text{86}\)

---

83 A common European framework for ICT Professionals in all industry sectors, http://www.ecompetences.eu/
Once the e-Invoicing Directive 2014/55/EU has been transposed into the national laws of EU Member States and the deadline for implementing the norm has passed, electronic invoices will be able to flow seamlessly across the EU\(^{87}\). Such activity plus other activities supported by governments at national level\(^{88}\) expect to result in a higher in a considerable increase in the market penetration in relation to the electronic share\(^{89}\) as is also depicted below.

This new collaborative space enables stakeholders interested in e-invoicing policy and market developments to exchange experiences and best practice on cross-border e-invoicing. It is open for use by the entire e-invoicing user community (all public administrations and private actors dealing with e-invoicing in Europe) to disseminate information, co-create the future and learn from one another.

### 5.8 GOOD PRACTICES IN E-INVOICING

**Standardisation**

The Commission-funded European Committee for Standardization (CEN) runs a number of activities on issues related to e-invoicing implementation. A series of informal meetings with representatives of standards organisations produced the report ‘e-Invoicing Standardisation Overview, issues and conclusions for future actions’\(^{90}\), in September 2012. Following the adoption of the E-invoicing Directive 2014/55/EU\(^{91}\) and in accordance with the provisions of Article 3\(^{92}\) within, the Commission issued a standardisation request for electronic invoicing to the European standardisation organisations in December 2014. The work is being carried out by the CEN Project Committee on Electronic Invoicing\(^{93}\) (CEN/PC 434).

---


\(^{88}\) Directive 2014/55/EU – Electronic invoicing in public procurement; PAs have to accept electronic invoices – Apply on all federal levels at the latest by November 2018 – Affects hundreds of thousands of Public Administrations and millions of Suppliers

\(^{89}\) see note 85


\(^{93}\) European Committee for Standardization, Electronic Invoicing,
EU funding for e-invoicing solutions
Under the Connecting Europe Facility\textsuperscript{94} (CEF), EU funding is available to support e-invoicing activities. Every year, call for grants are launched to select projects which can use EU money to set-up, upgrade and deploy e-invoicing solutions. For 2015, up to €7 million is being made available for EU applicants.

5.9 E-Identification (EID)
One of the reasons why smaller companies do not engage more in cross-border e-commerce is because the rules that apply to these transactions can be complex, unclear and may differ between Member States.

According to the EU repealing Directive 1999/93/EC, building trust in the online environment is key to economic and social development since according to the EU perceived matters, lack of trust because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services. In its conclusions of 4 February 2011 and of 23 October 2011, the European Council invited the Commission to create a digital single market by 2015, to make rapid progress in key areas of the digital economy and to promote a fully integrated digital single market by facilitating the cross-border use of online services, with particular attention to facilitating secure electronic identification and authentication.

This Regulation seeks to enhance trust in electronic transactions taking place in the internal market in order to establish a common foundation for secure electronic interaction between citizens, businesses and public authorities and as ultimate scope to increase the effectiveness of public and private online services, electronic business and electronic commerce in the EU. However, citizen and business trust depends on several aspects

- Given the current state and wording of the eIDAS Regulation, it may hinder the deployment of advanced privacy features. While transferring only the attributes necessary for the transaction does not solve the risk of profiling by authentication services, it would be a major step towards data protection and may trigger further considerations to stop processing unnecessary attribute values.
- For example, existing authentication methods in the ICT area, based on signed certificates containing the attributes of the user, aim at identifying entities with all attribute values contained in the certificate. Any usage of such an eID or certificate may expose a lot of the holder’s identity information.
- The next generation of eIDs could bring strong and efficient data protection to European citizens. In the electronic identification and trust services environment for electronic transactions, the realization of identification and authentication using an eID should prevent tracking of users. One of the possible technologies is thus Privacy-preserving Attribute-Based Credentials (Privacy-ABCs). In particular, the feature enabling users to only verify individual attributes instead of sending the complete set of identifying information is a leap forward for data protection. To actually be able to follow the technical development and to ensure technological neutrality, the architecture following inherently from the eIDAS Regulation should be open to alternative approaches.

Therefore, to ensure an appropriate interpretation, it is recommended that the meaning of security and privacy be emphasised, for instance by not only demanding the facilitation of

\textsuperscript{94} Connecting Europe Facility, https://ec.europa.eu/digital-single-market/connecting-europe-facility
privacy by design, but also fostering it through clarifications in the upcoming implementing acts. To preserve privacy in the long term, some clarifications of the legal text would be useful. All initiatives should go beyond the mere compliance with the legal framework on personal data protection and privacy by integrating those elements in the design phase.

5.10 GOOD PRACTICES IN EID FOR BUSINESSES

EU IDABC e-Identity and e-Security web:
IDABC stands for Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens. It takes advantage of the opportunities offered by information and communication technologies: -to encourage and support the delivery of cross-border public sector services to citizens and enterprises in Europe, -to improve efficiency and collaboration between European public administrations and, -to contribute to making Europe an attractive place to live, work and invest.

Applications for SMEs E-COMPASS
The SME E-COMPASS project designs and develops a “Real-Time Anti-Fraud Service for online European SMEs under a “Software-as-a-Service” framework. The platform is designed to work as the core engine of a merchant's fraud detection strategy and everyday work, demonstrating the following components95:

- Fully-functional web-based platform for order assessment, combining prior expert knowledge with automatic mechanisms for improving the cost-efficiency of the overall fraud detection process for SMEs;
- Reputation database exposing transactional attributes related to “Card Not Present (CNP)” fraud, aiming to increase connectivity, information sharing and collaboration efforts between a wide network of online SME merchants and antifraud professionals;
- Knowledge database of order scoring rules, empowered with a blend of supervised learning and intelligent models, for extracting patterns of fraudulent activity targeting online SMEs.

---

95 e-Compass, Applications for SMEs, http://www.sme-ecompass.eu/applications-for-smes.aspx
6 CONCLUSIONS

In terms of Societal Needs for open eGovernment, we recognize that, in contrast to current, traditional government practice, eGovernment takes the form of a dialog with societal actors. This creates a higher level of citizen engagement than a request for a 4 or 5 year mandate only. By using and open eGovernment tools, both the legislative and the executive branches of government have the potential for a much more fine-grained interaction with society. It is also becoming clear, with the advent of social media and digital literacy in general, that many citizens expect these changes, and will fairly naturally adopt them, as they currently do in other domains in their lives. However, for this to happen there is a need for user-friendly, accessible and trustworthy services.

In government, inclusiveness is paramount. Special care needs to be taken to include all of society, and not rush forward without equal participation for all members of society. There is still a 'digital divide' to contend with and remote rural areas, immigrants, the elderly and disabled people have specific needs that open eGovernment provision must be aware of.

The second challenge that needs to be addressed is the one of ethical and robust data management. Especially in the government’s core roles in care and control, data is generated and collected that is potentially privacy sensitive, or sensitive in terms of security. It is imperative that we understand that security and privacy do not form a zero-sum game; they are perfectly able to co-exist and actually need each other. These two aspects continue to be perceived as having conflicting needs even within the government domain, as the continued demands to weaken encryption for civic use demonstrate. In eGovernment security of data trumps all other considerations. Without an exemplary record in this respect, trust will never be built, and without trust there can be no eGovernment. The provenance of (big) data, and its potential for bias and exclusion is cause for concern in an eGovernment context, and could lead to policy and control decisions based on self-fulfilling assumptions.

Expertise is needed in the Public Sector and should not only be bought from industry, but also be sustainably embedded in-house, in order to provide for continuity, efficiency, transparency and a level playing field for when the market is needed. Public authorities are also in need of a dedicated budget for open eGovernment development and service delivery. Sustainability in open eGovernment, in a financial sense, needs to be addressed as well. Often benefits are enjoyed not where the immediate costs are made; benefits are global, costs are local. New procurement guidelines can help to make many of the government’s operational systems inherently eGovernment and open-data friendly, reducing or eliminating extra cost when services are actually built.

From the perspective of the Public Sector, in a strategic sense there seems to be a lack of vision regarding the changing nature of government. Open eGovernment tools and technology are seen as just that, tools that facilitate current practices and allow for budget cuts. Political leadership, policies and funding are required for the Public Sector to develop a vision, adopt an Open eGovernment and adapt to a changing society.

Where the EU perspective is extremely relevant is in the need for standardisation. In order to be able to move from the local perspective to the national, and European context, the language of eGovernment needs to be harmonised. Actual standardisation of operational government practices, in terms of data, ICT-supported technology and services, require a European effort.
Regarding Industry needs, the European Single Digital Market is the main driver of eGovernment needs. Overall, transparency and clarity with regard to procurement, regulation, invoicing and identification will greatly facilitate business and commerce across borders, and take this single market closer to reality. It also would assist the ICT industry in contributing to a greater degree to the development and uptake of open eGovernment services. As with the public sector, harmonization of legislation, standards and terminology is a prerequisite; as well as an accessible and comprehensive source of information on relevant available eGovernment services. As the market and industry increasingly digitize, like the rest of society, addressing the digital divide becomes a very important need also in this domain. The market does not work when there are regional or socially unreachable ‘blank spots’.

This deliverable has described the needs of three broad stakeholder groups with regard to the up-take and provision of open eGovernment services. This preliminary needs assessment will be further validated in a foresight focus group exercise, where current and future needs will be discussed within small groups of experts within open eGovernment. The CLARITY consortium will then present a briefing paper on considerations for the up-take of open eGovernment services in Europe, which will present a clear overview of current and future needs and drivers in this field.