Towards the Implementation of the EU-Wide "Once-Only Principle": Perceptions of Citizens in the DACH-Region

Cigdem Akkaya, Helmut Krcmar

Towards the Implementation of the EU-wide "Once-Only Principle": Perceptions of Citizens in the DACH-Region

Cigdem Akkaya and Helmut Krcmar

[1] Chair for Information Systems, Technical University of Munich, Munich, Germany,
cigdem.akkaya@in.tum.de
[2] Chair for Information Systems, Technical University of Munich, Munich, Germany,
krcmar@in.tum.de

Abstract. This paper presents selected findings from a recent empirical research conducted in the context of modernization of public administrations. E-government adoption has reached a stagnation point over the last few years in the DACH region. The European Commission has been working intensively on projects aiming to overcome the existing digital barriers between EU Member States. Citizens repeatedly provide the same personal information to different public authorities, which causes frustration and inefficiency. The Once-Only Principle suggests that citizens should have the right of providing information to public authorities only once and that the provided data will be exchanged between national authorities of the EU Member States. By signing the Tallinn Declaration in October 2017, EU Member States have already committed to implement this principle. Sharing personal data of individuals between public authorities within national boundaries as well as with the public administrations of other EU Member States would assuredly ease-up data provision and increase efficiency. Yet, higher convenience comes at a cost of data protection and privacy, which becomes highly critical when sensitive personal data is involved. From this standpoint, a particular emphasis needs to be placed on understanding expectations, sensitivities and privacy related concerns of citizens, which is argued to be one of the key drivers behind the adoption of G2C e-government initiatives.

Keywords: E-Government, Single Digital Gateway, Once-Only Principle, Privacy and Data Protection, DACH Region.

1 Introduction

Utilization of e-government by transforming public service delivery is quite promising in terms of eliminating long queues, improving efficiency and providing higher convenience to citizens. Improving public service delivery by application of digital technologies is high on the political agenda of many EU countries. Despite considerable investments, success of most Government-to-Citizen (G2C) e-government initiatives remain far below expectations. It is not realistic to expect a sudden take-off without

analyzing the underlying barriers, which hold people back from an intensiver usage of digital public services. Although the sensitivities of nations may differ, privacy and data protection concerns are one of the widely recognized barriers to adoption of services in online contexts [1, 2]. For example, lack of confidential handling of data, fear of becoming a "transparent citizen", fear of data theft and lack of information about the usage of personal data shape the privacy related concerns and reluctance towards using e-government services in Germany [3, 4].

The issue of privacy becomes even more important considering the new initiatives of the European Commission (EC) that aim to modernize digital public services and improve their cross-border availability. The motivation of the project is clear. Increasingly more people cross national borders to live, study, work or retire. This creates additional documentation and paperwork. For instance, if a person works in one EU country but lives in another one (a.k.a 'cross-border commuters'), his or her (further "he") social security contributions are likely to be covered by the EU country where he works but if he loses his job, he may need to apply for benefits in the country where he lives. The necessary paperwork may be less in his original country. However, public authorities in the second country do not likely have any access to his personal records or any other previous information. Providing all this information to government agencies of another country is not only overwhelming and time consuming for individuals, but results also in additional financial burdens such as translation and notary costs.

In order to eliminate these problems and enhance cross-border activities within the EU, the EC has introduced a concept called the "Once-Only Principle" (OOP). With this concept, the provision of the same personal information to different government offices would be theoretically eliminated. Its implementation is quite essential due to its importance in successful cross-border digitalization. Indeed "enabling mobility of citizens and businesses[1] by cross-border interoperability" has been stated as one of the three policy priorities of the eGovernment Action Plan 2016-2020 [5]. Besides making life of citizens easier, exchange of information between government offices of different EU Countries could support fighting terrorism and crime.

In October 2017, by signing the Tallinn Declaration on eGovernment, the ministers in charge of eGovernment policy and coordination from 32 countries of the EU and the EFTA have committed to "take steps to identify redundant administrative burden in public services and introduce once-only options for citizens and businesses in digital public services by collaboration and data exchange across our administrations at national, regional and local level as well as with other countries for cross-border digital public services" ([6], p.4). The declaration acknowledges the protection of personal data and privacy by introducing the General Data Protection Regulation (GDPR). However, this regulation is focused mainly on interactions between companies and individuals rather than citizens and governments.

Data sharing and re-use of data, however, bring important questions about data protection. In some countries, data exchange between national public authorities is perceived with major resistance due to strong data protection regulations [7], therefore,

[1] The OOP is introduced for both citizens and businesses but we focus on citizens as G2B e-government goes beyond the scope of this paper.

individuals would be likely to be more reserved towards data exchange between public authorities of all EU Member States. The EU level documents are kept mostly quite high-level without providing much detail about implementation and their consequences for end-users. Neither the Tallinn Declaration [6] nor the eGovernment Action Plan 2016-2020 [5] specify the type, details or scope of information to be shared within the EU Member States. In fact, they mostly focus on benefits of this approach and potential savings to be achieved through its utilization.

We argue that design and implementation of such initiatives needs to be done with utmost care by taking the concerns and sensitivities of the individuals into account. To the best of our best knowledge, academic research on G2C e-government has not yet tackled the citizen perspective of the OOP with empirical analyses. Other than a few conceptual papers [8-12], a study focused on its legal perspective [13] and project reports [14][2], no empirical study reflecting the citizens' perspectives on OOP could be found. As the implementation of the OOP is still in its infancy, we aim to gain early insights, which could possibly be taken into consideration when planning its implementation. In particular, we focus on understanding privacy related concerns of the DACH region citizens. The following questions guide this research:

RQ1. How has the rate of G2C e-government adoption annually changed between the years of 2014 and 2017 in the DACH region?

RQ2. What are the characteristics of a modern government agency from the perspective of citizens in the DACH region? Do they consider the OOP as a characteristic of a modern government agency?

RQ3. What is the opinion of citizens in the DACH region regarding sharing data between public authorities?

RQ3.1. What is their opinion regarding data sharing between public authorities within their own country?

RQ3.2. What is their opinion regarding data sharing with public authorities of other EU Member States?

As we employ nationwide representative samples, the results are generalizable to the whole population.

2 Background and Literature Review

2.1 Digital Single Market Strategy and Digital Single Gateway

To facilitate the operation of the EU Single Digital Market, the EC has introduced the Single Digital Gateway Strategy in May 2015 [15]. This strategy aims to unlock the

[2] There has been some empirical studies conducted within the scope of the TOOP project however their focus were businesses rather than citizens.

full potential of the European Single Market. In particular, it foresees the free movement of persons, services and capital within the EU, irrespective of their nationality or place of residence.

The completion of the Digital Single Market was identified as one of the ten political priorities of the EC [15]. By opening up digital opportunities for people and business in the EU Member States, Europe's position as a world leader in the digital economy is aimed to be enhanced [15]. In order to streamline citizens' access to local authorities, the existing European portals need to be extended and linked to the Single Digital Gateway [15]. Currently, contact points between public authorities and citizens are fragmented and incomplete. Portals of the local authorities are mostly in the local language, which represent a substantial hurdle for cross-border activities.

By including this principle into the eGovernment Action Plan 2016-2020 [5], the EC aims to provide guidelines on supporting its implementation at regional and local levels. It is important to note that rather than developing a new portal, the Digital Single Gateway will be providing access to existing national portals from a single contact point. Overall, its development aims to support movement of individuals in cross-border settings by reducing the constraints imposed by existing borders.

2.2 The Once-Only Principle

OOP is one of the main cornerstones for enabling the efficiency of the Digital Single Market. The EC defines this principle as follows [5]:

> "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."

The particular benefits of the implementation includes reducing the administrative burden on citizens, achieving a more efficient government administration and increasing fraud prevention. According the SMART 2015/0062 report of the EC [16], the EU wide application of the OOP could result in annual net savings of as much as €5 billion per year. As a first step, the principle will be applied to exchange data between authorities within the same nation [6], as this is the prerequisite to cross-border data exchange. Implementation of it would likely require an update of the national infrastructures to ensure interoperability as well as a change in national legislations in particular data protection laws in some countries.

2.3 OOP Pilot Projects and Implementations

To explore and address the OOP related challenges in cross-border setting, the EC launched a call for proposals in 2016 [8]. After a careful analysis, two projects were selected for funding within the scope of the EU Horizon 2020 Research and Innovation

Funding Programme: 1) *The Once-Only Principle Project* (TOOP) [17] and 2) *Stakeholder Community Once-Only Principle For Citizens* (SCOOP4C) [18].

The TOOP focuses on the application of the OOP for businesses, while the SCOOP4C has the focus of e-services for citizens. The TOOP has been subject to three pilot projects to explore the feasibility of the concept for businesses, while there has not been any pilot projects conducted within the scope of SCOOP4C. According to a recent position paper [14], the implementation of the OOP for businesses in the EU Member States is still evolving[3], however not much is yet there at the cross-border e-Services level [16]. The EU strives to extend it across borders to further improve the efficiency of the Digital Single Market [15].

Another important issue is the clarification of which data regulation will be applied in case of cross-border e-services. Recognizing the importance of data protection in cross-border contexts, the EU has adopted a new data protection framework in 2016 to ensure data protection among the Member States. The GDPR came into force recently on May 25, 2018 [19]. Although the GDPR is aimed to supersede the EU Member State laws, changes in national legislations are necessary to ensure protection of citizens' privacy. Despite the required action of EU Member States, having a single regulation valid for all Member States is expected to be very beneficial considering the size of the EU in terms of eliminating conflicts such as which country's data protection regulation should be applied in cross-border settings [13].

Introduced as the most important change in data privacy regulation in 20 years [19], the data protection reform package underlines citizens' fundamental rights of data protection and foresees serious penalties up to 20 million Euro in case of breaches. Yet, in its current version, the GDPR is mainly focused on interactions between companies and individuals [19]. The implementation of the OOP would clearly benefit from a similar EU-wide data protection regulation defined for the G2C e-government context.

Estonia is one of the first countries that placed a special focus on the application of this concept both in national and in cross-border settings. The Nordic Institute for Interoperability Solutions Association was founded jointly by Finland and Estonia to develop online solutions to support cross-border operations as well as migration and commuting of citizens. In particular, data stored in numerous data repositories of the two countries are exchanged by utilizing the X-Road Technology. To support cross-border activities of citizens and businesses, its scope is planned to be extended to include the exchange of information between the tax authorities of the two countries [20].

Similar to its level of e-government take-off in the region [3, 4, 21, 22], Austria has taken the lead in implementation of the OOP concept in the DACH region. In Austria, financial aid is granted to families with newborn children automatically in most cases although up to six different government agencies are involved [18]. This is enabled through exchange of data in existing registries between public authorities. Due to positive feedback from the public, the Austrian government strives to fully automate the tax declaration and return service as well.

[3] There are various implementations for businesses in EU Member States, which are beyond the scope of this paper and can be found in [14].

3 Data Analysis and Results

This section provides empirical research results to tackle the research questions posed in the introduction section. Four in-depth surveys were conducted online between 2014 and 2017 by using representative samples [3, 4, 21, 22]. The samples included Internet users in private households. The data is weighted to be representative of the online population by central features of gender, age and formal education. Three relevant questions of this research will be discussed in this paper. Surveys have included other questions such as the knowledge of and satisfaction with online public services, which will not be discussed here due to space limitations.

3.1 Adoption of G2C E-Government Services in the DACH Region

The analysis of G2C e-government adoption between 2014 and 2017 reveal that, e-Government adoption in the DACH Region has reached a stagnation point over the last few years (see Fig. 1). In all years of analysis, Austria had the highest take-off levels, followed by Switzerland. Germany, on the other hand, remains relatively behind, reaching to its lowest level in 2017. Overall, a significant rise in the e-government adoption rate could not be observed in any of the DACH region countries over the past few years, despite the advancements in IT technology and various national and EU wide initiatives.

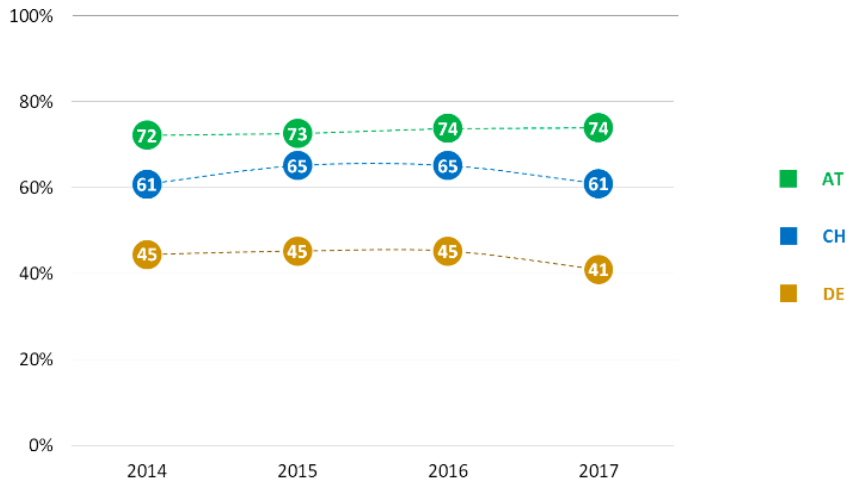

Fig. 1. Usage of G2C E-Government Services in the DACH Region (in percentages, based on [3, 4, 21, 22])

These findings confirm the findings of other recent analyses on G2C e-government adoption. According to the Digital Economy and Society Index (DESI) of the EC [23], Austria was ranked 6th in 2016 and 5th in 2017 among 28 EU countries in terms of its Digital Public Services, being placed over the average rate of development within the EU. In the same analysis, Germany was ranked 20th in both years, resulting in placement below the average rate of development within the EU Nations. Switzerland was not subject to analysis in this research. Similarly, the Capgemini EU eGovernment Benchmark report [24] categorized only Austria from the DACH region as one of the best performing countries in terms of e-government.

3.2 Characteristics of a Modern Government Agency from the Perspective of Citizens in the DACH Region

Next, we have questioned the characteristics of a modern government agency from the perspective of citizens. This survey item has revealed insights on citizens' perceptions related to the national and cross-border usage of the OOP concept.

Table 1. Characteristics of a Modern Government Agency from the Perspective of Citizens in the DACH Region (based on [3])

	DE	AT	CH
	1,000	1,003	1,013
Quick response to requests (within 1-3 days)	67%	77%	74%
Online appointment allocation and no waiting time at public authority	63%	67%	62%
Availability of a central portal for citizens	47%	56%	47%
Availability of online information about the processing status of the application	46%	59%	50%
Continuous processing online	45%	58%	51%
Government request my personal data only once, which can be reused by other national authorities in compliance with data protection regulations	32%	46%	42%
Government requests my personal data only once, which can be reused by other European authorities in compliance with data protection regulations	14%	19%	14%

As Table 1 indicates, the top two characteristics are the same for all three countries. A modern public authority should provide quick response to requests (within 1-3 days). Allocation of online appointments with no waiting time at public authority is the second

characteristic of modernity. Not surprisingly, these two characteristics are directly related to time savings, as traditional public authorities are widely accepted as being slow, inefficient and highly bureaucratic [25].

It is interesting to note that, the majority of the survey respondents did not consider the OOP as a characteristic of modern public authority. This perception was especially lower for German citizens compared to Austrian and Swiss ones. Exchange of personal data with other European authorities have encountered considerably much higher skepticism in all countries of analysis, although the compliance with data protection regulations was explicitly stated.

The discrepancy between perceptions toward personal data exchange between the national and EU-wide public authorities is striking. Although about one in every three citizens in Germany and one in every two citizens in Austria would consider exchange of personal data between national public authorities as a characteristic of modernity, more than four in every five individuals in all three countries have not seen any relation between modernity and exchange of their personal data at EU level.

The high sensibility of individuals regarding their personal data has also been subject to other studies in literature. Especially, the German nation is known to be highly sensitive towards initiatives, which involve storing or transferring of personal data. Various initiatives in the past involving storage or transfer of sensitive personal data such as the Electronic Health Card Project have failed due to privacy concerns of citizens despite large amount of investments [26]. Such projects were heavily contested in the past by citizens, non-governmental organizations and political parties due to direct infringement to personal privacy [27]. This elevated sensitivity has a direct influence on adoption of such projects as well [28]. For instance, although one in every two German citizens (49%) has the new residency cards, less than one in every three of them (15%) decided to activate the eID function, which is the essential component for using the services online [3]. Therefore, even if some concepts such as the OOP are to be introduced at EU-level, their implementation strategy needs to be in each country separately because nations tend to have different levels of sensitivities. Such assessment should take the experience gained from similar projects in the past in consideration as well as a careful assessment of the sensitivities of the citizens which can be partially assessed by utilizing nationwide surveys and focus group analyses.

3.3 Opinions of Citizens Regarding Share of Their Personal Addresses in the DACH Region

The third question focused on understanding perceptions towards the implementation of the OOP concept in cross-border settings. In order to concretize the question, it was asked on the specific example of ‘sharing their personal address with the public authorities of other EU Member States’.

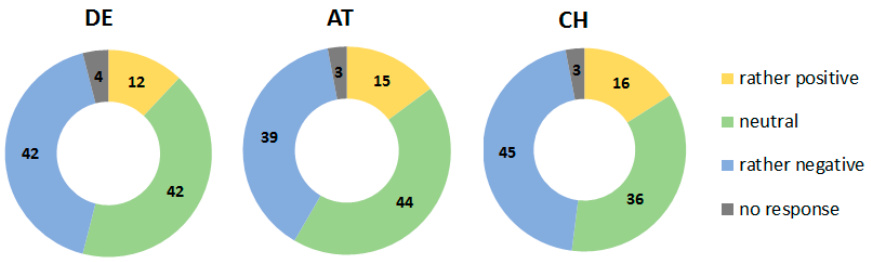

Fig. 2. Personal Opinions of Citizens in the DACH Region towards sharing of their personal address with the public authorities of other EU Member States (in percentages, based on [3])

Similar to the previous question, this analysis has confirmed the reservation of respondents towards implementation of the OOP concept in cross-border settings. Only 12 percent of German respondents, 15 percent of Austrian respondents and 16 percent of Swiss respondents have perceived this approach as "rather positive". The percentages of "rather negative" responses were, in contrast, about two to three times much higher.

Overall, our research has confirmed the importance of data protection and privacy concerns within the G2C e-government context. Furthermore, we have clearly observed that the survey respondents were clearly much more reserved towards sharing data with the governments of other EU Member States compared to data exchange between public authorities of their own country.

These results are in line with the findings of the recent TOOP survey, which revealed the perspective of businesses. Companies participating in the TOOP survey were significantly less willing to share data with authorities of other EU Member states compared to authorities in their own country [29]. Furthermore, data protection requirements were found as *the top challenge* for the pilot implementation of the TOOP project [29].

4 Discussion

Despite various national and EU-wide investments, G2C e-government adoption in the DACH region has reached a stagnation point. The OOP is one of the main concepts introduced by the European Commission to support modernization efforts within the EU. Citizens should deliver particular standard information to governments only-once and public authorities are allowed to exchange data among each other under consideration of the data protection regulations.

Yet, as being one of the initial studies reflecting the citizen perspective towards the implementation of the OOP, our research has shown that citizens of the DACH region are quite skeptical about it. Not even one every five respondents in the DACH region

regarded exchange of their personal address with EU Member States as 'rather positive'. There is no doubt that this principle has a great potential of simplifying government processes, speeding up applications and related paperwork. This convenience comes, however, on the cost of data protection and privacy. Indeed, exchange of data between all EU Member States would increase the vulnerability of data enormously. Special caution is required as potential data breaches in the G2C e-government context is likely to have enormous consequences. For instance, citizens can update their credit card numbers in case of credit card fraud but sensitive personal data of individuals – such as the place of birth, data of birth or fingerprints – cannot be replaced [28].

Even though the data protection will probably to be ensured via EU-wide regulations similar to the EU GDPR for companies [19], not every country has the most advanced security infrastructure in place. Even if they do, no country – including the ones enjoying highest e-government rankings – could be completely immune to data breaches and cyber-attacks. For instance, Estonia had to recently block all e-ID cards due to a massive security flaw, which could have irreversible consequences including identity theft [30].

Second, sharing data is not necessarily the interest of every citizen. Not every citizen plan to study, work or move to another EU Member State in the foreseeable future. Thus, for such citizens, exchange of personal information with other EU Nations would only increase the vulnerability of their information and cause higher data protection and privacy concerns without any additional advantages. On the other hand, citizens go through various life events in their own country – such as getting married or applying for pension benefits – during which citizens have to interact with various national public agencies. This could explain the less skeptical perception of survey respondents towards exchange of information between national authorities as this could simplify the application as well as speed up the processing of it for citizens. The high number of countries of the EU can be another reason of resistance towards EU wide data exchange.

Until now, there has not been much research in literature regarding the perceptions of citizens towards the EU wide implementation of the OOP concept. The findings of our study have confirmed that sharing personal data with public authorities is not necessarily seen as an aspect of modernity. In particular, citizens were relatively skeptical in case of cross-border data exchange. Furthermore, survey respondents would likely to have perceived the concept with even higher resistance, if the scope of exchange was not limited to their personal address. Yet, considering the amount of investments made by the EU, we assume that the scope of data exchange will go over exchange of personal address to gain considerable benefits.

Despite importance of this issue, there has not yet been much research in literature on reflecting the citizen perspective and their perceptions on these issues. As the implementation has not started in most of the EU Member States, results of future empirical research can provide some valuable insights towards planning of implementations. As we have only considered the countries of the DACH region, results may not be generalizable to the remaining EU Member States. Therefore, we suggest future research to conduct further empirical studies to analyze the perceptions of citizens in other EU Member States.

To sum up, EC initiatives such as the OOP are quite promising; however, they should be planned and executed with utmost care. Each nation would likely have different levels of sensitivity, which needs to be taken into consideration. In particular, benefits added by increased convenience provided by data sharing should be carefully analyzed against the increased risks of data protection and its potential implications. The rising cyber criminality, massive data protection flaws and the overall vulnerabilities in online systems are frequently discussed in various media. E-government is unfortunately no exception. The European Commission and the EU Member States should explicitly state which personal data would be exchanged, under which circumstances as well as the rights of citizens such as the necessity of consent and its withdrawal at any time. After all, reaching the annual net savings of as much as 5 billion per year would only be possible, if its implementation is planned and conducted with the utmost care.

References

1. Gefen, D., Karahanna, E. and Straub, D. W.: Trust and TAM in online shopping: An integrated model. MIS Quarterly, 27, 1, 51-90 (2003).
2. Beldad, A., De Jong, M. and Steehouder, M.: How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. Computers in Human Behavior, 26, 5, 857-869 (2010).
3. Krcmar, H., Akkaya, C., Müller, L.-S., Dietrich, S., Boberach, M. and Exel, S.: eGovernment MONITOR 2017: Nutzung und Akzeptanz digitaler Verwaltungsangebote - Deutschland, Österreich und Schweiz im Vergleich Initiative D21, fortiss GmbH (2017).
4. Krcmar, H., Dapp, M., Zepic, R., Müller, L.-S., Dietrich, S., Boberach, M. and Moy, T. eGovernment MONITOR 2016 Nutzung und Akzeptanz digitaler Verwaltungsangebote - Deutschland, Österreich und Schweiz im Vergleich, Initiative D21 e.V., Institute for Public Information Management (ipima) (2016).
5. European Commission. EU eGovernment Action Plan 2016-2020 (2016).
6. European Commission: Tallinn Declaration on eGovernment (2017).
7. Deutscher Landkreistag: The New German Coalition Agreement (2018).
8. Wimmer, M. A., Tambouris, E., Krimmer, R., Gil-Garcia, J. R. and Chatfield, A. T. Once Only Principle: Benefits, Barriers and Next Steps. In Proceedings of the 18th Annual International Conference on Digital Government Research Staten Island, NY, USA. ACM (2017).
9. Krimmer, R., Kalvet, T., Toots, M., Cepilovs, A. and Tambouris, E.: Exploring and Demonstrating the Once-Only Principle: A European Perspective. ACM (2017).
10. Buyle, R., De Vocht, L., Van Compernolle, M., De Paepe, D., Verborgh, R., Vanlishout, Z., De Vidts, B., Mechant, P. and Mannens, E.: Oslo: open standards for linked organizations. ACM (2016).
11. Veiga, L., Janowski, T. and Barbosa, L. S.: Digital government and administrative burden reduction. ACM (2016).
12. Kalvet, T., Toots, M. and Krimmer, R. Contributing to a Digital Single Market for Europe: Barriers and Drivers of an EU-wide Once-Only Principle. In Proceedings of the 19th Annual International Conference on Digital Government Research Delft, Netherlands. ACM (2018).

13. Tikhomirova, A.: Reinforcing Trust and Security in Digital Services and in the Handling of Personal Data. InterEU law east: journal for the international and european law, economics and market integrations, 3, 1, 145-153 (2016).
14. Krimmer, R., Kalvet, T., Toots, M. and Cepilovs, A.: The Once-Only Principle Project: Position Paper on Definition of OOP and Situation in Europe (updated version) (2017).
15. European Commission. A Digital Single Market Strategy for Europe (2015).
16. Cave, J., Botterman, M., Cavallini, S. and Volpe, M.: SMART 2015/0062: EU-wide digital Once-Only Principle for citizens and businesses (2017).
17. Krimmer, R.: TTOP Webpage http://www.toop.eu/ (2017), last accessed 2018/02/01.
18. SCOOP4C Webpage: Austrian federal government commits to implementing once-only principle in new e-government plan https://www.scoop4c.eu/news/austrian-federal-government-commits-implementing-once-only-principle-new-e-government-plan, last accessed 2018/02/20.
19. European Commission: General Data Protection Regulation (GDPR) Portal https://www.eugdpr.org/ (2017), last accessed 2018/06/15.
20. Nordic Institute for Interoperability Solutions (NIIS): Digital society solutions and cross-border cooperation https://www.niis.org, last accessed 2018/05/15.
21. Krcmar, H., Wolf, P., Rau, L. and Till-Stavrakakis, V. eGovernment MONITOR 2014 Nutzung und Akzeptanz von elektronischen Bürgerdiensten im internationalen Vergleich, Initiative D21 e.V., Institute for Public Information Management (ipima) (2014).
22. Krcmar, H., Wolf, P., Zepic, R., Müller, L.-S., Till-Stavrakakis, V. and Boberach, M. eGovernment MONITOR 2015 Nutzung und Akzeptanz von elektronischen Bürgerdiensten im internationalen Vergleich, Initiative D21 e.V., Institute for Public Information Management (ipima) (2015).
23. European Commission: The Digital Economy and Society Index (DESI) https://ec.europa.eu/digital-single-market/en/desi, last accessed 2018/06/10.
24. Capgemini. eGovernment Benchmark (2017).
25. Lotze, B.: KVR: Lange Schlangen und kein Ende, Süddeutsche Zeitung, http://www.sueddeutsche.de/muenchen/behoerden-kvr-lange-warteschlangen-und-kein-ende-1.3993214 (2018), last accessed 16.06.2018.
26.Elektronische Gesunheitskarte offenbar vor dem Aus http://www.sueddeutsche.de/wirtschaft/e-card-elektronische-gesundheitskarte-offenbar-vor-dem-aus-1.3617842 (2017).
27. Akkaya, C., Wolf, P. and Krcmar, H. Factors influencing citizen adoption of e-Government services: A cross-cultural comparison (Research in progress). In Proceedings of the 45th Hawaii International Conference on System Science Hawaii, USA. IEEE (2012).
28. Akkaya, C.: A Comprehensive Analysis on Citizen Adoption of E-Government Services: A Cross-Cultural Analysis. Technical University of Munich (2016).
29. Kalvet, T., Toots, M. and Krimmer, R.: The Once-Only Principle Project: Drivers and Barriers for OOP (1st Version) (2017).
30. Moon, M.: Estonia freezes residen ID cards due to security flaw https://www.engadget.com/2017/11/04/estonia-freezes-resident-id-cards-security-flaw/ (2017), last accessed 01.06.2018.