Project acronym:	CLARITY
Project title:	Champion eGovernment appLications to increAse tRust, accountabIlity and TransparencY in public services
Grant number:	693881
Programme:	Horizon 2020
Objective:	INSO-1-2015 ICT-enabled open government
Contract type:	Co-ordination and Support Action
Start date of project:	01st March 2016
Duration:	24 months

Deliverable D3.5
Critical Review of European Policy

Author(s):	Socorro Bernardos and Óscar Corcho (Universidad Politécnica de Madrid); Tally Hatzalis (Trilateral Research), Ivonne Jansen-Dings (Waag Society), Vivian Kiousi (Intrasoft), Serdar Temiz (Open Knowledge Sweden), Hugo Hedlund (Municipality of Skelleftea),

Dissemination level:	Public
Deliverable type:	Final
Version:	1
Submission date:	31st August 2017

Table of Contents

EXECUTIVE SUMMARY

This is deliverable report *D3.5 Critical Review of European Policy,* of the European Commission Horizon 2020 funded project CLARITY (grant agreement number 693881). The CLARITY project aims to support European Member states in their pursuit for greater trust, transparency and efficiency within government via the increased take up of open eGovernment initiatives.

Deliverable report *D3.5 Critical Review of European Policy* presents a critical review of European policies in order to highlight the extent to which existing policies prohibit or support the supply of open eGovernment applications to meet the gaps identified in *D3.4 Gap analysis: Matching eGovernment applications to identified needs*.

Literature, including websites, on policies from the EU and different Member States, especially Belgium, Greece, Luxemburg, Netherlands, Spain, Sweden and UK, has been thoroughly reviewed.

Policies regarding eGovernment, open government, data protection and privacy, eIdentification, cybersecurity, ICT education, eAccessibility, eHealth and eProcurement are studied. Since all policies should be supported by their corresponding budget, a review of funding is also included.

The policy review suggests that they go in the right direction in order to meet all the identified generic gaps in open eGovernment services, as well as the gaps highlighted for the four sectors discussed in the CLARITY project (general practice health, local government services, disability and small business and self-employed). However, most policies may involve changes in the existing open eGovernment services and make the development of new ones more difficult, at least initially. This has direct implications for local governments and small business and self-employed as potential open-eGovernment-service providers.

More importantly, these policies need to be fully implemented and the transposition of directives and the introduction of provisions to regulations should be carefully watched so that those gaps actually disappear.

Although the reviewed policies are funded by different programmes and strategies, additional investment is also essential.

Table 1 relates policies and generic gaps in a matrix, so as to show which gaps are affected by each policy. If a policy supports the provision of eGovernment services to meet a gap, a '+' symbol is written in the corresponding cell. If the gap is not fully addressed, a short phrase noting the coverage is added. In the opposite case, a '-' symbol is used instead, while an 'x' symbol denotes that the policy does not hinder or support the gap. Specific particulars

concerning a country are denoted with the country's ISO Alpha-2 code[1]. A similar matrix for the four sectors studied in the CLARITY project (general practice health, local governments, disabled and small business and self-employed) can be found in Table 2.

General gaps / Policies	Citizen centred design of services	ICT skills and access	eDemocracy and civic participation	Language and accessibility	Openness and open data	Access to citizen data	Once-only principle
eGovernment strategies	+	+ access + skills (ES, GR)	+ x (UK)	+ x (UK)	+	+ x (UK)	+
Open government strategies	+	x	+	x	+	x	+
Data protection and privacy	+ trust - trust (ES)	x	+ trust - trust (ES)	x	+ process transparency	+	+ preconditi on
eIdentificatio n	x	x	+ preconditi on	x	x	+ preconditi on	+ preconditi on
Cybersecurity	+ trust	x	+ preconditi on	x	x	+ preconditi on	+ preconditi on
ITC Education	x	+ skills	+ preconditi on	x	x	x	x
eAccesibility	+ elderly, disabled	+ access	+ preconditi on	+ accessibilit y	x	x	x
eHealth	x	+ access	x	x	+ process transparen cy x (ES)	+ health data x (ES)	+ eHealth
eProcurement , eInvoicing	x	x	x	x	+ procurem ent transparen cy	+ company data	+ eProcurem ent, eTender and eInvoicing

Table 1: The impact of European policies on the generic gaps.

[1] ISO Country Codes - ISO 3166: https://www.iso.org/iso-3166-country-codes.html

Sector gaps / Policies	General practice health	Local government services	Disability	Small Businesses & Self-employed
eGovernment strategies	+	+	+	+
		- complexity of service (re-) development		- complexity of service (re-) development
Open government stategies	+	+	+	+
		- complexity of service (re-) development		- complexity of service (re-) development
Data protection and privacy	+ trust, personal and sensitive data	+ trust	+ trust, personal and sensitive data	+ trust, shared law
		- complexity of service (re-) development		- complexity of service (re-) development
eIdentification	+ precondition	+ precondition	+ precondition	+ precondition
		- complexity of service (re-) development		- complexity of service (re-) development
Cybersecurity	+ precondition	+ precondition	+ precondition	+ precondition
		- complexity of service (re-) development		- complexity of service (re-) development
ITC Education	+ ITC skills	+ ITC skills	+ ITC skills	+ ITC skills
eAccesibility	+ precondition	+ precondition	+ precondition	+ precondition
		- complexity of service (re-) development		- complexity of service (re-) development
eHealth	+	+ eHealth	+ eHealth	+ eHealth
		- complexity of service (re-) development		- complexity of service (re-) development
eProcurement and eInvoicing	+ Health eProcurement	+ eProcurement	+ Disability eprocurement	+ eProcurement
		- complexity of service (re-) development		- complexity of service (re-) development

Table 2: The impact of European policies on the gaps of general practice health, local governments, disabled and small business and self-employed.

The findings of this report, as well as the previous ones, will guide the preparation of the blueprint with the next steps in encouraging the provision and take-up of open eGovernment

services in Europe, especially within the four CLARITY focus areas (general practice health, local government services, disability and small business and self-employed).

This report is expected to be useful by most of the stakeholders identifed in deliverable D1.1. Those in charge of policy development at all levels (supra-national, national, regional, local) may use the findings from this report to identify areas that need further development, or to find examples of how policy development has been addressed in other countries or regions, to inform their own policy development. Stakeholder groups that are affected by those services (e.g., citizens with disabilities, enterpreneurs, etc.) have the opportunity to learn about the policies that affect them and find examples of good practices in policy development in other countries or regions, so as to inform their policy makers.

1 INTRODUCTION

Deliverable report *D3.5 Critical Review of European Policy* presents a critical review of European and Member State policies in order to understand the extent to which existing and imminent policies prohibit or support the supply of open eGovernment applications to meet the gaps identified in Task 3.4. The review covers policies ranging from eGovernment and open government strategies, to policies regarding data protection and privacy, eIdentification, cybersecurity, ICT education, eAccesibility, eHealth, eProcurement, eTender and eInvoicing. It analyses which of these policies hinder or promote the implementation of particular eGovernment applications, features or functionalities and thereby their influence on European Member States' pursuit for greater trust, transparency and efficiency within government via the increased take up of open eGovernment initiatives.

This deliverable draws primarily on *D3.4 Gap analysis: Matching eGovernment applications to identified needs*, which detected gaps between expressed needs and available services to guide policy evaluation. D3.4 derived gaps by matching drivers in the up-take of eGovernment applications in Europe (see D2.1); needs (see D2.2) and considerations for up-take of eGovernment services in Europe (D2.3), against the existing catalogue of eGovernment applications (see D3.1).[2]

The deliverable content is also based on a thorough literature review of policy documents in the EU and some Member States, especially those which are related to researches of the CLARITY Consortium, namely Belgium, Greece, Luxemburg, Netherlands, Spain, Sweden and UK.

The report is structured as follows:

- Section 2 summarises the gaps found in D3.4 so that the reader does not need to turn to D3.4 in order to understand the rest of the deliverable. First a list of generic gaps is provided and then gaps in the four focal domains of the project (general practice health, local government services, disability and small business and self-employed) are presented.
- Section 3 briefly describes the policies that affect the identified gaps and reviews their impact on those gaps. European policies being implemented or approved for implementation as of August 2017 will be studied first at EU level and then at national level. In order not to be repetitive, the section does not to go into much detail for the analysed Member States and focus in differences from the EU level policies instead.
- Section 4 draws conclusions on the support or hindering of the reviewed policies to meet the generic gaps and the four-sector ones.

[2] All CLARITY deliverables are available on the project website at: http://clarity-csa.eu/resources

2 GAPS BETWEEN NEEDS AND OPEN EGOVERMENT SERVICES IN THE EU

For quick reference, this section summarises the key gaps in open eGovernment services, focusing first on a list of generic gaps underlining all domains and then on the four focal domains of the project (general practice health, local government services, disability and small business and self-employed). It highlights the user needs remaining unfulfilled and establishes the topic areas against which the positive or negative influence of key policies will be evaluated. The extended analysis of the gaps was presented in *D3.4*.

2.1 GENERIC GAPS

Citizen-centred design of services (G1): Relevance and usability are key for eGovernment services uptake, yet many governments continue to prioritise, design and deliver services based on their own requirements or own understanding of user requirements, which holds back user adoption and use. The gap analysis in CLARITY deliverable D3.4 found that there is very scarce literature on the service needs of citizens when it comes to public services. Most literature focuses on very broad needs, such as the need for access, for a single contact point from European to national and to local levels, for trust and engagement. Information on citizens' actual needs that can drive functional requirements for designing public services, for example needs around the road closure information, waste disposal, social services as well as on the expectations of users regarding these services that can drive non-functional requirements, e.g. the need for real-time updates, mobile access interoperability is loosely coupled. Due to their prevalence across e-services some of those needs are so important that they are separately analysed –see G2 regarding access, G4, G6 and G7.

There is a real need to go back and review the foundations of public services and do a thorough needs assessments with citizens. There is also a strong need for adopting service design methodologies that take into account the user perspective or even involve the users in the actual design, such as agile development.

ICT skills and access (G2): Research has found that both public servants and citizens' lack of ICT skills hinder the up-take of open eGovernment services in Europe, though this finding contradicts citizens' reported levels of self-confidence in their skills to make use of digital technologies at work, for learning, and to use online public services[3]. With respect to access, the 2016 European Benchmark Report reveals that only 1/3 of public service websites are mobile friendly. As smart mobiles are fast becoming the main device through which people access the internet, it is imperative that more services are provided through mobile friendly websites or apps.

3 Attitudes towards the impact of digitisation and automation on daily life. http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2160

eDemocracy and civic participation (G3): Two-way communication, involvement in decision making and quality participation is fundamental for empowerment, for user adoption and for building trust towards involved parties; hence their lack creates and/or maintains a trust deficit towards the public sector. Yet, according to the CLARITY catalogue, only three Member States (Finland, Latvia and Slovenia) provide or plan to provide eDemocracy and eParticipation as a service on eGovernment portals; a finding also recognised by a recent report from the European Parliament.[4] As mentioned above, this is particularly important for service design as well as service improvement, particularly at local authority levels.

Language and accessibility (G4): Foreign language support is underdeveloped and underused overall and this requires attention as this results in hindering access to services to non-native speakers. Language support should translate website text but must also include translation of forms and present information on translation services in a more accessible way. As for accessibility for disabled citizens, this does need considerable attention from eGovernment providers as accessibility options are often few and difficult to locate on government service web-portals. Public services relating to health are particularly sensitive in this respect and should be a matter of priority.

Openness and open data (G5): As recounted in the CLARITY deliverables, there is a need for more openness in eGovernment on all levels. This openness would foster transparency of governmental processes, open data furthermore will fuel data driven innovation and development of new public services by citizens and businesses.

Access to citizen data (G6): Allowing citizens to "own", use and amend their data could go a long way to make them more invested in the services they use and more trusting of government. Allowing citizens to amend their data would also cut down on information queries by governments and allow for faster resolution times. Yet, only 55% of the EU Member States made this possible for citizens.[5]

Once-only principle (G7): Citizens still need to submit their data more than once in their dealings with public service providers. The lack of integration, legacy systems and a siloed approach to service delivery stand in the way of fully realising this principle. The EC eGovernment Benchmark Report 2016[6] suggests that currently only 49% of services are

4 European Parliament, REPORT on e-democracy in the European Union: potential and challenges (2016/2008(INI), Committee on Constitutional Affairs, 16 February 2017. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0041+0+DOC+PDF+V0//EN

5 European Commission, EGovernment Benchmark 2016: A turning point for eGovernment development in Europe? Final Insight Report – Volume 1, p. 5.[Online] https://ec.europa.eu/digital-single-market/en/news/eu-egovernment-report-2016-shows-online-public-services-improved-unevenly., p. 49

6 European Commission, EGovernment Benchmark 2016: A turning point for eGovernment development in Europe? Final Insight Report – Volume 1, .[Online] https://ec.europa.eu/digital-single-market/en/news/eu-egovernment-report-2016-shows-online-public-services-improved-unevenly

modelled on the once-only principle with business, rather than citizen, services fairing generally better in this respect.

2.2 GENERAL PRACTICE HEALTH (GH)

There are strong socio-economic drivers to the introduction of eHealth. Maintaining the European welfare standards in the face of an increasing aging population and citizens' demands for personalised e-services while ensuring service parity is a challenge. A combination of some kind of digital health service along with access to a real person if digital platform cannot address a request seems to be people's preference to date[7].

eHealth public services focus currently on reducing administrative burdens by enabling self-service. They target people's needs for convenience in terms of booking and managing of medical appointments, accessing own medical records, ordering repeat prescriptions and consulting with health staff online if necessary. Given their relevance, generic gaps on accessibility and foreign language are particularly important here to ensure equal access to health services.

Despite the existence of technological solutions, only few countries have currently invested in the necessary technical infrastructure to provide such services or in the retraining of medical staff and administrators to competently interface with it.

2.3 LOCAL GOVERNMENT SERVICES (GL)

Local authorities are at the forefront of service provision and implementation of central government policies and often the first and sometime the only point of contact for citizens. Citizens' needs with regards to municipal services range from those associated with life events (e.g., births, marriages/civil partnerships, divorce, buying property, setting up businesses etc.) to access to local services with respect to, for example, Education (Schools, Libraries), Emergency Services, Healthcare, Law Enforcement, Public Transit, Social Services, Waste Management.

Relevant, community-based, user-friendly, accessible and reliable services is what citizens require from their local authorities, along with open lines of communication by non-online means to ensure that less ICT literate or capable citizens (such as senior citizens and persons with disability) have an equal access to local services. Civic participation is particularly pertinent in this case of public service design and improvement. In the least, citizens seek means to make their voices heard, to raise issues, to provide feedback on matters of interest. Hence, online information, online consultation and feedback and fully automated, self-service e-procedures become the focal drivers of local government service provision. But also, citizens are generally willing to use the knowledge, ambition and skills they have in order to take

[7] Mobi Health News, "Survey: 75 percent of patients want digital health services", 14 July 2014. http://mobihealthnews.com/34804/survey-75-percent-of-patients-want-digital-health-services

responsibility of their own environment and create solutions that fit their own local or niche needs (e.g. regarding the liveability and safety) in their street, neighbourhood or town. Such self-organised citizen groups seek local authorities' support. These are yet to be realised in many countries due to budgetary constraints, lack of coherent long-term vision at a National level, competing priorities, resistance to change and lack of know-how amongst public servants in local authorities. In addition, a coherent picture pan-European is difficult to decipher as local authorities and municipalities in some countries have more autonomy and are relatively independent economically to decide their agenda on their projects and budget than others.

2.4 DISABILITY (GD)

With 44 million people aged between 15 and 64 being persons with disability, it is paramount for EU to cater for their human rights for their full participation in society, by enabling them to enjoy all the benefits of EU citizenship; removing administrative and attitudinal barriers to full and equal participation; and providing quality community-based services, including access to personal assistance." This is only to be exacerbated demographics of an aging population, as most senior citizens will also face some form of physical or mental impediment.

Access to public services that allow for greater independence in daily life, empowerment and participation is the ultimate goal for eGovernment applications. In addition, due to the great complexity arising from combinations of conditions encountered from person to person, the need for customizable applications and personalised service provision is an imperative for persons with disabilities, perhaps due to lack of digital skills more prominent in this group, lack of awareness and understanding of new and digitised services, long-term reliance on face-to-face contact and paper exchange, lack of trust in open eGovernment services and a sense of vulnerability with respect to the exposure of their personal data.

Human-centric public services, in general, and disability-related ones, in particular, lag behind. There is a lack of technological solutions that aim to boost inclusivity and civic participation of disabled people on foundational issues, such as work, training and education. eGovernment service provision is held back partly because streamlining existing service provision is required prior to its digitization, to overcome organizational and IT systems fragmentation, resistance to data sharing and change and gaps in ICT skills amongst social workers. This demands substantial budgets that often local authorities and municipalities -often responsible for such services- cannot afford.

2.5 SMALL BUSINESSES & SELF-EMPLOYED (GS)

With SMEs representing 90% of all businesses in the EU and being a key factor for economic growth, innovation, job creation and social advancing and championing eGovernment services for this group is of great importance. Unlike large corporations, most SMEs are consumers, rather than developers of digital services. As such, clear instructions, information, advice and even end-to-end e-processes on setting up and running a small business in terms of licencing, inspection, taxation etc.; solutions that minimise the administrative burden; responsive income

services to better deal with fluctuation in income, particularly for self-employed would be of great benefit.

In contrast, some technology SMEs have found a niche to provide or participate in the development of digital services. Such companies want a level playing field and in terms of access to information regarding procurement opportunities and tenders of the public sector. Hence progress towards eProcurement, eTender and eInvoicing solutions particularly with respect to public procurement would be a great leveller, yet there is still much to achieve.

3 TYPES OF POLICIES RELATED TO THE IDENTIFIED GAPS

There are a number of policies that can affect the identified gaps. Obviously, eGovernment strategies and open government plans play a crucial role in the provision of open eGovernment services, but there are other gap-related topics whose policies can support or hinder the meeting of those gaps. The following is the list of types of policies that this deliverable analyses:

- eGovernment strategies
- Open government strategies
- Policies regarding data protection and privacy
- Policies regarding eIdentification
- Policies regarding cybersecurity
- Policies regarding ICT education
- Policies regarding eAccesibility
- Policies regarding eHealth
- Policies regarding eProcurement and eInvoicing

Since all policies should be supported by their corresponding budget, a review of funding corresponding to the implementation of such policies is also included in this deliverable.

The types of policies that have been analysed are quite heterogeneous, including strategies, plans, initiatives, recommendations, directives, regulations, law proposals and laws, bills, decrees, and acts[8]. Except for directive[9] and regulation[10] in the context of the EU, this

[8] We have tried to keep the original term or the closest translation of that term.

[9] In Community law a directive is a legislative instrument that is binding on the Member States to whom it is addressed as regards the result to be attained but leaves them free to determine the form and methods. Directives may be adopted under the EC Treaty either by the European Parliament and the Council or by the Council or by the Commission. The Community institutions use Regulations more often than Directives in judicial cooperation in civil matters. Once adopted, Community Directives still have to be transposed by each of the Member States, that is to say they must be implemented by national law. http://ec.europa.eu/civiljustice/glossary/glossary_en.htm

[10] In Community law, a Regulation is an instrument of general scope that is binding in its entirety and directly applicable in all Member States. Regulations can be adopted under the EC Treaty by the European Parliament and the Council or by the Council or by the Commission. Regulations are often used in the field of judicial cooperation in civil matters. They are

terminology may be confusing, especially since some terms are ambiguous (e.g. sometimes strategy and plan seem interchangeable, other times plans seem to be part of a strategy) and there are nuances related to the different EU Member States' legislation systems. Defining and clarifying terms is not part of this deliverable's mission. However, it is important to note that strategies, plans, initiatives and recommendations that are not supported by a rule (directive, regulation, law, etc.) are not mandatory.

Many of the policies discussed in this report are part of wider digital strategies. Analysing the whole strategies is beyond the scope of this deliverable, but references are provided where appropriate. That is why the EU Digital Single Market strategy[11], which constitutes the first pillar of the European Digital Agenda for 2020[12], will be frequently mentioned.

3.1 eGOVERNMENT STRATEGIES

eGovernment strategies arguably have a direct implication in the provision of open eGovernment services that meet the gaps identified in CLARITY deliverable D3.4.

3.1.1 *European Union*

The EU eGovernment Action Plan 2016-2020[13] was launched on 19th April 2016 with the view to realise the following vision:

"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."

It sets out a number of principles that forthcoming initiatives should observe in order to deliver significant benefits that eGovernment can bring to businesses, citizens and public administrations themselves and correspond to all identified gaps listed above with the exception of G2 regarding ICT skills. These include:

directly applicable, so they require no transposal into the Member States' domestic law and directly confer rights or impose obligations. http://ec.europa.eu/civiljustice/glossary/glossary_en.htm

[11] https://ec.europa.eu/digital-single-market/en

[12] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. A Digital Agenda for Europe. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52010DC0245

13 European Commission, Communication: EU eGovernment Action Plan 2016-2020 - Accelerating the digital transformation of government, 19 April 2016: https://ec.europa.eu/digital-single-market/en/news/communication-eu-egovernment-action-plan-2016-2020-accelerating-digital-transformation
http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15268

- **Digital by default:** public administrations should deliver services digitally (including machine readable information) as the preferred option (while still keeping 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. (Directly related to G2 regarding access).
- **Once-only principle:** public administrations should ensure that citizens and businesses supply the same information only once to a public administration. Public administration offices take action if permitted to internally re-use this data, in due respect of data protection rules, so that no additional burden falls on citizens and businesses. (Directly related to G7)
- **Inclusiveness and accessibility:** public administrations should design digital public services that are inclusive by default and cater for different needs such as those of the elderly and people with disabilities (Directly related to G4, despite foreign language accessibility is not explicitly mentioned)
- **Openness & transparency:** public administrations should share information and data between themselves and enable citizens and businesses to access control and correct their own data (directly related to G6); enable users to monitor administrative processes that involve them; engage with and open up to stakeholders in the design and delivery of services (directly related to G1); and "transform its websites to support increasing engagement and participation of citizens and businesses in EU programmes and policy making" (directly related to G3).
- **Cross-border by default**: public administrations should make relevant digital public services available across borders and prevent further fragmentation to arise, thereby facilitating mobility within the Single Market. (Directly related to G7 in order to apply the once-only principle at European level)
- **Interoperability by default:** public services should be designed to work seamlessly across the Single Market and across organisational silos, relying on the free movement of data and digital services in the European Union. (Directly related to G7 in order to apply the once-only principle at European level) In this regard, the revised European Interoperability Framework[14] was adopted on 23 March 2017. The framework, which should be implemented by Member States, gives specific guidance on how to set up interoperable digital public services. It offers public administration a total of 47 concrete recommendations on how to improve governance of their interoperability activities, establish cross-organisational relationships, streamline processes supporting end-to-end digital services, and ensure that both existing and new legislation do not compromise interoperability efforts.
- **Trustworthiness & Security:** All initiatives should go beyond the mere compliance with the legal framework on personal data protection and privacy, and IT security, by

[14] ANNEX to the COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS European Interoperability Framework - Implementation Strategy: http://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_3&format=PDF

integrating those elements in the design phase. These are important pre-conditions for increasing trust in and take-up of digital services.

Under the principle of Inclusivenes and Accessibility, eGovernment services should cater for ICT illiterates. The Action Plan does not explicitly address the need for ICT skilling (directly related to G2), however this topic is extensively covered by other policies (See section on ICT Education below).

3.1.2 *Member States*

Member States pursue their own strategies and activities, but they should observe the seven principles above. The achievement of these seven principles by the Member States is monitored by the bi-annual eGovernment Benchmark Report.[15] Some examples are shown in the following paragraphs. Differences with the involved gaps will be noted where necessary.

In **Spain**, eGovernment is part of a wider transformation of the Public Administration which aims to a fully electronic, interconnected, transparent Public Administration with a clear and simple structure. Adopted on October 2, 2015, The Digital Transformation Plan for the General Administration and its Public Agencies[16] (ICT Strategy 2015-2020), sets the framework for the reform of the administration. It establishes the principles, objectives and actions, as well as important milestones. It is a clear tool for the implementation of the Law on the Common Administrative Procedure of Public Administration[17], which deals with the external relations of the administration with citizens and businesses, and the Law on the Legal Regime of the Public Sector[18], which deals with the organization and internal relations within each administration and among different administrations. It is closely related to acts, policies and services of the European Union siding with the digital agenda for Spain[19] and the current strategy of the European Commission Digital Single Market[20].

In contrast to the EU Action Plan, the ICT Strategy 2015-2020 takes into account the training of public servants (directly related to G2 regarding skills) and has explicitly adopted user-centric principles to include public servants as well as citizens in the design of services (directly related to G1).

---

[15] eGovernment in the European Union:
https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_EU_June_2017_v4_00.pdf
[16] http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/Estrategia_TIC/20151002-Plan-transformacion-digital-age-oopp.pdf
[17] Law 39/2015 of 1st October, on Common Administrative Procedure of Public Administrations
http://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10565
[18] Law 40/2015, of 1st October, on the Legal Regime of the Public Sector: https://www.boe.es/buscar/pdf/2015/BOE-A-2015-10566-consolidado.pdf
[19] http://www.agendadigital.gob.es/agenda-digital/Paginas/agenda-digital.aspx
[20] https://ec.europa.eu/digital-single-market/en

In **Sweden** as well, the Government Bill 2009/10:175 Public administration for democracy, participation and growth (2009), which was passed by the Parliament on 2nd July 2010, is not an eGovernment legislative document per se. However, it contains a long chapter specifically on eGovernment, while most initiatives concerning restructuring of public administration are related to electronic means. It describes, in fact, steps for working with eGovernment in the state administration.[21] Since then different agencies within Swedish government have proposed and launched several policies aimed towards different areas of the digitalization of public services, e.g. ICT in education.

Nor is there an overall eGovernment law in **Belgium**[22]. The digital government is one of the five priorities of the action plan Digital Belgium[23], introduced on 20th April 2015. Digital Belgium is continuing the efforts to implement a digital transformation of the federal government, aiming at digital-by-default end-to-end interactions with citizens and organizations. Non-federal Belgian administrative entities have developed their own eGovernment strategies within their respective areas of competence. Wallonia (including the French Community) and Flanders Regional Governments have created dedicated structures to implement their respective strategies.

Greece has the Strategy for eGovernment 2014–2020, which highlights the following principles: Interoperability; Comply or explain; Consolidation; No–duplication; Once only; Feasibility and viability; Transparency; Accessibility; Security and privacy; and Participation of citizens. There is an Action Plan including the actions needed for the implementation of this Strategy. Key milestones are the creation of the governance structure of eGovernment, the staffing plan for the computer and eGovernment services and of public sector bodies and units with a similar object and the completion of catalyst projects forming the backbone of eGovernment.[24]

In the **Netherlands,** the Digital Government 2017 Vision Paper[25], which was presented to the House of Representatives in May 2013, employs a digital by default approach, in which citizens will gain the right to interact with government in a digital way. The general principle for the interaction is 'digital where possible and in person where needed'. In addition to the vision paper, a joint implementation agenda has been agreed by the different government levels, describing the actions government organisations take in order to help realise their ambitions. Actions comprise digitalisation from a user point of view (user centricity), improvement of

[21] eGovernment in Sweden:
https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Sweden_March_2017_v2_00.pdf
[22] eGovernment in Belgium:
https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Belgium_March_2017_v3_00.pdf
[23] http://www.digitalbelgium.be/en
[24] eGovernment in Greece:
https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Greece_March_2017_v2_00.pdf
[25] http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2013/05/23/visiebrief-digitale-overheid-2017.html

accessibility and usability of digital services, connection to and use of the generic digital infrastructure.[26] However little to no progress has been made in the area of access to citizen data.

The **UK** published the Government Transformation Strategy[27] in February 2017. It seeks to make the government more understanding, flexible and responsive to the needs of citizens through a digital transformation in government services. It broadly follows the citizen-centred service design,[28] however it does not envision much in the way of participation and eDemocracy engagements with citizens.

A month later, the UK Digital Strategy 2017[29] was introduced. It sets eGovernment and digital transformation of the UK civil service among its priorities. The strategy also creates the Digital Government Partnership where policy responses and possible applications of digital technology innovations will be explored.

In **Luxembourg**, the digital agenda Digital Lëtzebuerg[30] covers eGovernment services but goes beyond that scope to establish a solid financial foundation for innovation, provide teaching and training of new competences and help create new markets (big data, smart grids, health IT, financial technology, virtual currencies…) for Luxembourg's IT sector. In order to maximise the impact of this strategy, it is applied horizontally and is to become a key component of every political decision.[31]

3.2 Open Government Strategies

Open Government is based on the principles of collaboration, transparency and participation; functioning within an open governance framework. It is also about making government processes and decisions open, in order to foster citizen participation and engagement. Obviously, open government strategies play a key role in supporting or hindering the provision of open eGovernment services to meet the gaps identified in CLARITY deliverable D3.4.

---

[26] eGovernment in the Netherlands. https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Netherlands_March_2017_v2_00(1).pdf

[27] Cabinet Office, Government Digital Service, Government Transformation Strategy (Policy Paper, 9 February 2017) online at: https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy.

[28] See Recommendation 2, OECD, Public Governance and Territorial Development Directorate, Recommendation of the Council on Digital Government Strategies (15 July 2014), online at: http://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf.

[29] Department for Digital, Culture Media & Sport, UK Digital Strategy 2017 (Policy Paper, 1 March 2017) online at: https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy.

[30] http://www.gouvernement.lu/4242265/digital-letzebuerg/4242280/intro

[31] eGovernment in Luxembourg. https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Luxembourg%20_March_2017_v1_00.pdf

3.2.1 European Union

The European Union does not have a separate open government plan, instead it is one of the key guiding principles of the EU eGovernment Action Plan reviewed above. This open government approach requires optimising process flows, opening up public sector data and services and moving from a silo mentality to a coordinated and collaborative approach. Breaking the silos between public administrations across borders will increase their efficiency and facilitate the cross-border mobility of businesses and citizens, which is crucial to meet G7. Breaking the silos with stakeholders and eventually opening public sector data and services to third parties, in full compliance with the legal framework for the protection of personal data and for privacy, will allow them to reuse these data and services. This will enable the design of personalised, pro-active and location-based services, thus facilitating digital interaction between administrations and users. This ensures user-centricity of public services and fosters collaborative service creation, features which are clearly aligned to G1. Furthermore, by opening up to stakeholders in decision-making, which would help to meet G3, public administrations will become more trustworthy and more accountable.

Indeed, the use of public sector information is very important for open government. Directive 2003/98/EC[32] on the re-use of public sector information set out a framework for the conditions of its reuse and aimed to ensure equal treatment for commercial editors within the internal market. It laid down a clear obligation for Member States to make all documents re-usable unless access is restricted or excluded under national rules on access to documents and subject to the other exceptions laid down in the Directive. The scope of Directive 2003/98/EC was extended to libraries, including university libraries, museums and archives by Directive 2013/37/EU[33]; and Member States were obliged to transpose it by 18 July 2015. However, some countries did it later (e.g., Belgium) and others have still to do it (e.g., Sweden).

In spring 2018, the Commission will prepare an initiative to improve the access and reuse of public and publicly funded data, for example, in the areas of public transport and public utilities.

3.2.2 Member States

Open Government is also part of many State Members' Digital Strategies. In addition, most EU Member States are participants in the Open Government Partnership (OGP)[34] and, as such, have delivered country action plans developed with public consultation and subject of an independent, qualitative and quantitative assessment of progress. To give some examples:

---

[32] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1502964192551&uri=CELEX:32003L0098

[33] DIRECTIVE 2013/37/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1502963778405&uri=CELEX:32013L0037

[34] https://www.opengovpartnership.org/

The **UK** was one of the founding governments of the OGP in 2011 and it is currently implementing its third Open Government National Action Plan (2016-2018), in which 13 commitments for a transparent, responsible, and privacy-aware egovernment are made aimed towards supporting democracy, citizen participation and countering corruption. Plans for the broadening of open data access and consulting with open data users were declared. Specific commitments are also made to create business opportunities for SMEs through open contracting, as well as to open elections data through collaborations with the Local Government Association. The Action Plan broadly implements the openness and transparency principles of the EU eGovernment Action Plan 2016-2020[35] and of the 2014 OECD Recommendations.[36] The Re-use of Public Sector Information Regulations[37], which came into force on 18 July2015, implements into UK law the European Directive 2013/37/EU.

Although not a founding government, **Sweden** joined the OGP in 2011. Sweden's third Open Government Action Plan (2016-2018)[38] builds on three of the commitments in the previous Action Plan and one additional commitment: Putting citizens at the centre (eGovernment); Re-using public administration documents and open data; Improving opportunities for dialogue and transparency in aid management and implementation; and Developing a new format for dialogue with Civil Society Organisations (CSOs) (new commitment). In addition, an agreement has been made with the Swedish Association of Local Authorities and Regions to strengthen collaboration around eGovernment and open government. On the first of July 2010, five years after the implementation deadline of Directive 2003/98/EC on the re-use of public sector information, the Directive's provisions were incorporated into Swedish law by Act (2010:566);[39] and many local and national initiatives aimed at stimulating re-use of public sector information are up and running.

Spain also joined the OGP in 2011 but has delayed a year the publishing of its third Open Government Plan (2017-2019)[40] due to the temporary situation of the government between December 2015 and November 2016. The Plan contains 20 commitments structured around 5 main themes: Collaboration, Participation, Transparency, Accountability and Training, all of them relevant for the purposes of this deliverable. In addition, Madrid is one of the 15 participants in the Subnational Pioneer Pilot Program of the OGP, what can help other regional

[35] European Commission, EU eGovernment Action Plan 2016-2020: Accelerating the digital transformation of government, COM(2016) 179 final (Communication, 19 April 2016), online at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0179&from=EN, p. 4.

[36] See Recommendation1, OECD, Public Governance and Territorial Development Directorate, Recommendation of the Council on Digital Government Strategies (15 July 2014), online at: http://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf.

[37] The Re-use of Public Sector Information Regulations 2015. http://www.legislation.gov.uk/uksi/2015/1415/contents/made

[38] https://www.opengovpartnership.org/documents/sweden-third-national-action-plan-2016-2018

[39] Temiz, S. and Brown, T. (2017a) 'Open data project for e-government: case study of Stockholm open data project', Int. J. Electronic Governance, Vol. 9, Nos. 1/2, pp.55–84

[40] http://transparencia.gob.es/transparencia/transparencia_Home/index/GobiernoParticipacion/Gobierno-abierto/IIIPlan.html?cookies=OK#

and local governments in their open government strategies. In July 2015, Law 18/2015[41] amended Law 37/2007[42], which implements EU Directive 2003/98/EC on the re-use of Public Sector Information, to incorporate Directive 2013/37/EU into the Spanish legal system. In addition, Royal Decree 1495/2011[43] developed Law 37/2007 for public administrations at national level.

Greece is also implementing its third Open Government Action Plan (2016-2018)[44], which consists of 34 commitments, some of them transferred form the second Action Plan (2014-2016)[45]. The Law for the public sector information reuse and open data was published in October 2014(Government Gazette 237/A/ 31 October 2014), and it includes the open-by-default principle.

Luxembourg presented a letter of adherence to OGP, but has no published an Action Plan yet. The new Open Data portal[46] of the Government went online on April 2016. The current Re-use of Public Sector Information Law of 23th May 2016 modified the law of 4th December 2007.

Belgium is an example of country that has not joined OGP but has an open government plan. In August 2015, a new federal open data strategy[47] was adopted by the Belgian Council of Ministers with a five-year long plan of actions aimed to strengthen the Belgian digital ecosystem and to evolve towards a leaner, more efficient and more modern government. The key part was to make open by default all government data except data with privacy or security information. There is a bill that supports this strategy and regulates the reuse of government information.[48] Law on the re-use of public sector information (2007), adopted at federal level, transposes into Belgian Law the EU Directive 2003/98/EC. It is worth adding that Regional and Community Governments had to equally transpose the Directive on the re-use of public sector information. Flanders, the Brussels-Capital Region and the French and German-speaking Communities also have their own decrees which are greatly inspired from the relevant federal legislation. In 2016, the existing Flemish decree on re-use of public sector information was adapted to be in line with the new European Directive.[49]

---

[41] Ley 18/2015, de 9 de julio, por la que se modifica la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. http://boe.es/boe/dias/2015/07/10/pdfs/BOE-A-2015-7731.pdf

[42] LEY 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. http://www.boe.es/boe/dias/2007/11/17/pdfs/A47160-47165.pdf

[43] Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal. http://boe.es/buscar/pdf/2011/BOE-A-2011-17560-consolidado.pdf

[44] https://www.opengovpartnership.org/documents/greece-national-action-plan-2016-2018

[45] https://www.opengovpartnership.org/documents/greece-second-action-plan-2014-2016

[46] http://data.public.lu.

[47] http://www.decroo.belgium.be/nl/groen-licht-voor-federale-open-data-strategie-overheidsdata-voortaan-vrij-beschikbaar

[48] Digital Belgium: http://digitalbelgium.be/wp-content/uploads/2017/07/compressed_Brochure_DB_FINAL.pdf

[49] eGovernment in Belgium: https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Belgium_March_2017_v3_00.pdf

In the **Netherlands**, a vision document created in 2013[50] lead to a broad consultation phase in 2015, where organisations on all levels of society where invited to participate. The Dutch Open Government platform (www.open-overheid.nl) was launched together with the official Action Plan 2016-2018[51]. The Action Plan translates the national priorities into nine concrete actions, among them the launch of a Dutch Open Data award (Stuiveling Open Data Award), setting the national agenda and opening city council information. The consultation for the next two-year period is currently being organised in the same fashion, giving all manner of interested organisations the opportunity to help determine the priorities[52]. On 24th June 2015 the Dutch re-useof public sector information act was published. The act ensures the transposition in Dutch law of the European Directive 2013/37/EU.

3.3 DATA PROTECTION AND PRIVACY

Governments collect and share data in order to e.g., personalize services, fulfil the once-only registration principle and ensuring interoperability of data within and across borders.

Considering how vital data is to the provision of open eGovernment services, it is clear that data protection and privacy regulations are crucial for the development of the field. 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.[53] Section 3.2 of *D2.2 Preliminary needs analysis for the up-take of eGovernment services in Europe* contains a thorough analysis of this issue.

The Charter of Fundamental Rights of the European Union[54] declares that:

"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."

This right needs further development. Thus, data protection and privacy of citizens have been the subject of wider legislation at both European and Member State levels.

---

[50] https://www.rijksoverheid.nl/documenten/rapporten/2013/09/01/visie-open-overheid

[51] https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/15/aanbiedingsbrief-bij-actieplan-open-overheid-2016-2017

[52] http://www.open-overheid.nl/open-overheid/lees-mee-en-reageer-evaluaties-actieplan-open-overheid/

[53] Oxford Internet Institute, "Breaking Barriers to eGovernment: Overcoming obstacles to improving European public services." Modinis Study, Contract no. 29172. 30 August 2007 (p 6) https://www.oii.ox.ac.uk/archive/downloads/research/egovbarriers/deliverables/1b/A_Legal_and_Institutional_Analysis_of_Barriers_to_eGovernment.pdf

[54] Official Journal of the European Union, Charter of Fundamental Rights of the European Union (2012/C 326/02) 26 October 2012. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN

3.3.1 *European Union*

The new legal framework established at the European level is the General Data Protection Regulation (GDPR) (2016/679)[55], which repeals current Directive 95/46/CE and will apply across the EU by the end of May 2018. In addition, the Directive 2016/680 for the police and criminal justice sector protects citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities. It will in particular ensure that the personal data of victims, witnesses, and suspects of crime are duly protected and will facilitate cross-border cooperation in the fight against crime and terrorism

According to the GDPR, when personal data are processed, people will have enforceable rights, such as[56]:

- The right to be informed that their personal data is being processed in a clear and understandable language;
- The right to have access to their own data;
- The right to rectify any wrong or incomplete information;
- The right, in some cases, to object to the processing on legitimate grounds;
- The right not to be subjected to an automated decision intended to evaluate certain personal aspects relating to them, such as their performance at work, creditworthiness, reliability, and conduct; and
- The right to receive compensation from the data controller for any damage they suffer, etc.

The obligations of a data controller (i.e. an entity either in the public or private sector which is responsible for processing personal data, for example, a medical practitioner, a company, a sports club, public administration, etc.) are the following[57]:

- To ensure that people's rights are observed (i.e. inform them, give access to their data);
- To ensure that data are collected only for specified, explicit and legitimate purposes, that they are kept accurate and up to date and for no longer than is necessary;
- To ensure that the criteria for making data-processing legitimate are observed, for example, when they give their consent, sign a contract, or have legal obligations, etc.;
- Confidentiality of the processing;
- Security of the processing;
- Notification to the data protection authority, in some cases; and

[55] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[56] Protection of personal data in the European Union eujls08b-1002_-_protection_of_personnal_data_a4_en

[57] Protection of personal data in the European Union eujls08b-1002_-_protection_of_personnal_data_a4_en

- To ensure that, when a transfer of data occurs to countries outside the EU, these countries guarantee an adequate level of protection.

The cost of falling foul of the rules can be high: up to €20 million or 4% of global annual turnover.

All these features might make open eGovernment applications more difficult to develop and maintain, and existing applications may need major changes to adapt to the GDPR, which will be a matter of concern for all open-eGovernment-service providers, including local governments. Nevertheless, their accomplishment will facilitate the meeting of all the gaps where trust is concerned. Besides, some features have a direct impact in specific gaps: G5 as the GDPR can help to process transparency and to create a balance between open data a private data; G6 since the access to own data is explicitly supported.

The GDPR will also "facilitate business by simplifying rules for companies in the Digital Single Market. A single law will also do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year."[58] Besides, a lack of trust in old data protection rules held back the digital economy and quite possibly businesses[59].

Although "the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States", the GDPR "also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data')."[60] The GDPR specifically lists health data, genetic data and biometric data as sensitive personal data and permits Member States to introduce further conditions around the processing of those data. (See eHealth).

While the GDPR already sets the rules for personal data, non-personal data is outside the scope of the current rules, meaning that restrictions on the free movement of such data can be imposed at national and regional level too. By autumn 2017, the Commission will prepare a legislative initiative on the cross-border free flow of non-personal data based on principles such as free movement of data, porting data and/or availability of certain data for regulatory control purposes.

The Commission will also continue work on liability and other emerging data issues, e.g. ownership of non-personal data

[58] http://ec.europa.eu/justice/data-protection/reform/index_en.htm
[59] http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_en.htm
[60] Clause 10 of GDPR

3.3.2 *Member States*

Obviously, open eGovernment services could be supported or hindered depending on the provisions and laws introduced by each Member State. The following paragraphs describe the situation in several European countries.

In **Spain**, the adaptation of its legislation to the GDPR requires the elaboration of a new law that substitutes the current one (LO 15/1999[61]). In June 2017, a draft of the new law, Ley Orgánica de Protección de Datos de Carácter Personal (LOPD)[62], was published. This draft consists of 78 articles organized in 8 chapters, 13 additional provisions, 5 transitory provisions, 1 derogation provision and 4 final provisions. As well as the general questions shared with the GDPR, there is an issue that can affect open eGoverment services: Article 77.2 rules that public administrations' sanction would be a reprimand, so some newspapers have reported that it will exonerate them from fines[63] . If this is approved, it will arguably contribute to the distrust of open eGovernment services controlled by public administrations, since they will not be 'punished' when not acting rightly.

In the **UK**, general data protection rules will be updated with a new Data Protection Bill[64], which will incorporate the principles of the GDPR into UK law, applicable even after Brexit. This Bill will offer personal data protection to citizens when interacting with government outside of the area of law enforcement. The Bill is also the main document which clarifies the right of individuals to access and amend their personal data.

In **Sweden**, the Personal Data Act[65], which came into force on 24th October 1998, was adopted to bring Swedish law into compliance with the requirements of the EU Data Protection Directive 95/46/EC. The Act lists certain fundamental requirements concerning the processing of personal data. These demands include, inter alia, that personal data may only be processed for specific, explicitly stated and justified purposes and if the person registered gives his/her consent. Exemptions to this rule include the exercise of official powers, or the fulfilment of a legal obligation by the controller of personal data. In many areas of the administration there are special registry laws to supplement or replace the provision in the Personal Data Act.[66]

---

[61] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal https://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf

[62] Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal www.mjusticia.gob.es/cs/Satellite/Portal/1292428451504

[63] http://www.eldiario.es/cv/Proteccion_de_datos-anteproyecto-ley_organica-justicia-politica_0_658634231.html

[64] Department for Digital, Culture, Media & Sport, A New Data Protection Bill: Our Planned Reforms (Statement of Intent, 7 August 2017) online at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635900/2017-08-07_DP_Bill_-_Statement_of_Intent.pdf

[65] http://www.datainspektionen.se/in-english/legislation/The-Personal-Data-Act/

[66] eGovernment in Sweden: https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Sweden_March_2017_v2_00.pdf

The **Dutch** Personal Data Protection Act[67] was adopted by the Dutch Parliament in July 2000 and came into force on 1st September 2001. It sets the rules for recording and using personal data, and ensured the transposition in Dutch law of the European Directive 95/46/EC.[68]

The Data Protection Act of 2 August 2002, which implements Directive 95/46/EC and which was amended by the law of 27 July 2007, governs the processing and use of personal data in **Luxembourg**. This act goes beyond the framework of the EU Directive by covering not only natural, but also moral persons. It contains specific provisions on the processing of medical data by health services, the processing of personal data for surveillance purposes and in the workplace; and applies to data controllers and data processors that process personal data on behalf of the controller.[69]

In **Belgium**, the Law on the protection of private life with regard to the processing of personal data of December 1992 was significantly modified in 1998 in order to transpose the EU Directive 95/46/EC. This law is now available in its 'consolidated version' dated August 2007.[70]

Greece adopted Law 3471/2006 on 28th June 2006, revising Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data was adopted, and intending to the enactment of preconditions with regard to the personal data processing and for the assurance of the confidentiality in telecommunications. Law 3471/2006 was amended by Law 3917/2011 and Law 4070/2012.[71]

3.4 eIDENTIFICATION

Many open eGovernment applications require the identification of the user to ensure the service is provided to the right person and in order to customise their interaction with the Public Administration. A secure electronic identification (eIdentification) can guarantee the unambiguous identification of a person and make it possible to access online services and to carry out electronic transactions in a safe way.

These aspects really matter in open eGovernment services, because citizens and businesses need to trust that only they and authorised people can access their data, something essential to

[67] http://wetten.overheid.nl/cgi-bin/deeplink/law1/title=Wet%20bescherming%20persoonsgegevens
[68] eGovernment in the Netherlands. https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Netherlands_March_2017_v2_00(1).pdf
[69] eGovernment in Luxembourg. https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Luxembourg%20_March_2017_v1_00.pdf
[70] eGovernment in Belgium: https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Belgium_March_2017_v3_00.pdf
[71] eGovernment in Greece: https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Greece_March_2017_v2_00.pdf

meet G6 and G7. Without eIdentification, users would only have access to a very limited number of open eGovernment services, they would not be able to access their data and they would have to submit their data every time they wanted to use a service. They would also need eIdentification for electronic voting and other forms of eDemocracy, what makes it crucial to meet G2.

3.4.1 *European Union*

The lack of common legal basis prevented Member States from recognising and accepting eIDs issued in other Member States. The eIDAS Regulation[72], approved in July 2014, provides a solution to these issues by ensuring the cross-border mutual recognition of eID means. As of 29 September 2018 the recognition of notified eID will become mandatory. This means that EU citizens will be able to use the eID means they use at national level also to access public services across borders in other Member States[73], enabling to meet G7 not only at national level, but also at European level.

3.4.2 *Member States*

Since the eIDAS Regulation does not impose a particular eId on all Member States, they have their own eIdentification rules and procedures. In April 2017, ClubPSCo produced a comparative chart of the different means carried out by the different Member States to adapt to the eIDAS Regulation[74]. According to this chart there were few Member States with laws and procedures already defined.

In summer 2016, the **Belgian** government passed the Digital Act, a law that enforces the equivalence between paper and digital formats. With the Digital Act, Belgium is among the first countries to implement the eIDAS[75] regulation. In addition, it has developed Itsme[76], the mobile version of a physical identification (which it complements). This mobile app allows every Belgian to unequivocally prove his identity online, hence replacing card readers and the many passwords on the Internet. Itsme can be used for example to make a payment in a webshop, to sign an online document or access governmental services online.

On 25 May 2016, the **Swedish** parliament voted on the supplementary law, which will support the implementation of the eIDAS Regulation. The law entered into force on 1 July 2016 and, as of 29 September 2018, the Swedish authorities using national eIdentification cards are

[72] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[73] https://ec.europa.eu/digital-single-market/node/50812

[74] http://clubpsco.fr/wp-content/uploads/2017/04/eIDAS-European-comparison-chart-2017-04-03.pdf/

[75] Digital Belgium. Status June 2017: http://digitalbelgium.be/wp-content/uploads/2017/07/compressed_Brochure_DB_FINAL.pdf

[76] https://brand.belgianmobileid.be/d/YShKZtiEUmGM/belgianmobileid-styleguide

expected to switch to the usage of specific European eIdentifications in the provision of their digital services.[77]

In **Spain**, articles 9 and 10 of the Law 39/2015 on the Common Administrative Procedure of Public Administration[78] establish the eIdentification and electronic signature systems for citizens to interact with the eGovernment services; and articles 42 and 43 of Law 40/2015 on the Legal Regime of the Public Sector regulates the use of digital signature methods by public administrations. Article 45 imposes requirements for the interoperability of electronic signatures not based on electronic certificates. Besides, electronic identity cards, DNIe[79], have been issued since 2006.

Greece has Law 4325/2015[80] (Government Gazette 47/A/11-05-2015), which extends the law 3979/2011 regarding "Electronic Identification" (Article 10) and "Electronic Exchange of Public Documents – Security of Information Systems of the Public Sector" (Article 13) while it amends the law 2690/1999 on the "Ex officio internal search of (electronic) certificates"(Article 12). Secure timestamping and receipt confirmation of electronic documents is regulated by the Ministerial Decision IDA/F.40.4/3/163 (Government Gazette 401/B/22-2-2013).[81]

The **UK** has developed the GOV.UK Verify service, which handles online identification of individuals through a decentralized and cooperative system of certified companies.[82] Although not a policy, this service is a necessity for the functioning of eGovernment and currently gives access to 12 government services. Commitment to further developing the scope of GOV.UK Verify is reaffirmed in the UK Digital Strategy 2017[83].

In December 2016 the eIDAS implementation act passed both Chambers of Parliament in the **Netherlands**. The legislation implements parts of the eIDAS regulation, by means of changes in existing Dutch laws, like telecommunications law, Civil Law and General Administrative Law.[84] The objective of the eIdentification policy is to modernise access to eGovernment services to achieve a higher level of trust in online identification. In the future, people will be

[77] eGovernment in Sweden: https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Sweden_March_2017_v2_00.pdf
[78] Law 39/2015 of 1st October, on Common Administrative Procedure of Public Administrations http://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10565
[79] http://firmaelectronica.gob.es/Home/Ciudadanos/DNI-Electronico.html
[80] (Government Gazette 47/A/11-05-2015) https://www.e-nomothesia.gr/kat-demosia-dioikese/n-4325-2015.html?q=43252015
[81] eGovernment in Greece: https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Greece_March_2017_v2_00.pdf
[82] Cabinet Office, Government Digital Service, GOV.UK Verify (Guidance, 17 February 2017) online at: https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify.
[83] Department for Digital, Culture Media & Sport, UK Digital Strategy 2017 (Policy Paper, 1 March 2017) online at: https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy.
[84] eGovernment in the Netherlands.

able to choose several ways to log in and identify themselves. The login solutions will be provided both by the government itself in various public domains (e.g., an extra layer of security on the current version of DigiD authentication service, a new eDriving licence and new identity card eNIK) and by private parties (banking solutions and market solutions under the trust agreement of Idensys).

There is currently a central eIdentity infrastructure in **Luxembourg** that provides an electronic ID card, LuxTrust S.A., a public/private partnership, created in 2003, to manage the development of a common Public Key Infrastructure (PKI) in order to secure eCommerce and eGovernment in Luxembourg. The consortium that was awarded the PKI contract was presented in July 2006.[85] A national eIdentification card is issued since 2014.[86]

3.5 CYBERSECURITY

As aforementioned, for open eGoverment services to take off, Europeans need trust and confidence. Cybersecurity is fundamental in order to gain them.

3.5.1 *European Union*

In 2013 The EU Commission and the High Representative jointly adopted the Cybersecurity Strategy for the European Union[87]. It outlines the EU's vision in this domain, clarifies roles and responsibilities and proposes specific activities at EU level. The following action is especially relevant to provide trust for open eGovernment services: "achieving cyber resilience, by increasing capabilities, preparedness, cooperation, information exchange and awareness in the field of Network and Information Security, for the public and private sectors and at national and EU level." Following this, the Directive on security of network and information systems (the NIS Directive)[88] was adopted by the European Parliament on 6th July 2016. The Directive entered into force in August 2016 and Member States have 21 months (May 2018) to transpose the Directive into their national laws and 6 months more to identify operators of essential services.

[85] eGovernment in Luxembourg. https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Luxembourg%20_March_2017_v1_00.pdf

[86] eIDAS: current state of play and the Luxembourgish approach. http://www.eu2015lu.eu/en/agenda/2015/12/01-02-conf-egovernment-ctie/presentations/day1/04_Lionel_Antunes_eIDAS.pptx

[87] http://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[88] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

The Digital Single Market Strategy[89] also recognises the importance of trust and security. In particular, tackling cybersecurity challenges together is one of the three emerging challenges identified in the mid-term review of May 2017[90]. The actions to be implemented are:

- By September 2017, the Commission will review the EU Cybersecurity Strategy and the mandate of the European Union Agency for Network and Information Security (ENISA)[91], to align it to the new EU-wide framework on cybersecurity.
- The Commission will also work to propose additional measures on cybersecurity standards, certification and labelling to make connected objects more cyber secure.

One of the Commision's objetives is to embed cybersecurity in the future EU policy initiatives from the start, in particular with regard to new technologies and emerging sectors such as connected cars, smart grids and the Internet of Things (loT)[92]. If this is followed, future policies related to open eGovernment services will support/favour citizen's trust and, therefore, will help to the uptake of such systems/applications.

3.5.2 *Member States*

In 2013, **Spain** approved a National Cybersecurity Strategy[93] which defined the structural items of cybersecurity. However these items are not configured yet. For instance, Spain still has to implement the NIS Directive into its legal system (although works regarding the transposition of the Directive are currently being carried out)[94]. As of now, cybersecurity of Public Administrations is ruled by Royal Decree 3/2010[95], which establishes the National Security Schema for electronic administration. In fact one of the action plans of the National Cybersecurity Strategy aims to guarantee the fully implementation of such National Security Schema.

In **Belgium**, the Law of 1st July 2011 on the security and protection of critical infrastructures established a national point of contact competent for the protection of critical infrastructure, the national analysis of threats targeting this critical infrastructure, as well as the obligation for each operator of a critical infrastructure to establish a security plan. The legislator will have

[89] https://ec.europa.eu/digital-single-market/en/digital-single-market
[90] https://ec.europa.eu/digital-single-market/en/news/digital-single-market-commission-calls-swift-adoption-key-proposals-and-maps-out-challenges
[91] https://www.enisa.europa.eu/
[92] https://ec.europa.eu/digital-single-market/en/policies/cybersecurity
[93] http://www.dsn.gob.es/en/file/932/download?token=9-T_SSTE
[94] INFORME ANUAL DE SEGURIDAD NACIONAL 2016, chapter 3 Cybersecurity: https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0ahUKEwi1yZP1l5rVAhUBVxQKHR2oB5AQFgg_MAQ&url=http%3A%2F%2Fwww.lamoncloa.gob.es%2Fserviciosdeprensa%2Fnotasprensa%2FDocuments%2F140217-Informe_Anual_de_Seguridad_Nacional_2016.pdf&usg=AFQjCNHt1eS6_Dks1GHrKWLPBh1kquMzaw
[95] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica: https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1330

the task of co-ordinating the NIS Directive with this law and other existing legislation.[96] In May 2017, it was decided to accelerate the efforts undertaken in the field of cyber security, with a comprehensive package of concrete measures under 6 priorities: 24/7 callcenter for SMEs & companies; sensitization campaigns; protection of critical public infrastructure; early warning system critical infrastructure; web tool for cybercrisis analysis and international cooperation.[97]

In **Luxembourg**, the Council of Government approved the creation of two new governmental entities during a session held on 15th July 2011: the Luxembourgish Cyber Security Board and the Governmental Computer Emergency Response Team[98] with the aim of strengthening its existing entities for fighting against cyber-attacks.

The **Swedish** Government presented a national strategy for developing and enhancing cybersecurity in June 2017. The strategy outlines objectives in six priority areas and will help to create the long-term conditions for all stakeholders in society to work effectively on cyber security, and raise the level of awareness and knowledge throughout society.[99]

In the **UK**, the importance of cybersecurity threats has been acknowledged and a separate National Cyber Security Strategy 2016-2021[100] has been set in place to tackle the issue. In the strategy, the role of government as a defender is accented upon with regard to online access to government services, and particular efforts are envisioned to strengthen government cybersecurity, including at the local level. In January 2017, the UK government confirmed that it will be implementing the EU's Network and Information Security Directive (NIS Directive) regardless of Brexit.

The **Netherlands** has a sophisticated and mature legal and policy framework for cyber security, which includes the National Cyber Security Strategy[101] and renews its cyber security framework every two years. The last Cybersecurity strategy of the Netherlands, National Cyber Security Strategy 2 - From Awareness to Capability extended alliances with public and private parties, both national and international, setting out responsibilities and concrete steps.

[96] http://www.linklaters.com/Insights/Publication1403Newsletter/June-2017/Pages/Belgium-The-NIS-Directive-turns-one-time-implementation.aspx
[97] Digital Belgium. Status June 2017: http://digitalbelgium.be/wp-content/uploads/2017/07/compressed_Brochure_DB_FINAL.pdf
[98] https://www.govcert.lu/en/
[99] http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf
[100] Her Majesty's Government, National Cyber Security Strategy 2016 to 2021 (1 November 2016), online at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
[101] https://www.ncsc.nl/english/current-topics/national-cyber-security-strategy.html

Greece has not developed a national cybersecurity strategy yet, however according to the European Union Agency for Network and Information Security, Greece is in the process of preparing a cybersecurity strategy.[102]

3.6 ICT EDUCATION

Education remains the responsibility of the EU's Member States. However, the European Commission is promoting various initiatives aimed at increasing training in digital skills for the workforce and for consumers; modernising education across the EU; harnessing digital technologies for learning and for the recognition and validation of skills; and anticipating and analysing skills needs. Clearly, this will affect the meeting of G2 regarding skills.

3.6.1 *European Union*

In 2006, the European Parliament and the Council of the European Union recommended[103] that "Member States develop the provision of key competences for all as part of their lifelong learning strategies, including their strategies for achieving universal literacy". They also proposed a Reference Framework which sets out the digital competence as one of the eight key competences which all individuals need for personal fulfilment and development, active citizenship, social inclusion and employment. For them learning and acquiring digital competences go beyond pure ICT skills and involve the safe, collaborative and creative use of ICT, including coding.

Moreover, the 2015 Joint Report of the Council and the Commission on the implementation of the strategic framework for European cooperation in education and training (ET 2020)[104] included as a priority 'relevant and high-quality learning', which "requires a more active use of innovative pedagogies and tools for developing digital competences: … Several Member States report initiatives to increase teachers' and learners' digital competences and one third have introduced national strategies for the digitalisation of education. Nevertheless, huge challenges remain. Societies are becoming increasingly digital, thus boosting demand for digital competences. Education and training must address this need, which requires investment in infrastructure, organisational change, digital devices and digital competences of teachers, trainers, school leaders and other members of educational staff, as well as the creation of digital (and open) educational resources and high-quality educational software"

On 10th June 2016 the European Commission published a new Skills Agenda for Europe[105], working together to strengthen human capital, employability and competitiveness. The new agenda sets out to improve the quality and relevance of skills formation, to make skills and

[102] https://www.cyberwiser.eu/greece-gr
[103] Recommendation of the European Parliament and the Council of the European Union, 2006/962/EC
[104] 2015 Joint Report of the Council and the Commission on the implementation of the strategic framework for European cooperation in education and training (ET 2020) New priorities for European cooperation in education and training (2015/C 417/04)
[105] http://ec.europa.eu/social/main.jsp?catId=1223&langId=en

qualifications more visible and comparable and advancing skills intelligence, documentation and informed career choices. The agenda includes two main initiatives regarding digital skills:

- The 'Upskilling pathways' initiative helps low-skilled adults to acquire a minimum level of literacy, numeracy and digital skills.
- The Digital Skills and Jobs Coalition[106] initiative mobilises companies, non-for profit organisations, educational providers, social partners and Member States in Europe who work together to tackle the lack of digital skills in Europe. The aim is to ensure that everyone acquires the digital skills they need to remain productive and employable and included.

3.6.2 *Member States*

On 10th May 2017 the European Commission published the annual Europe's Digital Progress Report (EDPR)[107], which monitors progress in digital policies in the Member States. The report concludes that "a number of Member States have adopted digital skills strategies and action plans aimed at enhancing digital literacy and skills or are in the process of doing so. Ireland, Latvia and the Netherlands are examples of 'early movers' in this respect. Hungary and Portugal are among those having launched dedicated strategies more recently. Most Member States have digital strategies for education", many of them included in broader digital strategies.

In addition, some Member States have incorporated Computer Science (CS) into their basic education curricula. A study conducted in October 2014 among 20 European Ministries of Education[108], found that computer programming and coding was already part of the curriculum in 12 countries: Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Greece, Ireland, Italy, Lithuania, Poland, Portugal and the UK (England). Seven more countries also planned to integrate this matter into their curricula in the future: Belgium Flanders, Spain, Finland, France, Luxembourg, Netherlands and Turkey. They differ in their administration level (national, regional, local), their education level (primary, secondary) and their compulsory nature.

In 2014 **England** was one of the first countries to mandate computer programming at primary and secondary schools[109]. Digital skills are supported also by the newly introduced Cyber Schools Programme**,**[110] aimed at the development of cybersecurity skills among schoolchildren

[106] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition
[107] https://ec.europa.eu/digital-single-market/en/news/european-digital-progress-report-review-member-states-progress-towards-digital-priorities
[108] http://www.eun.org/c/document_library/get_file?uuid=521cb928-6ec4-4a86-b522-9d8fd5cf60ce&groupId=43887
[109] https://www.gov.uk/government/publications/d5-london-summit-themes/d5-london-teaching-children-to-code
[110] Department for Digital, Culture, Media & Sport, Cyber Schools Programme (Guidance, 17 February 2017), online at: https://www.gov.uk/guidance/cyber-schools-programme.

by 2021 and through the Digital Skills Partnership,[111] a platform intended to facilitate the entry of people on the digital skills employment market.

In **Spain**, the current Education Law[112] has an order[113] that establishes the digital competence as one of the key competences that have to be taken into account during primary and secondary education, but here is no consensus among the different Regions in their adaptation of the law. Navarra and Madrid are relevant examples[114]: Navarra has included contents of computer programming in the area of mathematics in the fourth and fifth courses of primary education and Madrid has incorporated the subject 'Technology, Programming and Robotics' in the first three courses of secondary education.

Even though the **Netherlands** score high in ICT skills in relation to other EU countries, still one in five people have little to no experience[115]. Educating people in this field is currently addressed in regular education (on all levels). For those already out of the schooling system most cities offer classes and workshops in community centres or through commercial operators. However, as ICT skills are quickly become a prerequisite to move through our society, government needs to take a more active role in this field.

Luxembourg presented the Digital Strategy for Education[116] in May 2015. One of the projects initiated by this strategy are the free computing classes being introduced to young Luxembourgers through a launch of "Maker Spaces" at three secondary schools starting from the 2015/2016 school year. The Maker Spaces will be open to the schools which host them as well as other schools, after-school clubs, youth clubs, parents and associations.[117]

In 2016 the **Swedish** National Agency for Education submitted two proposals for national strategies for the digitization of primary and secondary schools to the Swedish government which have yet to be adopted[118]. The proposals argue for the provision of "adequate digital competence" and the use of digital tools and resources for improvement of results and streamlined operations.

---

[111] The Digital Skills Partnership is established by the UK Digital Strategy 2017. Department for Digital, Culture Media & Sport, UK Digital Strategy 2017 (Policy Paper, 1 March 2017) online at: https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy.

[112] LOMCE, Ley Orgánica 8/2013

[113] Orden ECD/65/2015

[114] José-Manuel Cabrera-Delgado (2017). "Computational Science in the Educational Curriculum". Revista de la Asociación de Inspectores de Educación de España. https://doi.org/10.23824/ase.v0i27.584

[115] https://www.cbs.nl/nl-nl/achtergrond/2016/30/ict-vaardigheden-van-nederlanders

[116] http://portal.education.lu/digital4education/

[117] eGovernment in Luxembourg. https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Luxembourg%20_March_2017_v1_00.pdf

[118] https://www.skolverket.se/skolutveckling/resurser-for-larande/itiskolan/nationell-strategi

3.7 EACCESIBILITY

Policies regarding electronic accessibility (eAccesibility) are key to meet G4, and thus, are very important to the Disability sector, one of the four sectors addressed by the CLARITY project. This issue is included in eGoverment plans (See eGovernment Strategies), but there are also specific laws worth considering.

3.7.1 *European Union*

DOTCOM: the Disability Online Tool of the Commission[119] has a thorough analysis about ICT and web accessibility in the EU and Member States. At the EU level:

Directive 1999/5 (R&TTE Directive)[120] addresses the conformity of radio and telecommunications terminal equipment with certain essential requirements, including the requirement that equipment is designed in such a way as to enable people with disabilities to use it without, or with minimal, adaptations. The Directive empowers the Commission to decide what types of apparatus should be designed in a way so as to support their use by persons with disabilities. This power has not yet been used by the Commission. The eCommunications package deals to some extent with the accessibility of electronic services. The package consists of six directives and one regulation, of which two have disability-specific provisions (Directive 2002/21[121] and Directive 2002/22[122]). In 2009, the package was updated. The 'Better Regulation' Directive[123] establishes a harmonised framework for the regulation of electronic communications services, electronic communications networks, associated facilities and associated services, and certain aspects of terminal equipment to facilitate access for disabled users. The Directive aims to ensure end-to-end connectivity and interoperability between equipment, networks and services for end-users with disabilities by including some aspects of terminal equipment in the material scope of the Directive. The 'Users' Rights' Directive[124] makes numerous references to the right to 'equivalent access' (including choice and affordability) of disabled end-users to services available to other end end-users. This functional equivalence implies the same usability of services by all users, even if the means to achieve this are different for disabled end-users. Equivalence of access should be guaranteed by national consumer protection requirements. The Directive encourages use of European standards to achieve e-accessibility of services (including through public procurement procedures). The Directive makes an important link between the provision of electronic

[119] http://www.disability-europe.net/dotcom
[120] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31999L0005
[121] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0050:EN:PDF
[122] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0022
[123] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF
[124] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF

communications services and the terminal equipment used to provide them (currently covered by the R&TTE Directive).

In October 2016 the Web Accessibility Directive[125], which regulates accessibility of public sector websites and mobile applications, was formally adopted. The Directive agreed text reportedly covers websites and mobile applications of public sector bodies with a limited number of exceptions (e.g. broadcasters, livestreaming), refers to the standards to make websites and mobile applications more accessible and requires regular monitoring and reporting of public sector websites and mobile apps by Member States. In December 2015, the Commission published a proposal for a Directive[126] on accessibility requirements for products and services (also known as the European Accessibility Act), which includes provisions addressing web accessibility relating to the private sector. The proposal is currently under discussion.

Member States have until 23rd September 2018 to transpose the Web Accessibility Act into their national legislation. Although the Directive does not apply to EU institutions' websites and mobile applications, those institutions are encouraged to comply with the Directive's accessibility requirements. The European Commission are committed to leading by example for Web accessibility and have announced they will adopt implementing acts by the end of 2018[127]. Since January 2010, all new EUROPA websites have been created in compliance with the World Wide Web Consortium standard WCAG 2.0, level AA. Additionally, the Information Providers Guide[128] details the accessibility requirements that everyone who develops and publishes material for EUROPA websites has to conform with.

3.7.2 *Member States*

Many national authorities in Europe are committed to the accessibility of public websites and most Member States have introduced guidelines or regulation based on WCAG 2.0[129], and consequently the level of accessibility of the government websites is much higher than that of private sites.[130]

[125] DIRECTIVE (EU) 2016/2102 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.327.01.0001.01.ENG&toc=OJ:L:2016:327:TOC
[126] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2015:0615:FIN
[127] https://ec.europa.eu/digital-single-market/en/web-accessibility
[128] http://ec.europa.eu/ipg/standards/accessibility/index_en.htm
[129] Web Content Accessibility Guidelines (WCAG) 2.0: https://www.w3.org/TR/WCAG20/
[130] https://ec.europa.eu/digital-single-market/en/web-accessibility

The following are some examples of the current situation in several Member States:

Articles 5 and 5a in the revised Constitution of **Greece** (2001)[131] state the equal right of all to information and participation in the Information Society. In particular, facilitating access to electronic means of information and communication, as well as to the production, exchange and dissemination of information electronically is an obligation of the state. eAccessibility standards in the provision of eGovernment services became compulsory by Ministerial Decision on 12 April 2012[132], whereby the websites of the public sector must comply with the WCAG 2.0, at least to the AA level.

In **Spain**, Law 56/2007[133] on measures to promote Information Society established an eAccessibility obligation: "As from 31 December 2008, the web pages of the Public Administrations will satisfy at least the average level of content accessibility criteria generally acknowledged. As an exception, this obligation will not apply when the technological solution supporting a functionality or service does not allow for such accessibility". Furthermore, Royal Decree 1494/2007[134] provides that "the information available on the web pages of the Public Administrations will have to be available to the elderly and people with disabilities with a minimal level of accessibility that fulfils the priorities 1 and 2 of the standard UNE 139803:2004." [135]

The Accessibility Observatory[136] is an initiative that aims to help improve the accessibility level of the portals of the Spanish Public Administrations at all levels (General State Administration, Regional Governments and Local Governments). The accessibility review of the Observatory is performed by an automated methodology[137] developed specifically for this observatory and based on the standard UNE 139803:2012[138], which replaced the standard UNE 139803:2004[139] in a Resolution in 2012[140] and is equivalent to WCAG 2.0.

---

[131] http://www.disabled.gr/lib/?p=7465
[132] http://www.nomotelia.gr/photos/File/yap-989-12.htm
[133] http://www.boe.es/buscar/doc.php?coleccion=iberlex&id=2007/22440
[134] http://sid.usal.es/idocs/F3/LYN11920/3-11920.pdf
[135] UNE 139803:2004 Aplicaciones informáticas para personas con discapacidad. Requisitos de accesibilidad para contenidos en la Web. http://www.tawdis.net/recursos/downloads/UNE_139803.pdf
[136] http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030180388
[137]https://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Accesibilidad/pae_Observatorio_de_Accesibilidad/15-07-09-Metodologia_Observatorio_Accesibilidad_Web-UNE2012-v1_0/Metodologia_Observatorio_Accesibilidad_Web-UNE2012-v1_0.pdf
[138] http://administracionelectronica.gob.es/PAe/accesibilidad/normativa
[139] Resolución de 3 de septiembre de 2012, de la Dirección General de Industria y de la Pequeña y Mediana Empresa, por la que se publica la relación de normas UNE anuladas durante el mes de julio de 2012. http://boe.es/boe/dias/2012/10/02/pdfs/BOE-A-2012-12325.pdf
[140] Resolución de 3 de septiembre de 2012, de la Dirección General de Industria y de la Pequeña y Mediana Empresa, por la que se publica la relación de normas UNE anuladas durante el mes de julio de 2012. http://boe.es/boe/dias/2012/10/02/pdfs/BOE-A-2012-12325.pdf

Accessibility has been continuously promoted in the **UK**, last by the 2017 Digital Skills and Inclusion Policy[141]. Internet access and digital skills across the population is supported by focusing on key aspects of inclusion and providing means to measure and support the process throughout and at different policy levels. The latest updated action plan[142] to support the improvement of public websites, IT equipment and online content to suit the needs of disabled people aims to contribute to an inclusive digital economy for people with specific needs. It covers regulation, accessible consumer technology and digital equipment, website services, accessible content, and awareness and promotion.

In November 2010, BSI (the UK National Standards Body) published a new national standard for web accessibility (BS 8878), whose code of practice applies to all products delivered via a web browser, including websites, web services and web-based applications such as email.

In August 2015, the **Swedish** government decided that the Swedish Post and Telecom Authority should be responsible for the national guidelines on web accessibility. The guidelines were developed by the eGovernment Delegation.[143] The Swedish Agency for Participation has produced an impact assessment[144] of the Web Accessibility Act that concludes the need for information efforts as well as support and guidance for different actors if the implementation is to be successful.

Within the **Netherlands** government websites are obligated to comply with accessibility standards as formulated on www.forumstandaardisatie.nl since 2008[145]. The legislation is formulated broadly as a 'apply or explain' principle. Even though this does not state clearly that accessibility is required, the Ministry of Interior has translated this into a set of rules that every government website and service has to comply with in order to receive a formal accessibility declaration[146]. The roadmap for more extensive legislation is clearly explained on the DigiToegankelijk.nl website[147].

Nor is there a law in Belgium which obliges companies and governments to adapt the accessibility of their websites to persons with a disability. There is however the law of May 10, 2007, which states lack of reasonable adaptations for persons with disability, is equivalent to discrimination. The different regional governments (the Flemish, the Walloon and the Brussels Metropolitan Region) want all websites to be labelled 'Anysurfer', which stands for a better

[141] Department for Digital, Culture, Media & Sport, Digital Skills and Inclusion Policy (Policy Paper, 5 April 2017) online at: https://www.gov.uk/government/publications/digital-inclusion-and-skills-policy/digital-skills-and-inclusion-policy.
[142] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/77984/e-Accessibility-Action-Plan_June2011.pdf
[143] eGovernment in Sweden: https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Sweden_March_2017_v2_00.pdf
[144] http://www.mfd.se/stod-och-verktyg/publikationer/rapporter/rapporter-2016/konsekvensutredning-om-tillganglighetsdirektivet/
[145] http://wetten.overheid.nl/BWBR0024717/2008-11-23#search_highlight1
[146] https://www.digitoegankelijk.nl
[147] https://www.digitoegankelijk.nl/beleid/wet-en-regelgeving

and more user-friendly websites. Since 2002 the Walloon government has been working on the National Action Plan to close up the digital gap.

In **Luxembourg**, the Accessibility Act (2001) does not mention the question of Web accessibility and there are no legal directives in communication technology laws. However, the 'e-Luxembourg' project launched by the Luxembourg Government concerns eAccessibility and the accessibility of official governmental or municipal websites. RENOW (Référentiel de normalisation web des sites gouvernementaux luxembourgeois – Guidelines on the creation of web sites for the Luxembourg Government) assists the Luxembourg Government in web design for all.

3.8 eHEALTH

Information and Communication Technology for health and wellbeing (eHealth) is becoming increasingly important to deliver top-quality care to European citizens. The eHealth Action Plan 2012-2020[148] of the European Commission aims at making use ICT to improve healthcare in Europe. One of the focus of the Action Plan is to develop common standards to enhance interoperable healthcare systems among Member States, which is critical to face G7 in eHeath in general, and general practice health in particular.

3.8.1 *European Union*

The European Commission has already put in place several activities to improve EU interoperability & standardisation in healthcare. During the period 2013-2020, the Commission will use the Connecting Europe Facility (CEF)[149] and the European Regional Development Fund (ERDF)[150] to push for a large-scale diffusion of innovative tools, the replicability of good practices and services for health, ageing and wellbeing, with a particular attention on improving equal access to services.[151]

eHealth is also a focus of the mid-term review of the Digital Single Market strategy. "The Commission wants to unlock EU added value for citizens, patients and researchers. It will work with interested Member States to ensure secure cross-border transfer of health records electronically and use e-prescriptions to dispense citizens' medication when people are travelling abroad. In addition, it will promote high-performance computing capacity to unlock the potential of big data for health through advanced data analytics such as in areas of development of medicines and early detection of emerging infectious diseases."[152]

[148] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=4188
[149] https://ec.europa.eu/digital-single-market/en/connecting-europe-facility
[150] http://ec.europa.eu/regional_policy/en/funding/erdf/
[151] https://ec.europa.eu/digital-single-market/en/interoperability-standardisation-connecting-ehealth-services
[152] http://europa.eu/rapid/press-release_MEMO-17-1233_en.htm

Together with the eHealth Action Plan 2012-2020, the Commission issued a Staff Working Document (SWD) on Telemedicine[153] to help deal with the legal aspects related to data protection rules, privacy matters and reimbursement.

Moreover, the European Commission has been facilitating an industry-led 'Code of Conduct on mobile health (mHealth) apps'[154], covering the topics of privacy and security. The objective of this code is to foster citizens' trust in mHealth apps, raise awareness of and facilitate compliance with EU data protection rules for app developers. It is at the moment of writing this report being looked at by the Article 29 Working Party on data protection[155]. Once approved by this independent EU advisory group, app developers will be able to voluntarily commit to follow its rules. This will support the addressing of G2, regarding mobile access.

It is worth noting that these three initiatives, the eHealth Action Plan the SWD on Telemedicine and the Code of Conduct on mHealth apps, are intended as guidelines, and are not binding on Member States.

Both the SWD on Telemedicine and the Code of Conduct can help in terms of trust for general practice health. Trust in eHealth services, such as pan-institutional patient summary records or ePrescription systems, becomes/is especially important as they process data which is among the most sensitive personal data. Thus, data protection is one of the key issues which will allow patients and healthcare providers to use eHealth services (See Data Protection and Privacy). Some countries have set specific rules, others rely on general health and data protection legislation.

3.8.2 *Member States*

In the **UK**, the storage and use of health and social care data is protected in a number of ways, in particular the Common Law Duty of Confidentiality and Data Protection Act (1998), to be replaced by new UK data protection legislation, which provide the legal framework for the processing of all personal data, other specific legislation such as the Control of Patient Information Regulations (2002), as well as non-legislative measures such as the Caldicott principles. In addition, to protect sensitive data, data security standards developed by the National Data Guardian for Health and Care will be implemented. The Government will introduce a national opt-out model to allow people to decide how their data is used. The Government has also said that transparency over how data is used is vital. By March 2020, people will be able to use online services to see more clearly how their data collected by National Health Service has been used for purposes other than individual care.[156]

[153] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1251
[154] http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=16125
[155] https://ec.europa.eu/digital-single-market/en/news/current-initiatives-unlock-potential-mobile-health-europe
[156] https://www.bhf.org.uk/news-from-the-bhf/news-archive/2017/july/government-response-to-the-national-data-guardian-review

In **Spain** there is no specific eHealth law as of August 2017. According to the ninth additional disposition of the new LOPD, the Spanish Government will deliver a draft of a new law about health, genetic and biometric data two years after the LOPD itself enters into force. Nevertheless, several eHealth services, such as electronic appointment and electronic prescription, are provided at regional level and efforts are being done to make those regional systems inter-operable.

Sweden has implemented several eHealth-related initiatives. In March 2016 the Swedish Government and the Swedish Association of Local Authorities and Regions (SKL) agreed on a vision for eHealth efforts to be achieved by 2025. The vision takes into account current projects being undertaking aiming to make better use of digitalisation opportunities in both health care and social service sectors. In August 2016, the Swedish Government commissioned the Swedish Agency for Innovation Systems (Vinnova) to undertake further efforts to take advantage of digitalisation opportunities for better health and health care from 2016 to 2017.[157]

The government has adopted goals to facilitate the use and development of eHealth services in the **Netherlands**. By 2019, 80% of the chronically ill population and 40% of other members of the population should have access to their own medical records. Also by 2019, 75% of the chronically ill and elderly population should be able to monitor certain aspects of their own health (such as blood pressure and cholesterol levels) and share this data with their health provider. Those who receive homecare should have access to 24-hour-a-day telecommunication with their healthcare provider, if they so choose[158].

The Dutch government has taken a number of steps to address these goals. National eHealth Week 2016 aimed to raise awareness of eHealth amongst practitioners and patients, highlight the country's experience with eHealth, and learn from eHealth adoption in other countries. The government has also developed zorgvoorinnoveren.nl, a website to support healthcare innovators who wish to make new digital applications, and is working with healthcare administrators and IT systems suppliers to develop standards for facilitating digital data sharing.

Like Sweden and the Netherlands **Belgium** also does not have specific eHealth legislation but has committed to create a common governance structure designed to ensure political and operational coordination of a twenty point action plan that should lead to an electronic patient file, giving patients and caregivers easy access to their personal health data[159].

[157] eGovernment in Sweden: https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Sweden_March_2017_v2_00.pdf

[158] https://www.government.nl/topics/ehealth/government-encouraging-use-of-ehealth

[159] http://www.plan-egezondheid.be

3.9 EPROCUREMENT AND EINVOICING

eProcurement refers to the use of ICT by public sector organisations when buying supplies and services or tendering public works. The provision of these services is very important to access that market for companies in general and Small Businesses and Self-Employed, one of the four sectors studied in the CLARITY project, in particular.

3.9.1 *European Union*

The EU has decided to undertake a thorough rethinking of the public procurement process with procurement digitalisation. This goes beyond simply moving to electronic tools; it rethinks various pre-award and post-award phases with the aim to make them simpler for businesses to participate in and for the public sector to manage. It also allows for the integration of data-based approaches at various stages of the procurement process.[160]

The timeline of the new rules and initiatives on eProcurement in the EU is the following:

- In 2013, the e-Procurement Golden Book of Good Practice[161] was produced by the Multi-Stakeholder Expert Group on eProcurement (EXEP), which 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.
- In February 2014, Directive 2014/23/EU[162] on the award of concession contracts, Directive 2014/24/EU[163] on public procurement and Directive 2014/25/EU[164] on procurement by entities operating in the water, energy, transport and postal services sectors were adopted by the European Parliament and the Council of the European Union.
- In April 2014, Directive 2014/55/EU[165] on electronic invoicing (eInvoicing) in public procurement was adopted by the European Parliament and the Council of the European Union.

[160] https://ec.europa.eu/growth/single-market/public-procurement/e-procurement_en
[161] e-Procurement Golden Book of Good Practice (*11 March 2013*)
https://ec.europa.eu/docsroom/documents/15443/attachments/1/translations/en/renditions/native
[162] DIRECTIVE 2014/23/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 February 2014 on the award of concession contracts: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2014_094_R_0001_01
[163] DIRECTIVE 2014/24/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 February 2014 on public procurement and repealing Directive 2004/18/EC: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2014_094_R_0065_01
[164] DIRECTIVE 2014/25/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32014L0025
[165] DIRECTIVE 2014/55/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014 on electronic invoicing in public procurement: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0055

- In January 2016 the standard form for the European Single Procurement Document[166] (ESPD) was established. It is a self-declaration form used in public procurement procedures by public buyers 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. With ESPD, companies are able to meet these obligations with a single form. The actual documents will only have to be provided by the winner of the tender
- By April 2016 (transposition date for the aforementioned Directives 2014/23/EU, 2014/24/EU and 2014/25/EU), tender opportunities and tender documents had to be electronically available. However, a series of Member States were late in implementing them and only did so weeks or months after the deadline. As of 16 February 2017, several Member States (Belgium, Estonia, Spain Lithuania, Luxembourg, Austria, Finland, Sweden) still need to implement and notify national measures implementing Directives 2014/24/EU and 2014/25/EU in full[167].
- By April 2017, central purchasing bodies had to move to full electronic means of communication including electronic bid submission.
- By October 2018 (two years after the expected transposition of Directives 2014/23/EU, 2014/24/EU and 2014/25/EU) electronic submission should be made mandatory for all contracting authorities and all procurement procedures.
- By November 2018 Directive 2014/55/EU will have to be transposed in Member States. Member States must ensure that all public sector contracting authorities are able to receive and process electronic invoices from suppliers which follow the new European standard for eInvoicing[168]. This European standard has been prepared by CEN Technical Committee 434 and its five parts have been published in May and June 2017.
- Moreover, some initiatives driving the transition to eProcurement are integrated into other broader Commission initiatives such as eGovernment and the reduction of administrative burdens.

[166] COMMISSION IMPLEMENTING REGULATION (EU) 2016/7 of 5 January 2016 establishing the standard form for the European Single Procurement Document: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0007

[167] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the review of the practical application of the European Single Procurement Document (ESPD) 17.5.2017. Table 1 in the Annex to the Report which provides for the date of entry into force of national legislation transposing Directives 2014/24/EU and 2014/25/EU for each Member State

[168] Electronic invoicing - Part 1: Semantic data model of the core elements of an electronic invoice, Electronic invoicing - Part 2: List of syntaxes that comply with EN 16931-1, Electronic invoicing - Part 3-1: Methodology for syntax bindings of the core elements of an electronic invoice, Electronic invoicing - Part 4: Guidelines on interoperability of electronic invoices at the transmission level, Electronic invoicing - Part 5: Guidelines on the use of sector or country extensions in conjunction with EN 16931-1, methodology to be applied in the real environment: https://standards.cen.eu/dyn/www/f?p=204:32:0::::FSP_ORG_ID,FSP_LANG_ID:1883209,25&cs=126F1BDBC8D6D6141F550EB578B4A9CF4

The use of electronic tools in public procurement can help to increase transparency, which is included in G5, and offers new business opportunities by improving the access of enterprises, including small and medium-sized ones to public procurement markets.

However, more detailed provisions to encourage interoperability and standardisation of eProcurement processes are needed[169], which is key in order to facilitate the meeting of G7. Besides, many potential users have concerns about the security of eInvoicing systems and the potential for misrepresentation in fraud.

3.9.2 *Member States*

Spain is one of the Member States that had not incorporated Directives 2014/23/EU, 2014/24/EU and 2014/25/EU to its legal body by April 2016. The existence of a temporary Government for a year caused the draft of the law to be delayed for discussion until November 2016. The new law, Proyecto de Ley de Contratos del Sector Público[170]**,** is currently (as of August 2017) under discussion; it was approved by the Congress on 27th July 2017, and it will be processed by the Senate from September 2017. As of August 2017 there is an online Public Sector Procurement Platform[171], implementing article 334 of the current law[172], where tenders and their awardings are published. Regarding eInvoicing, the current law[173] contains measures to promote its use and regulates the registration of invoices in the Public Sector. An online eInvoicing Platform[174], which allows the submission and consultation of eInvoces issued to the Public Administrations which have adhere to the system, supports this law.

Belgium has still to transpose Directives 2014/23/EU, 2014/24/EU and 2014/25/EU too. Its current legislation includes Law on public procurement and several public works contracts, public supply contracts and public service contracts (15th June 2006), which was modified on 12th January 2007 and published in the Belgian Monitor of 15th February 2007; Law on the acceptance of bids, information to candidates and tenderers, and time limits on public procurement and several public works contracts, public supply contracts and public service contracts (10th February 2010). These laws grant electronic means of procurement with the same legal value as that of traditional means. On the 12th of July 2013, the Flemish government

[169] https://ec.europa.eu/growth/single-market/public-procurement/e-procurement_en
[170] Proyecto de Ley de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo, 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014: http://www.congreso.es/portal/page/portal/Congreso/Congreso/Iniciativas?_piref73_2148295_73_1335437_1335437.next_page=/wc/servidorCGI&CMD=VERLST&BASE=IW12&PIECE=IWA2&FMT=INITXD1S.fmt&FORM1=INITXLBA.fmt&DOCS=6-6&QUERY=121.cini.+no+%40fcie+no+concluido.fase.
[171] https://contratacionde lestado.es/wps/portal
[172] Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público: https://www.boe.es/buscar/doc.php?id=BOE-A-2011-17887
[173] Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público: http://www.boe.es/boe/dias/2013/12/28/pdfs/BOE-A-2013-13722.pdf
[174] https://face.gob.es/

decided that by the 1st of January 2015 it had to be possible for private enterprises to send their invoices in an electronic form to all the Flemish government organisations. For the exchange of these e-invoices the Flemish administration started to use Mercurius in 2014, which is the e-invoicing platform provided by the Belgian federal government. [175]

In **Greece**, Law 4155/2013 for Public procurement (Government Gazette 120 A'/29.05.2013), as amended by Law 4281/2014 (Government Gazette 160 A'/08.08.2014), effectively codifies existing laws, Precedential decrees and Ministerial decisions regarding Public procurement considering the National System for eProcurement. In conjunction with the introduction of the eProcurement legislation, targeting the harmonisation with the relevant EU Directives, additional efforts have been undertaken by the Greek Government to revise the Greek public procurement legal framework, consisting of a complex set of laws, presidential decrees and regulations. To this end, the presidential decree 118/2007 simplifies the public procurement procedures, broadens participation to public sector competitions and introduces increased penalties in case of non-compliance to the specific competition terms and conditions. The new decree partially revises the existing legislation in this area while at the same time still maintains a major part of it.[176]

In the **UK**, the use of electronic means in the public procurement process is regulated by the Public Contracts Regulations 2015[177] (Statutory Instrument 2015 No.102) which came into force on 26 February 2015. It implements European Directive 2014/24/EU. The regulations apply to England, Wales and Northern Ireland. Corresponding legislation for Scotland is contained in the Public Contracts (Scotland) Regulations 2015[178] and in supplementary public procurement legislation available on the website of the Scottish Executive. Directive 2014/25/EU, is implemented by the Utilities Contracts Regulations 2016[179] for England, Wales and Northern Ireland and the Utilities Contracts (Scotland) Regulations 2016[180] (Scottish Statutory Instrument 2016 No. 2) for Scotland.[181]

As from 1 April 2013, the Procurement Act 2012 applies to all procurement conducted by (semi) public organisations in the **Netherlands**[182]. The act was updated in 2016, adding

[175] https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Belgium_March_2017_v3_00.pdf
[176] https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_Greece_March_2017_v2_00.pdf
[177] http://www.legislation.gov.uk/uksi/2015/102/contents/made
[178] http://www.legislation.gov.uk/ssi/2015/446/contents/made
[179] http://www.legislation.gov.uk/uksi/2016/274/contents/made
[180] http://www.legislation.gov.uk/ssi/2016/49/contents/made
[181] https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_United_Kingdom_March_2017_v3_00.pdf
[182] http://wetten.overheid.nl/BWBR0032203/2016-07-01#search_highlight0

guidelines for sustainability in procurement. And since 2017 all procurement above a certain threshold have to be digitally publiced on TenderNed[183].

In **Luxembourg**, the Public Procurement Act[184] of 25th June 2009 (which transposes the EU public procurement directives 2004/17/EC and 2004/18/EC), and the implementing regulation of 27th August 2013 allow for the use of electronic means in the public procurement process (electronic publication of calls for tender and electronic submission of offers).

3.10 BUDGET PROVISIONED FOR THE IMPLEMENTATION OF THE PREVIOUS POLICIES

For all the described policies and initiatives to achieve/bring the wanted outcomes, they have to be supported by sufficient funding.

3.10.1 *European Union*

The Joinup report on eGovernment in the European Union[185] analyses the relation of several funding sources and their relations to eGovernment and open Government. In this deliverable their relations to the identified gaps are added:

- Horizon 2020[186] is an EU Research and Innovation programme with nearly EUR 80 billion of funding available over seven years (2014 to 2020). It covers seven different domains of actions, called 'Societal Challenges', that reflect policy priorities of the Europe 2020 strategy and addresses major concerns shared by citizens in Europe and elsewhere. The Societal Challenge 6 'Europe in a changing world – Inclusive, innovative and reflective societies' deals with a series of societal issues and, among others, addresses directly problems related to eGovernment and modernisation of public administrations. The research and innovation actions in this area for 2014 and 2015 focused on demonstrating the open and collaborative government concept through the following topics:
  - Research into using emerging technologies in public sector (help to meet G4 and G7).
  - Pilots on open participation of the youth in decision-making processes (help to meet G3).
  - ICT-enabled open government; innovation actions for mobile, personalised public services and transparency of public administrations (help to meet G1, G2 and G5).

[183] https://www.rijksoverheid.nl/onderwerpen/aanbesteden/elektronisch-aanbesteden
[184] http://www.legilux.public.lu/leg/textescoordonnes/recueils/marches_publics_2015/
[185] eGovernment in the European Union:
https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment_in_EU_June_2017_v4_00.pdf
[186] https://ec.europa.eu/programmes/horizon2020/

- Design and creation of innovative applications by SMEs, in order to foster the delivery of mobile public services (eGovernment apps) for local and regional public authorities (help to meet G2, GL and GS).

The Work Programme 2016-2017[187] supports eGovernment related activities through the following topics:

- Applied co-creation to deliver public services (help to meet G1 and G3)
- Co-creation between public administrations: once-only principle (help to meet G1, G3 and G7).
- Policy-development in the age of big data: data-driven policy-making, policy-modelling and policy-implementation;
- Understanding the transformation of European public administrations (help to meet all the gaps and in all four sectors).
- New business models for inclusive, innovative and reflective societies (help to meet G4).

- The European Structural and Investment Funds[188] (ESIF) provide investments in the field of eGovernment in less favoured regions, as this is seen as a strategic component of their economic and social development. Each ESIF must support eleven thematic objectives (TO), including thematic objectives 2 and 11 which are particularly relevant to the modernisation of public administrations.
  - TO2 aims at enhancing access to, use and quality of ICT. The main specific characteristics describing TO2 are:
    - Extending broadband deployment and the roll-out of high-speed networks (help to meet G2 and G7).
    - Developing ICT products and services, eCommerce and enhancing demand for ICT.
    - Strengthening ICT applications for eGovernment, eLearning, eInclusion and eHealth (help to meet all the gaps, especially G4 and GH).
    - Enhancing the accessibility, use and quality of information and communication technologies, through the development of digital literacy, investment in eInclusion, eSkills and related entrepreneurial skill (help to meet G2, G4 and GS).
  - TO11 aims to enhance institutional capacity and to support the efficiency of public administrations. Two investment priorities are foreseen under TO11:
    - Investment in institutional capacity and in the efficiency of public administration and public services at the national, regional and local levels with a view to reforms, better regulation and good governance (help to meet all gaps, especially GL);

[187] Horizon 2020 Work Programme 2016 – 2017:
http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-societies_en.pdf
[188] https://ec.europa.eu/info/funding-tenders/european-structural-and-investment-funds_en

- Capacity building for all stakeholders delivering education, lifelong learning, training and employment and social policies, including through sectorial and territorial pacts to mobilise in order to reform at the national, regional and local levels (help to meet all gaps, especially G2, G4 and GL).

eHealth has additional funding sources via health-related programmes. For example, the European Commission has already put in place several activities to improve EU interoperability & standardisation in healthcare. During the period 2013-2020, the Commission will use the Connecting Europe Facility (CEF)[189] and the European Regional Development Fund (ERDF)[190] funding programmes to push for a large-scale diffusion of innovative tools, the replicability of good practices and services for health, ageing and wellbeing, with a particular attention on improving equal access to services.[191] Moreover, eHealth can help to support citizens' empowerment through self-management of health and disease, which is one of the focus of the first Societal Challenge of Horizon 2020, Health, Demographic Change and Wellbeing[192].

There are also a number of EU funded projects that address on Digital Inclusion[193]. The Commission's actions particularly addresses people with physical and cognitive disabilities, youth and the NEETs (Not in Employment, nor in Education or Training), the economically inactive, immigrants and the elderly. The Active and Assisted Living Programme[194] is a funding activity that aims to create better conditions of life for the older adults and to strengthen the international industrial opportunities in the area of ICT.

Cybersecurity has specific funding too. Since the launch of the Digital Single Market Strategy, the European Commission has stepped up its efforts to better protect Europeans online, including the adoption of different legislative proposals (See Cybersecurity), a significant investment in research and innovation and the development of networks[195]. In particular, Societal Challenge 7 of Horizon 2020, 'Secure societies – Protecting freedom and security of Europe and its citizens'[196], can support research, development and innovation in this field.

In spite of all these funding programmes and strategies, the mid-term review of the Digital Single Market strategy shows that substantial additional investment in digital skills and

[189] https://ec.europa.eu/digital-single-market/en/connecting-europe-facility
[190] http://ec.europa.eu/regional_policy/en/funding/erdf/
[191] https://ec.europa.eu/digital-single-market/en/interoperability-standardisation-connecting-ehealth-services
[192] http://ec.europa.eu/programmes/horizon2020/en/h2020-section/health-demographic-change-and-wellbeing
[193] https://ec.europa.eu/digital-single-market/en/news/eu-funded-projects-digital-inclusion
[194] http://www.aal-europe.eu/
[195] https://ec.europa.eu/digital-single-market/en/policies/strengthening-trust-and-security
[196] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens

infrastructure and technologies, combining resources from the EU, Member States and private sector is essential.[197]

3.10.2 *Member States*

The following are some examples of funding in some EU Member States:

In **Spain**, the last report on the advance of eGovernment[198] showed a large decrease of the investment in ICT in the State's Public Administration (over 65% from 2008 to 2013), which negatively affected the development and upgrade of public services. However, a comparison of the reports of the budget for ICT in the State's Public Administration[199] shows a steady increase since 2013. The Spanish Digital Agenda[200] has a budget for the different plans that make it up, being the Digital Public Service Plan[201], the Trust in the Digital Field Plan[202] and the Digital Inclusion and Employability Plan[203] the most relevant for open eGovernment services.

In **Sweden**, Vinnova[204] (the Swedish Innovation Agency) and IIS[205] (the Internet Foundation in Sweden) are key funders to open eGovernment services in addition to public authorities. Innovation Capacity in the Public Sector is one of Vinnova's strategic areas. Vinnova supports the development of an innovation-oriented public sector by stimulating and enabling investment in research and innovation activities. Vinnova had 7 open data calls for open data related projects. In addition, there are several examples of open-eGovernment-related projects funded by Vinnova, such as the information security and values for public e-services project[206]; Citizen E-Hub[207] project to have a wider platform for citizens to interact with public authorities; IMAIL[208] (Intelligent eGovernment services for eGovernment) to facilitate and increase accessibility for communication between citizens / companies and government agencies.

IIS is an independent public-service organization that acts to ensure positive development of the internet. IIS is responsible for the internet's Swedish top-level domain, .se, and the

---

[197] European Commission - Fact Sheet. Commission publishes mid-term review of the 2015 Digital Single Market strategy. Questions and Answers (May 2017): http://europa.eu/rapid/press-release_MEMO-17-1233_en.htm

[198] Informe sobre el grado de avance de la Administración Electrónica de junio de 2013: https://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/OBSAE/Informes/Informe_sobre_grado_avance_administracionelectronica_en_AGE_junio_2013.pdf

[199] Presupuestos de Tecnologías de la Información y las Comunicaciones de la Administración del Estado. https://administracionelectronica.gob.es/pae_Home/pae_OBSAE/pae_Informes/pae_PresupTICAdminEstado/pae_PrepDescarga.html#.WX9LTbZLe9I

[200] http://www.agendadigital.gob.es/Paginas/index.aspx

[201] http://www.agendadigital.gob.es/planes-actuaciones/Paginas/plan-servicios-publicos.aspx

[202] http://www.agendadigital.gob.es/planes-actuaciones/Paginas/plan-confianza-ambito-digital.aspx

[203] http://www.agendadigital.gob.es/planes-actuaciones/Paginas/plan-empleabilidad.aspx

[204] https://www.vinnova.se/

[205] https://www.iis.se

[206] https://www.vinnova.se/p/informationssakerhet-och-varden-for-offentliga-e-tjanster/

[207] http://www2.vinnova.se/sv/Resultat/Projekt/Effekta/2009-04551/Citizen-E-hub/

[208] https://www.vinnova.se/p/imail---intelligenta-e-tjanster-for-egovernment/

operation of the .nu top-level domain. In relation to open eGovernment services, ISS has 3 type of topics where ISS runs and funds several projects: the Digidelnätverket network, Digital participation and open data.

The **United Kingdom** pursues a multi-stranded funding strategy for developing eGovernment Technologies. On the one hand, £6.6bn are set aside to fund the SMEs that develop and provide eGovernment applications and services. Financially supporting the eGovernment app supplier ecosystem is a strategic goal as UK who seeks to gain global leadership on eGovernment service provision. Return on investment are expected to accrue on the one hand from cost cutting efficiencies in eGovernment services, taxation of domestic companies serving UK's needs for digital government services which is expected to reach £20bn by 2015 and export know-how and consultancy services to the rest of the world. Given the anticipated stable government income of successful SMEs and start-ups, this strategy has attracted $110.1m investment from venture capitalists in 2015 and $76.1 in the first quarter of 2016. It is worth noting that a percentage of local government and sector specific (e.g. Health, Transport) funds are also directed to ICT transformation initiatives not accounted for here.

Investments in ICT have grown continuously in the **Netherlands** from 2009 onward by both government and business[209]. Starting at 14%, in 2014, this had grown to 19% of the total investments[210]. The Netherlands Enterprise Agency oversees all funding sources available for governments, institutions, businesses, research facilities, schools and individuals over the whole spectrum of available topics. For ICT related activities the Dutch Government provides opportunities for all of these stakeholders. Different lines of credits are made available for SME's and businesses to innovate. There are funds to stimulate collaboration between different entrepreneurs working on the same domain within a region. And a process of vouchers are meant to stimulate research institutions to share knowledge and apply their research in a business context[211].

4 CONCLUSION

This deliverable presents a review of European and some Member State policies in order to understand the extent to which policies prohibit or support the supply of open eGovernment applications to meet the gaps identified in D3.4.

To that end, policies regarding eGovernment, open government, data protection and privacy, eIdentification, cybersecurity, ICT education, eAccessibility, eHealth and eProcurement have been studied.

[209] https://www.cbs.nl/-/media/_pdf/2016/26/ike2016_web.pdf
[210] https://www.cbs.nl/nl-nl/nieuws/2017/26/bovengemiddelde-groei-ict-sector
[211] https://www.rvo.nl/subsidies-regelingen?f%5B0%5D=sectoren%3A5845

The review of those policies let us conclude that they go in the right direction in order to meet all the identified gaps in open eGovernment services. In particular:

- G1, **citizen-centred design of services**, is key in all reviewed eGovernment Strategies. In addition, policies such as the eAcessibility ones address specific citizens. Moreover, other policies, such as the data protection and privacy and cybersecurity ones, affect marginally to meet this gaps by contributing to citizens' trust, either by increasing it (e.g., GDPR) or by decreasing it (certain interpretations of the new Spanish LPPD).
- G2, **ICT skills and access**, is taken into account by eGovernment Strategies regarding access. Additionally, eAccesibility and eHealth policies stress the importance of compliance not only for websites, but also for mobile apps. In regard to ICT skills, only some eGoverment Strategies plan for it (e.g., Spain), but all countries have wider Digital Agendas that do. Besides some Member States, as the UK, have included ICT-related subjects in their curricula.
- G3, **eDemocracy and civic participation**, is supported by both eGovernment and Open Goernment Strategies. Moreover, several policies, such as eIdentification, Cybersecurity and ITC education, help to set the foundations so that his gap can be met.
- G4, **language and accessibility**, is addressed by most eGovernment Strategies and eAccessibility-specific policies. This policies focus on the access for the elderly and people with disabilities. However, we could not find any language-specific plans or recommendations that could apply to eGovernment services with the exception of the Report on the EU eGovernment Action Plan 2016-2020[212], which "considers that, for the full functioning of cross-border eGovernment services, language barriers must be addressed, and that public administrations, especially in border regions, should make their information and services available in the languages of their Member States but also in other relevant European languages" and "calls on the Commission to accelerate its efforts in translating its websites into all the EU official languages". On the other hand, the European Commission is very keen to promote language learning across Europe so as to improve basic language skills and it is working with national governments to meet an ambitious goal: enabling citizens to communicate in two languages other than their mother tongue[213], so language will hopefully be less of an issue in the future for EU citizens.
- G5, **openness and open data**, is supported by both eGovernment and Open Goernment Strategies. Additionally, policies regarding Data Protection and Privacy, eHealth and eProcurement contribute to process transparency in their specific field.

[212] Report on the EU eGovernment Action Plan 2016-2020. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0178+0+DOC+XML+V0//EN

[213] http://ec.europa.eu/education/policy/multilingualism_en

- G6, **access to citizen data**, is addressed by most eGovernment Strategies (with the exception of Luxembourg and the UK) and by Data Protection and Privacy policies. In addition, eIdentification and Cybersecurity policies help to set the foundations to meet it. Moreover, eHealth policies deal with access to one's own health data; and eProcurement policies, to one's own company data.
- G7, **once-only principle**, is supported by both eGovernment and Open Goernment Strategies too, and is also helped by Data Protection, eIdentification and Cybersecurity policies. Additonally, eHealth and eProcurement policies favoure this principle within their respective fields.

The meeting of the general gaps will obviously affect the meeting of those gaps in the provision of open eGovernment services for the four sectors studied in the CLARITY project. Thus, all reviewed policies impact the four sectors to a greater or lesser extent. Next is a summarisation of the most important policies regarding each sector:

- **General practice health** is specifically supported by eHealth policies, which currently focus on reducing administrative burdens by enabling self-service. Given the sensitive nature of health data, Data Protection and Privacy policies are essential and, in addition to general laws, some countries (e.g. UK) have specific health-data protection laws. eAccessibility and ICT Education policies play a major role too in order to ensure equal access to health services. Staff training, which is also basic, is explicitly addressed by some eGovernment strategies (e.g., Spain, Greece).
- **Local government services** are greatly helped by eGovernment and open government strategies since they are often the implementation of central government policies. Due to local administrations being the closest to citizens, citizen-centred design and eParticipation initiatives are of especial relevance. In addition, given that lack of resources is frequently an issue, the reuse of open services is also very important for the provision of services at this administration level.
- **Disability** is clearly affected by eAccessibility policies. In spite that some Member States (e.g., the Netherlands) do not have specific eAccessibility laws, all the reviewed Member States and the EU are committed to website and mobile-app accessibility and include this in their eGovernment strategies. Another item in these strategies, which is especially important for this sector, is citizen-centred design, since customizable applications and personalised service provision is an imperative for people with disabilities. Perhaps due to lack of digital skills more prominent in this group, ICT Education policies are particularly relevant here.
- **Small businesses and self-employed** are evidently favoured by policies that promote the once-only principle, (cross-border) interoperability and shared law, since this allows them to devote their efforts to their mission and not to adapt their procedures to deal with different administrations. eProcurement policies are also important in terms of access to information and bidding regarding procurement opportunities and tenders of the public sector. Open approaches benefit this sector too by making public sector data and services available for reuse.

On the negative side, most policies may involve changes in the existing open eGovernment services as well as make the development of new ones more difficult, at least initially. This has direct implications for local governments and small business and self-employed as potential open-eGovernment-service providers.

However, the reviewed policies need to be fully implemented so that those gaps disappear. Moreover, some regulations and directives need still to be transposed into the Member States' legal systems, e.g. the GDPR and the NIS Directive. Depending on the particular implementations, the provision of open eGovernment applications to meet the identified gaps will be supported or not.

The financial issue is fundamental for implementations to be carried out. Although the reviewed policies are funded by different programmes and strategies, the mid-term review of the Digital Single Market strategy shows that substantial additional investment in digital skills and infrastructure and technologies, combining resources from the EU, Member States and private sector is essential.[214]

Finally, one has also to take into account that the meeting of the gaps can be hindered by technological issues, e.g., some functionalities and/or services use solutions that do not allow for accessibility.

Table 3 is a matrix of policies and generic gaps that can help to better understand which gaps are affected by each policy. If a policy supports the provision of eGovernment services to meet a gap, a '+' symbol is written in the corresponding cell. If the gap is not fully addressed, a short phrase noting the coverage is added. In the opposite case, a '-' symbol is used instead, while an 'x' symbol denotes the policy does not hinder or support the gap. Specific particulars concerning a country are denoted with the country's ISO Alpha-2 code[215].A similar matrix for the four sectors studied in the CLARITY project (general practice health, local governments, disabled and small business and self-employed) can be found in Table 4.

The next steps for CLARITY include the creation of the CLARITY blueprint, which takes all the research work of the CLARITY project and provides for the next steps for open eGovernment services in Europe to encouraged take-up of eGovernment applications within the four CLARITY focus areas. The findings of this deliverable, as well as previous deliverables will be further developed to provide guidance on: 1.) available and emerging solutions; 2.) emerging business models; 3.) technology and data gaps; 4.) emerging data models; 5.) policy gaps and 6.) social considerations. This information will broaden stakeholder understanding of what is required to enhance the provision and take-up of eGovernment services in Europe.

[214] European Commission - Fact Sheet. Commission publishes mid-term review of the 2015 Digital Single Market strategy. Questions and Answers (May 2017): http://europa.eu/rapid/press-release_MEMO-17-1233_en.htm
[215] ISO Country Codes - ISO 3166: https://www.iso.org/iso-3166-country-codes.html

General gaps / Policies	Citizen centred design of services	ICT skills and access	eDemocracy and civic participation	Language and accessibility	Openness and open data	Access to citizen data	Once-only principle
eGovernment strategies	+	+ access + skills (ES, GR)	+ x (UK)	+ x (UK)	+	+ x (UK)	+
Open government strategies	+	x	+	x	+	x	+
Data protection and privacy	+ trust - trust (ES)	x	+ trust - trust (ES)	x	+ process transparency	+	+ preconditi on
eIdentification	x	x	+ preconditi on	x	x	+ preconditi on	+ preconditi on
Cybersecurity	+ trust	x	+ preconditi on	x	x	+ preconditi on	+ preconditi on
ITC Education	x	+ skills	+ preconditi on	x	x	x	x
eAccesibility	+ elderly, disabled	+ access	+ preconditi on	+ accessibility	x	x	x
eHealth	x	+ access	x	x	+ process transparency x (ES)	+ health data x (ES)	+ eHealth
eProcurement, eInvoicing	x	x	x	x	+ procurement transparency	+ company data	+ eProcurement, eTender and eInvoicing

Table 3: The impact of European policies on the generic gaps.

Sector gaps / Policies	General practice health	Local government services	Disability	Small Businesses & Self-employed
eGovernment strategies	+	+	+	+
		- complexity of service (re-) development		- complexity of service (re-) development
Open government stategies	+	+	+	+
		- complexity of service (re-) development		- complexity of service (re-) development
Data protection and privacy	+ trust, personal and sensitive data	+ trust	+ trust, personal and sensitive data	+ trust, shared law
		- complexity of service (re-) development		- complexity of service (re-) development
eIdentification	+ precondition	+ precondition	+ precondition	+ precondition
		- complexity of service (re-) development		- complexity of service (re-) development
Cybersecurity	+ precondition	+ precondition	+ precondition	+ precondition
		- complexity of service (re-) development		- complexity of service (re-) development
ITC Education	+ ITC skills	+ ITC skills	+ ITC skills	+ ITC skills
eAccesibility	+ precondition	+ precondition	+ precondition	+ precondition
		- complexity of service (re-) development		- complexity of service (re-) development
eHealth	+	+ eHealth	+ eHealth	+ eHealth
		- complexity of service (re-) development		- complexity of service (re-) development
eProcurement and eInvoicing	+ Health eProcurement	+ eProcurement	+ Disability eprocurement	+ eProcurement
		- complexity of service (re-) development		- complexity of service (re-) development

Table 4: The impact of European policies on the gaps of general practice health, local governments, disabled and small business and self-employed.