CITADEL

Empowering Citizens to Transform European Public Administrations

Deliverable 2.2

Initial recommendations for transforming the public sector processes and services

Editor(s):	Steven Van de Walle Koen Migchelbrink
Responsible Partner:	KU Leuven
Status-Version:	Final – V1.0
Date:	30/09/2017
Distribution level (CO, PU):	PU

Project Number:	GA 726755
Project Title:	CITADEL

Title of Deliverable:	Initial recommendations for transforming the public sector processes and services
Due Date of Delivery to the EC:	30/09/18

Work package responsible for the Deliverable:	WP2 – Understand to Transform
Editor(s):	Steven.vandewalle@kuleuven.be Koen.migchelbrink@kuleuven.be
Contributor(s):	Marisa.escalante@tecnalia.com Inaki.etxaniz@tecnalia.com pieter.gryffroy@timelex.eu
Reviewer(s):	Gatis.Ozols@varam.gov.lv
Approved by:	All Partners
Recommended/mandatory readers:	Recommended to all partners

Abstract:	This document provides the initial recommendations and KPIs for transforming public administrations into more effective, efficient and citizens' centric organizations. Specifically, this document focusses on recommendations aimed at increasing public officials' willingness to participate with citizens (Voice and Exit), reduce citizens' non-use of electronic government services, PA compliance with GDPR, and the digital maturity assessment of public administrations. The recommendations are based on research presented in WP2 D2.1
Keyword List:	WP2, Initial recommendations, Initial KIPs, Public officials, Willingness to Engage, Non-use, E-government services, digital government, administration, GDPR, Compliance, interoperability, digital maturity.
Licensing information:	This work is licensed under Creative Commons Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0) http://creativecommons.org/licenses/by-sa/3.0/

Disclaimer	This document reflects only the author's views and neither Agency nor the Commission are responsible for any use that may be made of the information contained therein

Document Description

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
V0.1	29/06/2017	Initial Table of Contents	KUL
V0.2	29/08/2017	Initial information requirements based on user-exit and non-take-up study in t2.1	KUL
V0.3	17/08/2018	Major update recommendations and KPIs regarding public officials' willingness to engage and usage and prevention of non-take up.	KUL
V0.4	14/09/2018	The inclusion of recommendations and initial KPIs by TECNALIA and Time.lex	TECNALIA, Time.lex & KUL
V0.5	26/09/2018	Amendments according to internal CITADEL review	VARAM, KUL, TECNALIA & Time.lex
V1.0	26/09/2018	Document ready for submission	TECNALIA

Table of Contents

Terms and abbreviations

DPIA	Data protection Impact Assessment
DPO	Data protection officer
GDPR	General Data Protection Regulation
KPI	Key Performance Indicator
KUL	University of Leuven (Katholieke Universiteit Leuven)
PA	Public Administration
WP	Work Package

Executive Summary

This deliverable (D2.2) of the CITADEL project presents a summary of the main empirical findings from WP2 based on secondary data analysis, a survey with vignette study and a series of interviews with citizens. It provides initial recommendations for transforming public sector processes and services aimed at making them more citizen-oriented and more digital. Each conclusion and recommendation is followed by a number of KPIs to be used by public organizations to organise public engagement and inclusive digital services. This deliverable will be updated in one year´s time after inputs from the use cases have been taken on board. The final recommendations and KPIs will be presented in D2.3.

1 Introduction

1.1 About this deliverable

This is deliverable D2.2. of WP2 on 'understanding to transform'. It contains the initial requirements for information selection on how to transform public administrations. These requirements and recommendations are based on an analysis of secondary data, an empirical study on non-use of public services, a survey and vignette study among civil servants, and the digital maturity assessment model questionnaire. The recommendations are linked to an initial set of KPIs for public organisations looking at involving citizens in designing more user-centric pubic services. As an intermediate document, to be updated in D2.3, it pertains to defining the parameters and selecting relevant information. The parameters contain the generalized information requirements on which evaluations of specific topics can be made. The parameters and recommendations identified in this report serve as input for the WP4 ICT Enablers, particularly the KPI Report and DIGIMAT.

1.2 Document structure

The document is structured along four lines. One is focusing on the involvement maturity of public administrations: are they willing and able to incorporate citizen input into the design of services? The second line focuses on the drivers of non-use and non-take up of public services by citizens, and how this non-take up can be remedied. The third line focuses on GDPR compliance by PAs. The fourth and final part focuses on the digital maturity of PAs. In conclusion we provide a summarizing list of all initial KPIs formulated in this document.

2 Initial conclusions, recommendations and information requirements for improving public officials´ willingness to engage citizens

In order to take citizens´ exit and voice signals into account, public officials and their organizations have to be willing to engage with this input. The recommendations formulated below are based on three sources of data. One is a screening of existing data sources on the extent to which public officials are willing to engage with citizens and use their input. The second is a survey among public officials in the use cases of the CITADEL project (VARAM, City of Antwerp, and Puglia Region). The third is a vignette experiment among public officials in the City of Antwerp. Detailed findings have been reported in D2.1 [1] and its appendices. D2.2 formulates broad recommendations based on these data and proposes a number of KPIs for public organizations who want to monitor their organizations´ or officials' willingness to engage with citizens.

2.1 Citizen support for expert decision making remains high

The analysis of secondary data revealed that many citizens have low confidence to take part in politics, and that they also evaluate a system in which experts make decisions relatively positively. Yet, there are important differences across countries in the extent to which citizens value expert decision-making. In particular, respondents from Denmark, Sweden and Switzerland are more hesitant about a political system based on expert decision making than respondents from Hungary, Slovenia, and Poland. The two factors appear to go together. At the same time, our own surveys found that public officials have strong democratic attitudes.

Initial KPIs

- Number of citizens having sufficient confidence to take part in public decision-making
- Public support for expert decision-making
- Extent of support for democratic values among public officials

2.2 Input legitimacy of a participatory process is important

The vignette study showed that there is a strong and positive relation between the input legitimacy (e.g.: turnout and participants' representativeness) of a participatory process and the willingness of public officials to engage with citizens. This is especially the case when the citizens who participate are representative. It means that for public officials to listen to citizen, not just any input will be used in decision-making, but mainly input coming from representative groups of citizens, and input provided by a large group of citizens. Input coming from small and non-representative groups is more likely to be disregarded.

In a time when it has become easier for citizen to express their voice and to use exit to express dissatisfaction; public officials still value traditional inputs through processes resembling traditional democratic processes highly.

Initial KPIs

- Socio-demographic composition of citizens providing input resembles that of the wider population
- Number of citizens participating in service delivery and design

2.3 Citizen engagement: slower but better?

Our survey found that public officials are positive about public participation, even though they think it slows down the decision-making process. In particular, public officials think that citizen participation improves the decision-making process by bringing in new ideas. Other traditional concerns about involving citizens did not emerge from the survey. Unlike what is suggested by the literature, officials do not express strong concerns about a potential reduction of their own influence on decisions, and they do not disregard the value of participation altogether.

Initial KPIs

- Number of public officials thinking that participation slows down decision making
- Number of public officials thinking participation improves decision making

2.4 Public officials have concerns about citizens´ competence and motives to get involved in decisions.

The literature on public participation tends to assume that many citizens do not have the necessary skills and knowledge to participate, and that therefore their input will not be very relevant. At the same time, it is also thought that citizens mainly participate in order to further their own personal interests. It is important to check whether public officials also hold these views. If this is the case, it can be expected that public officials will be less willing to engage with citizens. The survey found that respondents are pessimistic about the competences of citizens to participate in administrative decision-making. They also think that citizens do not participate to pursue the interests of the entire community, but rather to further their own interests.

Initial KPIs

- Proportion of public officials thinking citizens have sufficient skills and knowledge to contribute to decision making
- Proportion of public officials thinking citizens participate to pursue the interests of the entire community

2.5 Perceived administrative burdens

Thus far, research has shown that bureaucratic and administrative burdens like red tape are a major barrier to effective citizen participation [2], [3]. A detailed look at public officials' perceptions of red tape in their core activities, in the form of perceived rule functionality and perceived compliance burdens, further specifies the willingness of public officials to participate with citizens. Our survey indicated that respondents are generally positive about the lack of red tape in their organizations (more information in D2.1), indicating organizational readiness to start public engagement

- Public officials' perceptions of the compliance cost of the rules with which they have to comply in their core activities.
- Public officials' perceptions of the rule functionality of the rules with which they have to comply in their core activities.

2.6 Vignette experiments are a good yet resource-intensive way of capturing public officials´ views

To obtain information about public officials´ willingness to engage with citizens we used a survey experiment with vignettes. The advantage of this approach is that it allows us to manipulate the content of the vignettes and in this way, obtain information from the public officials that are less subject to acquiescence and social desirability bias. At the same time, however, during the process we have noticed that the method requires a high number of respondents, especially when the researcher want to manipulate several variables; for this reason, the current study could only look at the effects of input legitimacy. In order to obtain sufficient power for the experiment, we have had to survey the entire population of public officials in A and B grades in the city of Antwerp. More economic ways of collecting data need to be considered for follow-up research.

3 Initial conclusions, recommendations and information requirements for improving usage and preventing non-take up of digital services

Based on a screening of existing open data sources, an initial literature review, and field work among non-users of electronic services (see details in D2.1 [1]), a number of general conclusion and recommendations can be formulated. The analysis of non-adoption motives generally confirms the findings from the existing literature. It did highlight a number of specific findings though. More in particular, it drew attention to a difficult dilemma for public organizations wanting to stimulate digitization: should abundant offline alternatives be offered to guarantee broad access, or does this unduly hamper take-up of digital services? We discuss the findings in relation to the Technology Acceptance Model and earlier literature on the motives for adopting new (government) technologies.

3.1 Hardware and Internet access remain an issue

The study revealed that not having a computer or Internet access remains an important reason for not using online services. This is a finding that has emerged repeatedly in research on non-use of digital services, even in highly developed countries were internet penetration rates are very high (see, e.g. van Deursen et al., [4]); This is especially the case for older people. Several of the centers where interviews were conducted are located in remote areas. In these areas, broadband connections are mostly not yet available and existing connections and Internet accessibility is not as good as in the cities. Also, people living in these areas have lower income levels and many households cannot afford computers and Internet access at home.

For Europe as a whole, we know the overall Internet access rate is high (see detailed findings in D2.1 [1]). However, there remain important differences across Europe, with very high access in some countries (e.g., the Netherlands), but considerably lower access in e.g. the Czech Republic, Lithuania and Portugal, indicating unequal Internet access across Europe.

An eye-opening finding was that several respondents mentioned the lack of scanning equipment as a reason to visit the offline Citizen Service Centers. One could argue that this is not an issue related to technology access, but rather one related to poor service design where paper-based documents remain necessary in an e-government context.

Access to the electronic services requiring authorization on *latvija.lv* remains an issue for many people who do not use and/or do not know how to use Internet banking, have no e-signature and/or eID card. This shows that the issue of digital government services and non-take up of electronic services is related to the wider e-environment and infrastructure, including electronic banking or online shopping.

Initial KPIs:

- Online shopping penetration rate
- Number of households without a single smartphone, tablet or scanning device
- Number of citizens actively using online banking facilities
- Number of inhabitants/service beneficiaries without electronic ID card or government portal login credentials
- Number of households without internet connection
- Extent of broadband coverage in rural areas

3.2 Discrepancies in ICT skills among citizens need to be addressed

D2.1 [1] showed that digital skills of citizens, defined as their ability to use the Internet and have at least a basic level of digital skill, differ widely. There remain important differences within and across countries. Statistics show that citizens from North-western European countries appear better equipped to tackle the challenges of digital transformations than respondents from South-Eastern European countries. This has implications for the likely take-up of new digital government services in the latter group of countries.

Initial KPIs:

- Number of citizens without basic digital skills
- Number of citizens without basic digital skills, broken down by SES group
- Number of citizens without basic digital skills, broken down by level of urbanization of residence
- Citizens' self-reported satisfaction with ICT skills
- Number of clients/citizens aged 65+

3.3 Public officials´ digital skills need to be upgraded

Not all public employees are ready to make the switch to digital. Our analysis reported in D2.1 [1], based on the European Working Condition Surveys(EWCS), showed that persons working in the public sector are positive about their skills in relation to their job requirements, but their skills satisfaction is lower than that for respondents not working in the public sector. Public officials also more often than workers in other sectors reported that they needed further training to cope well with their duties. While this could be a source of concern, the absolute number of persons reporting they need further training to cope with their duties indicates that a digital transformation would not be an impossible hurdle. Other studies [5] have also shown that internet skills do not differ substantially between public administrators and ordinary citizens, but that ordinary citizens score marginally higher on operational internet skills, whereas public administrators score marginally higher on formal internet skills, information internet skills and strategic internet skills. No recent data on this issue could be located.

Initial KPIs:

- Number of public officials having basic ICT skills
- Public officials' self-reported operational, formal, information and strategic internet skills
- Public officials´ satisfaction with digital skills
- Number of public officials who have participated in formal ICT-related training

3.4 Make digital transformation a priority for all public officials, not just for those involved in mass processes

We found that top civil servants in most countries see e-government as moderately important, but there are again differences across countries. E-government is considered a priority especially for public officials working in organizations involved in routine high-volume service delivery, where digital services can have a large impact. Other parts of the public sector that are not involved in mass processes also need to make e-government a priority.

Initial KPIs:

- Priority attached to digital transformation by public officials, by sector

3.5 Supplying alternatives may hamper the take-up of online service

In the case we studied, we found that the Latvian government has opened a large number of citizen service centers, and more are planned to open in the future. The easy access to this alternative results in people finding it more convenient to use the offline alternative rather than using the service online. The fact that the offline alternative exists and can be used with ease is an important reason for its continued use. In the Latvian case, the high number of CSCs and easy access may be a factor in stopping people from switching to online services. The Technology Acceptance Model in this case suggests low perceived usefulness of the new technology, and an ease of use that is only marginally different from the existing widely available offline alternatives.

Initial KPIs:

- Reported convenience of offline services compared to online equivalents
- Number of users of offline services where online alternative is available
- Evolution in the number of citizens switching from physical to digital services
- Number of citizens exiting digital services to return to non-digital alternatives

3.6 Offline services have a support function for making people go online

We found that citizens appreciate in-person help in order to make the transition to using online services. Offline offices may help citizens make the step towards online service use. This is in line with earlier work that has shown that it is not the digital skills citizens' possess that are essential in predicting citizens´ online channel choice [6]. This finding also suggests that trust in government, a factor that is often studied in e-government adoption research, is probably not a strong explanatory factor, because citizens do visit the physical government centers to directly interact with government employees. Respondents appreciate the possibility of asking questions and receiving professional advice. This not only related to complex cases but also to more mundane issues like filling-out forms. Respondents are afraid of making mistakes and seek reassurance. They have the perception that the online system is too complicated. Even simple systems can be seen as complicated. The complexities of the electronic system, the fear to make a mistake, and the lack of understanding the procedure have a negative impact on the use of the electronic services. At the same time, stimulating citizens to go online is not just a task for government, as private parties have a similar interest in stimulating their customers to go online; this is for instance the case for banks and utility companies.

Initial KPIs:

- Citizens´ trust in public administration
- Citizens' trust in electronic government services
- Perceived difficulty of using electronic government services
- Citizens' fear of making mistakes on government forms
- Distance to closest offline alternative service in the neighbourhood
- Number of citizens visiting their bank branch for routine operations instead of using internet bank

3.7 Do not underestimate the social function of public services

Our study showed that visiting physical public service offices is seen as a way of socializing. We found that people like to go to the Citizen Service Centers to find out about news in their area. Especially older people or unemployed, who have more time can meet other people with similar problems and/or interests and discuss. This aligns with sociological research discussing the role of public meeting points in rural areas [7], a function fulfilled by offline government service centers. Making public services digital will undermine the social function of public services and alternatives may have to be provided to keep the local social fabric intact.

3.8 Stimulate legal compliancy

From the interaction with public administrations and the use cases in particular, we found that legal issues could be a factor that might be hindering the proper or optimal performance of public service provision. In most, if not all cases, it is not the legal rules themselves that prevent optimal results but a lack of clarity on the rules and how to apply them within the organization as a whole. This can lead to the specific relevant staff members creating unwanted and unintended hurdles for the organization as a whole in their respective functions, by over-applying certain rules or applying them incorrectly. Of course, the opposite may happen as well. An incorrect understanding may lead to a way too lenient application of certain rules, leading to invalid actions or even illegal activities and serious compliancy risks. In order to provide optimal public services, legal compliancy should be a prerequisite. Therefore, we also focused on determining what guidance and/or training is needed for such compliancy to be facilitated.

GDPR compliancy is of course of high relevance here, since the GDPR will be applicable to virtually all public service provisions. Moreover, the GDPR requires the PAs to facilitate a range of data subject requests, which are also in a sense a service that the PAs should render in an optimal way.

Initial KPIs:

- Presence of general role-related legal training and guidance for staff
- Presence of guidance on the use of electronic documents and instruments such as e-signatures, e-timestamps and e-authentication methods in the provision of public services
- Presence of guidance on e-privacy aspects for online interactions with citizen
- Presence of legally compliant procedures deal with data subject rights requests under the GDPR
- Presence of information on data processing in clear and intelligible language in all relevant places and easily accessible by citizen (website, platform, at place of physical provision of services, other interactions)
- Relevant personnel have received basic training on data protection principles and GDPR
- PA has a DPO, which is involved in all data protection matters relating to public services
- Presence of legal guidance concerning data protection principles and requirements (choice of legal basis, complying with data processing principles, fulfilling information duty)
- Low level of legal issues manifested at the PA concerning the foregoing
- Low level of legal certainty/clarity measured at the PA concerning the foregoing

.

4 Initial recommendations to support PA transformation

This section offers general recommendations based on the first conclusions of the analysis carried out to develop the DIGIMAT [1].

The main objective to assess the Digital Maturity of a Public Administration is to provide recommendations for its improvement. The scope of the maturity model was centred on the digital aspects of e-government and e-services engineering and delivery. However, the maturity model will also record other aspects, such as the willingness of civil servants to co-create with citizens, recommendations on how to address the social factors of non-use, as well as additional aspects that facilitate a customer centric service design mindset and approach in PA.

We have divided the recommendation in this chapter in two different areas: the first deals with the legal aspects related to GDPR whereas the second is focused on technical and organizational issues.

4.1 Improving Legal compliance with GDPR

The main legal aspect measures relate to how well the PA has implemented data protection law, namely the GDPR. This should be an essential part of digital maturity in the delivery of public services, especially e-services.

Four general levels of GDPR compliance have been defined:

- **Clear compliance issue(s**) = high risk of trouble if data protection authority investigates
- **Paper compliance or low compliance** = risk of trouble if data protection authority investigates, but the most essential things have been taking care of, although significant gaps exist compared to best practice
- **Medium compliance =** low risk of trouble if data protection authority investigates, concepts have been applied both formally and in an acceptable manner in practice.
- **Full compliance =** near to no risk if data protection authority investigates, GDPR has been fully implemented according to best practices.

These levels are addressed per topic. There are ten topics, representing essential elements of GDPR compliance. Organizations should strive toward the ideal situation of full compliance. For each topic, recommendations are gathered that would help an organization to achieve higher levels. The recommendations are not binding legal advice.

4.1.1 Topic 1: Awareness and training

From “compliance issues” to “low compliance”: Make sure to have a written data protection policy detailing guidelines on how to deal with personal data within your organization. Organize GDPR training. Ensure you can have some proof

From “low compliance to “medium compliance”: Ensure that your policies are intelligible and accessible. Give regular training, with focus on specific GDPR aspects. Ensure that you can prove what the training entailed and who attended, if necessary.

From “medium compliance” to “full compliance”: Make sure that policies are not only easy-to-understand and easily accessible, but verify that people know when to consult them and how to use them. Gather proof on this. Give regular GDPR training and updates, specific to different profiles. E.g. HR people get different training than the marketing team or civil servants who directly interact with the public in public service provisioning. Ensure you can provide proof of these educational efforts, including test results for (essential) personnel, based on their identified needs.

Initial KPIs:

- Presence of a written data protection policy
- Understandability and accessibility of internal GDPR related policies
- Number of times GDPR training is provided
- Specificity of GDPR training (regarding topics and personnel)
- Presence of GDPR-tests and test results

***Bonus tip**: CITADEL has created several privacy literacy exercises. These are a perfect tool for civil servants to test their knowledge and awareness level, while simultaneously learning the GDPR principles through taking the test and reading the explanation provided.*

4.1.2 Topic 2: GDPR governance and DPO

From "compliance issues" to "low compliance": Appoint a DPO, create or maintain a governance structure for GDPR and makes sure the DPO is involved where necessary. Additionally, and in a broader sense, make sure that the DPO is involved in the high-profile data protection/privacy related topics.

From "low compliance to "medium compliance": Make sure the DPO is reasonably independent (can report to management, does not receive instructions) and has sufficient knowledge. Have a governance structure which includes the DPO as a standard member with an appropriate role. Make sure the DPO is involved in most of the data protection related issues.

From "medium compliance" to "full compliance": make sure that you have a fully trained DPO who is a true specialist in GDPR compliance and has a thorough understanding of the systems used by the PA and the operational functioning of the PA. Automatically involve the DPO in all matters related to data protection. Make sure all employees know who the DPO is and how and when to contact the DPO.

Initial KPIs:

- Presence of a DPO
- DPO is independent and competent
- Presence of a GDPR governance structure
- Inclusion of the DPO in high-profile data protection/privacy issues
- The DPO is known to be the DPO and reachable to all personnel

4.1.3 Topic 3: Record and oversight of processing activities

From "compliance issues" to "low compliance": Keep a record, update it and have other relevant information centrally available.

From "low compliance to "medium compliance": Ensure the record has been verified, that it is updated regularly and that there is a central repository for extra compliance information and compliancy relevant documents. Have guidelines on the use of these documents and the use of the repository.

From "medium compliance" to "full compliance": Ensure that the record really matches reality. Update regularly, not only at set intervals but also when changes in the operation mandate this. Have a central repository which clear role-based access rules and rules on the use of the information. Make sure that for all processing activities, clear documentation on choices made is present, not just in a piecemeal manner. Have structure and oversight in the documentation.

Initial KPIs:

- Updated GDPR records are kept
- GDPR records are verified
- Existence of a repository of compliance information and relevant documents
- Guidelines on the use of compliance documents are present.
- Clear documentation is present on all processing activities
- Presence of structural oversight on all compliance related documentation

***Bonus tip**: many supervisory authorities have models and guidance available to help you organize a record of processing activities and the additional structure that enables you to have a clear oversight of processing activities. As the questions clarify, the record need not reflect all information you have about your processing activities, but this information should be kept internally.*

4.1.4 Topic 4: communication about processing (data processed, purpose of processing, legal ground)

From "compliance issues" to "low compliance": Make sure you have policies/notices for the website (very visible), as well as for all GDPR relevant projects, but certainly specific policies for sensitive projects or projects with potential strong impact. Ensure that policies contain all of the legally required minimum information, and that all purposes of the intended activities are at least covered by a legal base.

From "low compliance to "medium compliance": Ensure that differentiated policies are present for all projects which require this. The DPO should be consulted as much as possible, certainly for sensitive projects. Policies and notices should contain all legally required minimum information, as well as the legally required additional information in those cases which require it. The purposes of the intended processing activities, and the legal basis invoked are detailed more specifically in the policy/notice

From "medium compliance" to "full compliance": Ensure that differentiated policies are present for all projects which require this and always involve the DPO. Make sure the privacy policies/notices are truly easy to understand and contain all legally required information (basic and extended, depending on the situation) in an easy-to-understand format. Ensure that the different purposes are clearly distinguished and that it is easy to understand which legal ground is invoked exactly for which part of the processing covered by the policy/notice, as well as the consequences that are tied to this choice of legal basis in terms of the potential for the data subject to make certain requests for the exercise of his/her rights.

Initial KPIs:

- Website policies/notices are visibly presented online
- Policies contain all legally minimum required information, including intended activities
- Presence of differentiated information for all projects for which this is mandatory
- Presence of additional legal information in projects where this is required
- The DPO is always included in all projects that require its inclusion
- Privacy policies/notices are easily understandable and contain all legally required information (basic and extended, depending on the situation)
- The different purposes and legal grounds are readily distinguishable from the documents.

4.1.5 Topic 5: Consent in the PA

From "compliance issues" to "low compliance": Consent must not be used in every case, nor is it plausible that consent is never used. Define some approach to the use of consent as a legal ground, at least defining some case where consent is useful as a last measure alternative and some cases where consent is not appropriate. Gather consent explicitly and with an affirmative action. The consent should be allowed to be withdrawn in principle, without any requirement for the data subject to give reason.

From "low compliance to "medium compliance": Make sure consent is well understood as a legal ground within the organization, as a result of study, training or experience. Most people involved in the choice of the legal ground must have a good grasp of the concept and its application, and involve the DPO when they deem it necessary. Ensure consent is gathered explicitly and with an affirmative action and is accompanied by specific, clear and intelligible information, although it is allowed to do this as part of a larger communication. There must be a procedure for giving effect to withdrawal of consent, in which the DPO is involved where the procedure doesn't yield the expected results. Satisfactory results are typically achieved for the data subject.

From "medium compliance" to "full compliance": Make sure that consent is fully understood by relevant staff, nonetheless formally involving the DPO in every case. Ensure that consent is gathered explicitly and through an affirmative action and is always accompanied by clear and intelligible information, which is easily accessible and stands out from the larger context, if any, so that the data subject can easily identify the relevant part and easily access it. Make sure there is an advance procedure to deal with data subject requests for withdrawal and that these are follow-up quickly, effectively and always yield a satisfactory result for the data subject, combining tried and tested procedures in which the DPO is formally involved with ad hoc treatment of exceptional cases.

Initial KPIs:

- Define when the use of consent as a legal ground is necessary
- Consent is gathered explicitly and under affirmative formulation
- Consent can be withdrawn without any requirements
- Consents is well understood, trainings on this topic are provided
- Consent is accompanied by specific, clear, and intelligible information
- The DPO is involved in situations in which the withdrawal of consent doesn't yield the expected results
- Presence of an advanced procedure to deal with data subject requests for withdrawal, including quick follow-up

4.1.6 Topic 6: Accommodating citizen's rights as data subjects

From "compliance issues" to "low compliance": Make sure there is procedure to deal with data subjects requests and an easy-to-reach point of contact. Ensure that most of the requests can be dealt with, if the data subject meets the conditions for the right in question. If you are not able to provide what is requested although you are under the law obliged to, explain the reasoning to the data subject and try to find a solution. Make sure to answer within the legal terms and to not charge unless the law allows this.

From "low compliance to "medium compliance": Ensure the DPO is either in charge or always formally involved and not just ad hoc when difficult situations pop up. Make sure there is guidance on how to deal with requests within the organization, covering also the scenarios when it is valid to refuse a request. You should be able to implement nearly every request, if valid. If this proves impossible there is a genuine effort to provide the data subject with an alternative

solution and a feedback loop to prevent similar issues in the future. Strive to answer within the minimum term of one month and as far as possible to implement decisions in that timeframe too. Inform clearly and do not charge unless legally allowed, while making this clear to the data subject.

From "medium compliance" to "full compliance": You must ensure that the procedure is fully integrated between all relevant departments and the DPO is either formally in charge or formally involved in every case. Additionally, there is specific guidance on how to deal with requests in a practical and easy-to-access manner, including templates (also for denial of invalid requests) and decision trees or equivalent tools. Valid requests are always able to be granted. Strive for even greater service in answering and implementing decisions, providing updates and support for the data subject. When dealing with unreasonable requests, let the data subject choose whether to agree to the charges or not, providing clear information and support.

Initial KPIs:

- There is a procedure to deal with data subjects requests and an easy-to-reach point of contact
- In case requests cannot be dealt with, reasons are provided and solutions are found
- the DPO is either in charge or always formally involved when difficult situations arise
- Answers to requests and decision implementations are provided within a month
- The citizen's rights as data subjects procedure is fully integrated between all relevant departments and the DPO
- There is specific guidance on how to deal with requests in a practical and easy-to-access manner

4.1.7 Topic 7: data breach management

From "compliance issues" to "low compliance": Make sure you have a data breach management procedure written down and that it is mentioned in training to staff. Verify through a test or an incident that it has basic functionality.

From "low compliance to "medium compliance": Make sure the data breach management procedure involves the right people and has a clear leadership. Ensure the policy has been communicated about within the organization so at least a core of relevant personnel know what to do and has access to the policy. Verify through a test or an incident that the policy is fully functional to deliver the necessary information to decide on whether to notify or not within the legal time limits.

From "medium compliance" to "full compliance": Make sure the data breach management procedure involves all the right people from the start and contains clear and practical guidance on how to deal with incidents. Ensure the procedure contains a clear feedback loop. Ensure that all personnel knows about the procedure and their role in it, and sufficient relevant roles have access. Verify, through a test or when an incident occurs, that the procedure functions properly, easily enabling you to contact the right people and gathering the needed information, leading you to -barring extreme technical difficulties- to always easily reach an informed decision well within the legal time limits.

Initial KPIs:

- There is a written data breach management procedure, communicated and practiced with the staff
- Staff exercises regarding the data breach management procedure are performed

- The data breach management procedure contains clear and practical guidance on how to deal with incidents
- The functioning of the procedure is tested on inclusion of the right people, information fathering, barring of extreme technical difficulties and legal time limits.

4.1.8 Topic 8: DPIA and data protection by design and default

From "compliance issues" to "low compliance": Ensure that within the organization, relevant people know how to carry out a DPIA. Equally, make sure that relevant profiles know how to implement data protection by design and default, e.g. by giving training or enlisting qualified trainers.

From "low compliance to "medium compliance": Ensure that the DPIA knowledge is surrounded by a framework for the organization which indicates when a DPIA is necessary based on the official guidance available, who to involve (DPO) and what consequences to attach to a DPIA, depending on the outcome. Make sure that the concepts of data protection by design and default are well understood and implemented in practice, building experience within the organization and providing guidance in the form of practical examples to be consulted at all times, next to appropriate training.

From "medium compliance" to "full compliance": Make sure DPIA's are part of a larger procedure detailing when to carry them out, who to involve, who to share the results with, the consequences etc. within the organization. Additionally, verify that the DPIA's are based on international best practices and are carried out appropriately. Ensure that the concepts of data protection by design and default are always implemented, through providing proper training and a plethora of supporting measures, tips and tricks, at the same time ensuring these concepts are part of all relevant workflows.

Initial KPIs:

- The relevant people know how to carry out a DPIA
- The relevant profiles know how to implement data protection by design and default
- There exists a DPIA knowledge framework based on the official guidelines regarding who to involve and what the consequences are
- The concepts of data protection by design and default are well understood and implemented
- Whether the DPIA's are based on international best practices and are carried out appropriately is verified
- Trainings on concepts of data protection by design are provided

4.1.9 Topic 9: International

From "compliance issues" to "low compliance": identify through your record of processing activities (ROPA) created when doing your initial GDPR compliance exercise which transfers you have knowledge of. Verify whether all of these are surrounded by appropriate safeguards and if not the case, work on rectifying this.

From "low compliance to "medium compliance": carry out an additional check to identify all transfers next to your initial and general GDPR compliance exercise. Ensure that for all transfers measures are in place.

From "medium compliance" to "full compliance": make checking for transfers a continuous exercise and implement this in existing procedures and workflows. Make sure there is reporting to the DPO and relevant staff and that for all transfers a safeguard mechanism is in place. If a

new transfer is found where such a mechanism is lacking, temporarily suspend the transfer until a solution is found.

Initial KPIs:

- Transfers are identified (using ROPA)
- The transfers are surrounded by the appropriate safeguards
- Additional checks on identifying safeguards are carried out
- All transfer measures are in place
- The checking of transfers is a continues exercise
- Transfers are reported to the DPO and the relevant staff
- Transfers are suspended when mechanisms are lacking

4.1.10 Topic 10: contracts

From “compliance issues” to “low compliance”: Make sure you have, through your initial GDPR compliance exercise, identified nearly all processors and have some form of contract with them that satisfies prima facie the conditions of article 28 GDPR. Ensure you have made good efforts to identify instances of joint controllership and that you have an arrangement fulfilling the conditions of article 26 GDPR, e.g. by creating a template. Make sure there is a clause in the employment contract referring to the labour rules/standards, with the latter containing at least basic information on data processing and instructions on how staff should process data.

From “low compliance to “medium compliance”: Make sure you have identified all processors and that you have a contract with all of them. Try to have contractual terms which are clear and without too much argument would hold in court under article 28 GDPR. Ensure you have an overview of sorts on sub-processors and that all or nearly all contracts contain reasonable provision on this. Ensure that nearly all instances of joint controllership have been identified and have the necessary contractual or other arrangements under article 26 GDPR. Provide guidance and/or training on this to the staff and try to create a template agreement to be used or otherwise provide guidance on how to create a joint controller agreement containing the essential provisions (which goes beyond what article 26 GDPR requires, which is very little). Make sure there is a clause in the employment contract referring to the labour rules/standards, with the latter containing information on data processing and instructions on how staff should process data in clear and plain language.

From “medium compliance” to “full compliance”: Make sure you have identified all processors and that you have a contract with all of them. Make sure all contractual terms are best practice or near enough that it doesn’t matter, ensuring compliance with article 28 GDPR. Ensure you have an overview on sub-processors and that all contracts contain clear rules on this. Ensure that all current instances of joint controllership have been identified and have the necessary contractual or other arrangements under article 26 GDPR and that there is a continuous assessment and guidance for the future. Provide this guidance and/or training broadly to relevant staff and try to create a template agreement to be used or otherwise provide guidance on how to create a joint controller agreement containing all necessary and useful provisions (which goes beyond what article 26 GDPR requires, which is very little). Make sure there is a clause in the employment contract referring to the labour rules/standards, with the latter containing information on data processing and instructions on how staff should process data in clear and plain language, which is easy to be understood. Make sure this information is easily accessible. Where feasible, use alternative techniques to plain text to additionally convey this information (video, training, drawings etc.).

Initial KPIs:

- All processors are identified
- The conditions of article 28 GDPR are satisfied 'prima facie'
- Arrangements for fulfilling article 26 GDPR are in place
- Employment contracts contain a clause on how employees should process data
- There is an overview of all sub-processors regarding contracts
- All instances of joint controllership are identified and have the necessary contractual or other arrangements under article 26 GDPR
- Guidance and/or training to relevant staff is provided
- There is a template agreement on how to create a joint controller agreement containing all necessary and useful provisions
- There is a clause in the employment contract referring to the labour rules/standards containing information on data processing and instructions on how staff should process data in clear and plain language

4.2 Improving the Digital Maturity in PA

The recommendations in this section refer to how PA organizations are prepared for the digital stage. The aspects analysed here are: general ICT Issues, data processing, how PAs uses the emerging technologies to deliver public services, and how PAs interact with the civil servants, citizens, and other external agents.

Enabling the access, use and re-use of public data enables the creation of a data-driven culture in the public sector. This serves to increase the openness of the administration, but also serves to maximise public economy and social value [8].

One challenge in making Public Sector Information (PSI) available and re-usable occurs whenever PSI contains personal data. In cases where PSI contains personal data, the primacy principle of data protection comes into play. It states that any PSI law has to be applied in coherence with data protection law, without exceptions, as the protection of personal data is recognized as a fundamental right [9]. In order to support the opening of PSI while protecting personal data, the PSI directive established a triple assessment:

1. Determine whether the PSI contains personal data.
2. Determine whether national access regimes restrict access to the PSI. If yes, the same restrictions apply to PSI publication and re-use as well.
3. PSI containing personal data that is opened for re-use should only be processed in compliance to data protection law.

Dynamic data is one of the most commercially valuable types of data, as it can be used for products and services that provide information in real time, such as travel or transport apps. Whenever possible, implement application programming interfaces (APIs) to access public dynamic data [10].

Provide several formats: To further reduce the barriers to reuse, it is important to provide the data in various open formats, including CSV, ODS, JSON, RDF, etc. Furthermore, it is important to look at domain specific standards to improve the semantic interoperability of published datasets (Geography Markup Language (GML) for geographical data, for example).

Make the digital public services accessible from different types of devices (e.g.: desktop computers, mobile smartphones) and different operating systems (e.g.: Windows, Linux, MacOS, iOS, Android, etc.). This will ease the access of the citizens regardless of their specific equipment or the moment of the day. At this respect, the *responsive* web design is

recommended, because it makes pages render well on a variety of devices and window or screen sizes, ensuring usability and satisfaction to the user.

Consider the development of a dedicated mobile application or *app*, a functionality that needs be installed on a device by the end user before it can be used. This kind of application requires an initial involvement of the user to install it but can provide a better user experience, more functionality than those offered by a simple web page.

The security mechanisms implemented are an important factor in the confidence the users have in using the PA's digital services. As a minimum, secure web connections (HTTPS), that ciphers all the communication, should be mandatory. More sophisticated mechanisms as user digital certificates or digital identity cards are also welcomed.
Initial KPIs:

- The PAs public data are reusable
- Public dynamic data is accessible through application programming interfaces (APIs)
- The data are provided in various open formats (CSV, ODS, JSON, RDF, etc.,)
- Datasets are published in accordance with domain specific standards
- The digital services are accessible from different types of devices
- Services are provided/accessible via a digital app
- Web connections are encrypted
- Web connections use digital certificates or digital identity cards

The services of a public administration should be designed in an integral manner, so that they are interoperable with others (i.e.: they share and integrate information). Interoperability can be achieved among the services of the same department, with other departments or even with services of another national/international PA.

Try to explore feedback mechanisms to improve public services. Creating feedback mechanisms for users can allow, on one hand, to increase the data quality and, on the other hand, discover flaws on the design, poor performance or defects in the workflow of services that, if attended, would conduit to better services.

Explore the possibility to use open standards when possible. Easy accessibility and findability is an important aspect of open data. It seems a good practice, for example, to agree on a common metadata format that makes datasets easier to find via a portal, such as the *DCAT Application Profile for Data Portals in Europe (DCAT-AP)* for describing open datasets. Other open specification can be (CPSV-AP [11], European Interoperability Framework [12], or the Linked Open Statistical Data (LOSD).

PAs should create a process to involve stakeholders when trying to design new digital services. This way they will develop clear business cases, reflecting the needs of citizens and public servants at the same time [8].

When implementing the digital strategy, the authorities should establish effective organisational and governance frameworks to co-ordinate implementation. In this sense, it is important to identify clear responsibilities that ensure overall co-ordination; and also to establish a system for checking decisions on spending on technology, to increase the level of accountability and public trust.

Initial KPIs

- The PA services are interoperable

- The PA provides a mechanism through which users can provide feedback on services
- Metadata are compiled using open standards
- Metadata are compiled using a common metadata format
- The design of new digital services includes the involvement of stakeholders

PAs should develop and implement digital strategies which ensure greater transparency, openness and inclusiveness of government processes and operations. For this reason, they have to adopt as the main goals of digital government strategies the accessibility, transparency and accountability. Furthermore, the authorities should address "digital-divides" to avoid the emergence of new forms of "digital exclusion" [8].

The group of citizens selected to participate in administrative decision-making processes is an important factor in the success of such initiatives. It is recommended that the following factors are taken into account in the selection process: make sure that they have sufficient knowledge, competence, and skills to participate effectively, and make sure they are representative of the target audience for the service in question. This will increase public officials' willingness to engage with citizens

When defining the digital services, it is always advisable to offer personalization capabilities to the user. This will make the experience more friendly and enjoyable, hence better engaging the final users to the digital version of the service. Some examples of personalization are to have a specific home page, to define a list of favourite/most used services, to have a preferred identification mode or to define the preferred feedback mechanism.

One of the aspects that do not receive the required attention in public institutions is the management of the implementation of digitalization projects. A recommendation in this sense is to reinforce the public sector's digital and project management skills, and to mobilise collaborations and/or partnerships with private sector actors if necessary. This will help to establish evaluation and measurement frameworks for projects' performance, to apply standard guidelines, and regular reporting on digital initiatives, to facilitate the conditional release of funding.

Initial KPIs

- The PA has an organizational and governance framework for coordinating the implementation of the digital strategy
- The PA implementation strategy of digital services complies with the principles of accessibility, transparency, and accountability
- The participation of knowledgeable, competent, and skilful citizens is stimulated
- The citizens participating in the decision-making process are representative of the policies target population
- Digital services make use of personalization capabilities
- The PA provides training in project management skills

5 KPI summary

Several KPIs have been formulated in this deliverable. The list below contains all KPIs

At the level of the service or the service environment:

- Extent of broadband coverage in rural areas
- Number of citizens actively using online banking facilities
- Number of inhabitants/service beneficiaries without electronic ID card or government portal login credentials
- Number of households without internet connection
- Distance to closest offline alternative service in the neighbourhood
- Presence of general role-related legal training and guidance for staff
- Presence of guidance on the use of electronic documents and instruments such as e-signatures, e-timestamps and e-authentication methods in the provision of public services
- Presence of guidance on e-privacy aspects for online interactions with citizen
- Presence of legally compliant procedures deal with data subject rights requests under the GDPR
- Presence of information on data processing in clear and intelligible language in all relevant places and easily accessible by citizen (website, platform, at place of physical provision of services, other interactions)
- PA has a DPO, which is involved in all data protection matters relating to public services
- Presence of legal guidance concerning data protection principles and requirements (choice of legal basis, complying with data processing principles, fulfilling information duty)
- Low level of legal issues manifested at the PA concerning the foregoing
- Low level of legal uncertainty/unclarity measured at the PA concerning the foregoing

At the level of public officials:

- Extent of support for democratic values among public officials
- Number of public officials thinking that participation slows down decision making
- Number of public officials thinking participation improves decision making
- Proportion of public officials thinking citizens have sufficient skills and knowledge to contribute to decision making
- Proportion of public officials thinking citizens participate to pursue the interests of the entire community
- Number of public officials having basic ICT skills
- Public officials' self-reported operational, formal, information and strategic internet skills
- Public officials´ satisfaction with digital skills
- Number of public officials who have participated informal ICT-related training
- Priority attached to digital transformation by public officials, by sector
- Relevant personnel have received basic training on data protection principles and GDPR

At the level of citizens:

- Public support for expert decision-making
- Number of citizens having sufficient confidence to take part in public decision-making

- Socio-demographic composition of citizens providing input resembles that of the wider population
- Number of citizens participating in service delivery and design
- Number of citizens without basic digital skills
- Number of citizens without basic digital skills, broken down by SES group
- Number of citizens without basic digital skills, broken down by level of urbanization of residence
- Citizens' self-reported satisfaction with ICT skills
- Number of clients/citizens aged 65+
- Reported convenience of offline services compared to online equivalent
- Number of users of offline services where online alternative is available
- Evolution in the number of citizens switching from physical to digital services
- Number of citizens exiting digital services to return to non-digital alternatives
- Citizens´ trust in public administration
- Citizens' trust in electronic government services
- Perceived difficulty of using electronic government services
- Citizens' fear of making mistakes on government forms
- Number of citizens visiting their bank branch for routine operations instead of using internet bank

Regarding improving legal compliance with GDPR:

- Presence of a written data protection policy
- Understandability and accessibility of internal GDPR related policies
- Number of times GDPR training is provided
- Specificity of GDPR training (regarding topics and personnel)
- Presence of GDPR-tests and test results
- Presence of a DPO
- DPO is independent and competent
- Presence of a GDPR governance structure
- Inclusion of the DPO in high-profile data protection/privacy issues
- The DPO is known to be the DPO and reachable to all personnel
- Updated GDPR records are kept
- GDPR records are verified
- Existence of a repository of compliance information and relevant documents
- Guidelines on the use of compliance documents are present.
- Clear documentation is present on all processing activities
- Presence of structural oversight on all compliance related documentation
- Website policies/notices are visibly presented online
- Policies contain all legally minimum required information, including intended activities
- Presence of differentiated information for all projects for which this is mandatory
- Presence of additional legal information in projects where this is required
- The DPO is always included in all projects that require its inclusion
- Privacy policies/notices are easily understandable and contain all legally required information (basic and extended, depending on the situation)
- The different purposes and legal grounds are readily distinguishable from the documents.
- Define when the use of consent as a legal ground is necessary
- Consent is gathered explicitly and under affirmative formulation
- Consent can be withdrawn without any requirements

- Consents is well understood, trainings on this topic are provided
- Consent is accompanied by specific, clear, and intelligible information
- The DPO is involved in situations in which the withdrawal of consent doesn't yield the expected results
- Presence of an advanced procedure to deal with data subject requests for withdrawal, including quick follow-up
- There is a procedure to deal with data subjects requests and an easy-to-reach point of contact
- In case requests cannot be dealt with, reasons are provided and solutions are found
- the DPO is either in charge or always formally involved when difficult situations arise
- Answers to requests and decision implementations are provided within a month
- The citizen's rights as data subjects procedure is fully integrated between all relevant departments and the DPO
- There is specific guidance on how to deal with requests in a practical and easy-to-access manner
- There is a written data breach management procedure, communicated and practiced with the staff
- Staff exercises regarding the data breach management procedure are performed
- The data breach management procedure contains clear and practical guidance on how to deal with incidents
- The functioning of the procedure is tested on inclusion of the right people, information fathering, barring of extreme technical difficulties and legal time limits.
- The relevant people know how to carry out a DPIA
- The relevant profiles know how to implement data protection by design and default
- There exists a DPIA knowledge framework based on the official guidelines regarding who to involve and what the consequences are
- The concepts of data protection by design and default are well understood and implemented
- Whether the DPIA's are based on international best practices and are carried out appropriately is verified
- Trainings on concepts of data protection by design are provided
- Transfers are identified (using ROPA)
- The transfers are surrounded by the appropriate safeguards
- Additional checks on identifying safeguards are carried out
- All transfer measures are in place
- The checking of transfers is a continues exercise
- Transfers are reported to the DPO and the relevant staff
- Transfers are suspended when mechanisms are lacking
- All processors are identified
- The conditions of article 28 GDPR are satisfied 'prima facie'
- Arrangements for fulfilling article 26 GDPR are in place
- Employment contracts contain a clause on how employees should process data
- There is an overview of all sub-processors regarding contracts
- All instances of joint controllership are identified and have the necessary contractual or other arrangements under article 26 GDPR
- Guidance and/or training to relevant staff is provided
- There is a template agreement on how to create a joint controller agreement containing all necessary and useful provisions

- There is a clause in the employment contract referring to the labour rules/standards containing information on data processing and instructions on how staff should process data in clear and plain language

Regarding improving the digital maturity in PAs:

- The PAs public data are reusable
- Public dynamic data is accessible through application programming interfaces (APIs)
- The data are provided in various open formats (CSV, ODS, JSON, RDF, etc.,)
- Datasets are published in accordance with domain specific standards
- The digital services are accessible from different types of devices
- Services are provided using a digital app
- Web connections are encrypted
- Web connections use digital certificates or digital identity cards
- The PA services are interoperable
- The PA provides a mechanism through which users can provide feedback on services
- Metadata are compiled using open standards
- Metadata are compiled using a common metadata format
- The design of new digital services includes the involvement of stakeholders
- The PA has an organizational and governance framework for coordinating the implementation of the digital strategy
- The PA implementation strategy of digital services complies with the principles of accessibility, transparency, and accountability
- The participation of knowledgeable, competent, and skilful citizens is stimulated
- The citizens participating in the decision-making process are representative of the policies target population
- Digital services make use of personalization capabilities
- The PA provides training in project management skills

6 Conclusion

In this document we presented the initial version of the recommendations and best practices to help the policy makers to adjust the policy processes in order to facilitate the cooperation between all PA stakeholders. Furthermore, we provide a first tangible set of KPIs, initially due in the follow-up document to this report (D2.3).

The recommendations, best practices, and KPIs contained in this document were structured along four lines. The first focussing on the involvement maturity of public administrations, their willingness and ability to incorporate citizen input into the design of services. The second focussing on the drivers of non-use and non-take up of public services by citizens. The third line engaged with ten recommendations and KPI's on how to increase and stimulate PA compliance with GDPR rules. The fourth and final line provided a first look into the recommendations and KPIs contained in the Digital Maturity Assessment model.

This report provides only the initial recommendations, best practices, and KPIs produced in CITADEL WP2. The final report, D2.3 – Final Recommendations for Transforming the Public Sector Processes and Services, provides a follow-up and extension to this report.

7 References

[1] CITADEL Consortium, "D2.1 - Requirements and parameters for selection of relevant information," 2018.

[2] S. K. P. K. Yang, "Further Dissecting the Black Box of Citizen Participation: When Does Citizen Involvement Lead to Good Outcomes?," *Public Adm. Rev.,* vol. 71, no. 6, p. 880–892, 2011.

[3] H. L. S. Y. Liao, "Exploring the antecedents of municipal mangers' attitudes toward citizen participation," *2017.*

[4] J. V. D. W. E. A. Van Deursen, "Why e-government usage lags behind: explaining the gap between potential and actual usage of electronic public services in the Netherlands," in *International Conference on Electronic Government*, Berlin, Heidelberg, 2006.

[5] J. A. G. M. v. D. A. J. A. M. van Deursen, "eVaardigheden en eAwareness van Nederlandse ambtenaren," Enschede, 2009.

[6] M. G. J. A. J. v. D. W. E. Ebbers, "Impact of the digital divide on e-government: Expanding from channel choice to channel usage," *Government Information Quarterly,* vol. 33, no. 4, p. 685–692, 2016.

[7] A. S. Lægran, "The petrol station and the Internet café: Rural technospaces for youth," *Journal of Rural Studies,* vol. 18, no. 2, p. 157–168, 2002.

[8] OECD, "Recommendation of the Council on Digital Government Strategies," 2014.

[9] European Commission;, "European Data Portal, The PSI directive and GDPR".

[10] European Commission;, "Proposal for a revised Public-Sector Information (PSI) Directive," 2018.

[11] European Commission;, "Core Public Service Vocabulary Application Profile (CPSV-AP)," 2018. [Online]. Available: https://ec.europa.eu/isa2/solutions/core-public-service-vocabulary-application-profile-cpsv-ap_en. [Accessed August 2018].

[12] European Commission;, "European Interoperability Framework," 2017. [Online]. Available: https://ec.europa.eu/isa2/eif_en. [Accessed August 2018].