Citizen Empowerment on the Basis of the new Freedom of Information Act in Austria - Make Information Freedom Great Again

Karl Pinter
Vienna University of Technology
Industrial Software (INSO)
Vienna, Austria
karl.pinter@inso.tuwien.ac.at

Dominik Schmelz
Vienna University of Technology
Industrial Software (INSO)
Vienna, Austria
dominik.schmelz@inso.tuwien.ac.at

Peter Ebenhoch
Vienna University of Technology
Industrial Software (INSO)
Vienna, Austria
peter.ebenhoch@inso.tuwien.ac.at

Thomas Grechenig
Vienna University of Technology
Industrial Software (INSO)
Vienna, Austria
thomas.grechenig@inso.tuwien.ac.at

Abstract

Austria is the only country in Europe that has official secrecy, so-called "Amtsgeheimnis", as a constitutional principle. In contrast to other countries, this has consequences for citizens in their dealings with the authorities. Information is therefore not free per se but is only released under certain conditions. These are severely restricted. This leads to a number of problems, for example, Austria is already among the worst 10 countries in terms of freedom of information. A new Freedom of Information Act is intended to change this. In this paper, the authors present a prototype that enables query processing between citizens and government agencies. Cloud services are used, and the data does not leave the respective data sovereignty. The draft law is currently under review.

1. Background and Related Work

Official secrecy ("Amtsgeheimnis") has constitutional status in Austria and is protected by law. There are historical reasons for this, among others. Going back far enough in history, it becomes clear that the Habsburgs needed professionals for the administration. These professionals were traditional to be found in the bourgeoisie [1, p. 125]. Against this background, relevant regulations and specifications were created that are still effective today.

1.1. Bureaucracy in Historical Context

Max Weber coined the term "iron cage" as a methaphor for a bureaucratized world [2, p. 38]. Official secrecy is a specific invention of bureaucracy to protect its own operation [3, chapter 3].

According to Weber, the basis for rational and legal rule is the ideal type [4, p. 473] of a bureaucracy [4, p. 334ff].

Weber [4, p. 344f] defines an authority is a continuous, rule-based operation of official business. Therefore, there are clear responsibilities, the services are delimited from each other. Responsibilities are defined. There is a hierarchy with authority to issue directives. The application and delimitation of coercive means is defined.

There are control and supervisory authorities, and there is also a right of appeal or complaint. Within the administration, work is done strictly according to rules. In any case, specialists are needed [4, p. 345f].

Civil servants receive remuneration in the form of a salary or benefits in kind. [4, p. 345]. There is no appropriation of position to an incumbent. The actions of the administration are recorded in writing. A legal rule can take very different forms, one of which is officialdom [4, p. 346].

Becker, Boeckh, Hainz, *et al.* [5] compared people living in former Habsburg territory, even though the national borders have since shifted. People within the borders of the Habsburg Empire have more trust in the judiciary and executive. This seems to stem from the fact that the bureaucracy in the Habsburg Empire was less prone to corruption and functioned as it did.

In summary, bureaucracy [6, p. 99] can be seen in a positive sense [4, p. 335ff]:

1. Predictability in a defined hierarchy
2. Performance and qualification in focus

URI: https://hdl.handle.net/10125/79662
978-0-9981331-5-7

3. Maximizing efficiency

4. General applicability

1.2. Civil Service Law and Administrative Action

In the "Hirtenbrief" 1783 of the emperor Joseph II [7] is already mentioned, how a civil servant has to behave. After the events of the "Vormärz", the 1848 March Revolution, the civil servant wage system and salaries were introduced in 1873 [8]. The "Service pragmatics" [9] introduced in 1914 was valid until 1979. The "Civil Servants Act" [10] and "Civil Service Employees Act" [11] has been in effect since 1979. Civil servants are appointed by "official notice" or "administrative decision", they are subject to a specific disciplinary law.

Since administration exists, it works in 3 stages or phases [12, p. 261]. It comes to the incoming mail (mailroom), then to the processing and at the end is the completion. In the "processing" step, modern administrations work with electronic file systems. Paper files are gradually replaced by electronic ones.

While the administration works in the said 3 phases, the model of 4 stages of digital government was proposed by Janowski [13, p. 226]. Put simply, stage 1 (Digitization or Technology in Government) digitizes analog artifacts. There is no redesign or improvement of existing processes [13, p. 226]. In stage 2 (Transformation or Electronic Government), the existing processes will be improved. So that they also facilitate interaction between authorities and organizations [13, p. 226]. In stage 3 (Engagement or Electronic Governance), the forms of interaction and processes are transformed. New possibilities arise - instead of the analog forms, "digital by default" is used [13, p. 226]. In stage 4 (Contextualization Stage), concrete plans and goals are pursued [13, p. 226]. The present prototype as presented in 3 is intended to enable citizens to strive towards level 4. In this context, the literature often talks about providing transparent opportunities for citizens to engage in decision-making processes to promote participation and understanding [14].

1.3. eGovermment Pillars

In 2016, the EU eGovernment Action Plan [15] set out how to promote digitization within the European Union. One vision was that public administration in the area of E-Government (E-Gov) should be guided and developed following defined pillars.

- "Digital by Default": Public administration should provide services primarily digitally and also communicate digitally with citizens.
- "Once only principle": All data should be collected only once by an authority, if possible, and then made available to others. This is to avoid multiple storages. The efficiency concerning communication with the citizen is also increased because there are no empty runs or redundant communication channels.
- "Inclusiveness and accessibility": As many citizens as possible should be able to use the services offered digitally.
- "Openness and transparency": There should be an exchange of data between the authorities. It should also be possible to act transparently in the direction of the citizen in order to give the citizen self-determination with regard to information.
- "Cross-border by default:": Certain data will be made available across borders to strengthen the inner-EU market.
- "Interoperability by default": A free exchange of data throughout the internal market should ideally be possible, including the exchange of public service data.
- "Trustworthiness and Security": Trust and security strengthen confidence in the authorities.

The solution presented by the authors is based on virtually all the cornerstones of the plan. Primarily, however, on "Openness and transparency".

1.4. Problem

Generally can be said: the state administration may only do what is provided for in the law [16, Art. 18 (1)]. On the other hand, private companies are allowed to do anything that is not prohibited by law.

The approach can be seen worldwide, which is striving massively in the direction of Open Government Data (OGD) [17] and freedom of information. In Austria, this maxim does not yet apply. Official secrecy prevents freedom of information by definition. The penal code clearly regulates the sanctions [18, §310]. Among 128 countries rated based on freedom of information, Austria is currently in the bottom 10 [19]. This is contrasted with the law on the obligation to provide information (Auskunftspflichtgesetz) [20].

A problem discussed in science is the absence of a universally accepted theoretical framework for

E-Gov [21]. This creates a broad scope for action in the implementation of laws.

The work is also in the context of the General Data Protection Regulation (GDPR) of the European Union, which creates the basis for the storage and processing of personal data. Not least, for this reason, a system of federated cloud was chosen to prevent data protection violations from occurring. The aim is to make it easier for citizens to exercise their rights by providing them with a system that takes the necessary steps away from bureaucratic offices.

We hope to stimulate discussion and encourage research so that the bureaucracy works for the citizen, in the sense of Max Weber, as discussed in section 1.1.

1.5. Related Work

Works by Max Weber are fundamental [2]. New Public Management (NPM) [22] emerged from these considerations [23] by Weber. NPM attempts to transfer methods used in the private sector to the public sector, thus also enabling quantification of work [24, p. 1].

Meyer [25, p. 63] defines Good Governance (GG) as "The principles of a prosperous state are summarized under the term 'good governance'." Reif [26] examined the role of the ombudsman in the context of human rights and GG. Hodijah [27] researched architectures based on the The Open Group Architecture Framework (TOGAF) model in terms of GG. Perdana [28, p. 1572] illustrated the importance of transparency and freedom of information to move toward GG.

Neamtu and Dragos [29, p. 11ff] examined the situation at the European level.

Zefferer, Ziegler, and Reiter [30, p. 11ff] investigated the topic of authentication in Federation as a Service (FaaS) solutions based on the SecUre iNFormatIon SHaring in federated heterogeneous private clouds (SUNFISH) Project [31], which attempted to federate the authority clouds without a specific look at data sharing with citizens in terms of freedom of information. This paper is distinct from a Federated Identity Architecture (FIA) as described by Carretero, Izquierdo-Moreno, Vasile-Cabezas, *et al.* [32], because this paper is aimed at a prototype with a strong national reference, without any focus on a vendor or existing solution.

Paulin [33] researched Beyond Bureaucracy (BB) systems. BB is defined as "... search for a novel paradigm for governance of juropolitical systems, where Information and Communications Technology (ICT) would eliminate the need for intermediary (human) agents in administering a society's common wealth ..." [33]. The presented approach in this paper can be understood as a preliminary stage for a BB system. Due to the multitude of possible expert systems and especially the always contextual linguistic subtleties, this is not possible at the moment. Further research needs to be done here on how to provide the most automated information possible without human intervention.

2. Case Description

2.1. Austria's Current Information Landscape

Based on the law on the obligation to provide information [20], citizens can make requests to an authority within the state of Austria. The latter answer them accordingly or rejects them. In doing so, it must always be weighed up which interests prevail. There are platforms through which inquiries can be made in Austria [34] and within the European Union (EU) [35] or United Kingdom (UK) [36].

Numerous problems immediately arise here, which were identified by the authors. There is no standardized form of how the requests are to be made. There are media breaks like printing of forms, filling out, signing, scanning, e-mailing, etc. Furthermore, there is no documentation of the inquiries and answers that is secure for the citizens. The contact data of the authorities must be obtained by the inquirer himself. As a result, citizens have to find their way around the organization of the administration.

If we compare the situation in Austria with other EU countries, we find that the principle of freedom of information already applies in all other states [37]. This has been recognized and debated by politicians for a long time [38].

2.2. Tromsø Convention

The Tromsø Convention ensures access to official documents held by public authorities. It is considered the first binding international legal instrument [39]. Transparency and trust in public authorities should be ensured.

The approach presented by the authors is intended to satisfy, among other things, the requirements of Article 2 "Each Party shall guarantee the right of everyone, without discrimination on any ground, to have access, on request, to official documents held by public authorities." [39, Art. 2].

The agreement does not regulate where the data is stored or how data exchange is to take place technically.

2.3. Draft Law Information Freedom

Currently, a draft law has been presented that aims to ensure freedom of information and thus abolish official secrecy [40]. A corresponding announcement is also reflected in the government agreement. This was largely rated well by citizens' rights organizations, although some passages were classified as "critical" [41].

The most important cornerstone of the planned law is a civil right to access state information. This also means that there must be access to state documents. Until now, requests and responses have been subject to fees, but in the future, they will be free of charge. The obligation to provide information is to be extended. Expert opinions, studies, and contracts must be published automatically under certain conditions. The current OGD platform is intended to serve as the central information registry.

The OGD directive [42] is the cornerstone for OGD data. Data is made available by the state in machine-readable form. Non OGD data continues to be protected by official secrecy. With the implementation of the envisaged Freedom of Information Act, the OGD platform will be placed as a central body. The dashboard presented by the authors could also be used to provide the number of cases and corresponding feedback directly as OGD data. The dashboard can therefore also serve as a benchmark as to whether the deadlines set out in the law are being exhausted or whether further measures need to be undertaken, like figure 4 shows.

The draft law does not include a commissioner [40] or ombudsman [26].

The currently planned response period is 4-8 weeks. Exceptions are foreseen, for example, for reasons of national security [40].

Administrative courts are to ensure enforcement. Here the authors intervene by means of the presented prototype. Enforcement of rights in court can only be meaningful if the evidence is as straightforward as possible. This applies to both sides. Authorities should also be able to easily prove that a request has been complied with in due time [40].

In the case of disputes, therefore, the effort for courts, citizens, and also for authorities should be minimized.

After the end of the review period, it becomes clear that many comments refer to the Freedom of Information Officer. Furthermore, the term information and also the deadlines are criticized [43].

The Data Protection Authority (DPA) shall advise public authorities regarding the Freedom of Information Act and ensure proper data protection.

The authors reflect on whether the use of forms could be a form of exercising power. The applicant who wishes to exercise his or her right to freedom of information would have to submit to the structure and form of the authority [44], [45]. The idea is, therefore, to develop a prototype that gives all sides the necessary design freedom to exchange data in a secure manner.

3. Implementation

In a first step, the authors compared the existing law with the draft law [40]. The current state in citizen requests is a rather simple, but unstructured process (see Figure 1). A citizen requests information (2) from a public authority (3) using an ID Service (1). Different forms of communication can be used. There is no logging from a third independent authority. The authority answers the citizen directly (4).

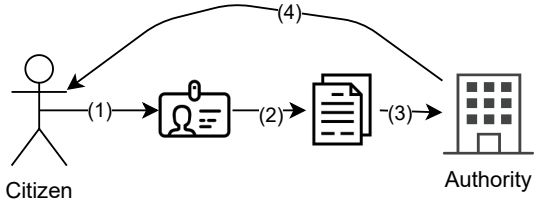

Figure 1. Simplified current process

Subsequently, in the prototype process, the differences and requirements for a prototype were worked out by also examining third party comments, as outlined in section 2.3.

Even though, many governments implement platforms with additional functionality in place the process lacks transparency and privacy for the citizen and third parties.

Therefore the process was improved by the authors and implemented in a prototype. Research has been conducted to scientifically solve the problems stated in section 1.4 while keeping the following objectives in mind:

- Transparency of processing
- Shared data ownership
- Privacy by design and default

A minimum list of requirements for a new system has been developed and is directly reflected in the implementation. The implemented Freedom of Information Act Austria (FIAA) Platform shows how data transparency requests can be performed by citizens with built-in traceability and transparency, while respecting data privacy. The general architecture is a federated private cloud architecture. The citizen

enters and stores its data in its private cloud and mirrors the data to the private cloud of the receiving party. The present paper does not aim at a concrete technical platform with regard to FIA; each authority should be able to use the respective suitable solution. Rather, it aims at transparent data exchange and the breaking of official secrecy.

Creating the prototype, the following design goals were derived from the aforementioned considerations:

- Easy ways for users to fill in their case.
- Ensuring the Web Accessibility Initiative (WAI) criteria.
- System is designed to support citizens and officials alike.
- The data must not leave the company's own sphere of control at any stage.
- Use of blockchain as stamping service.

As described in section 1.2, there are three phases in every administration. From a higher-level perspective, the process of a transparency request is defined as followed: a citizen submits a request under the Freedom of Information Act. The request is then sent to the mailroom (phase 1). After an initial legal review, the request is assigned to the relevant department, which also responds (phase 2). Before the answer is returned to the citizen, another check is made, and then the answer is given (phase 3).

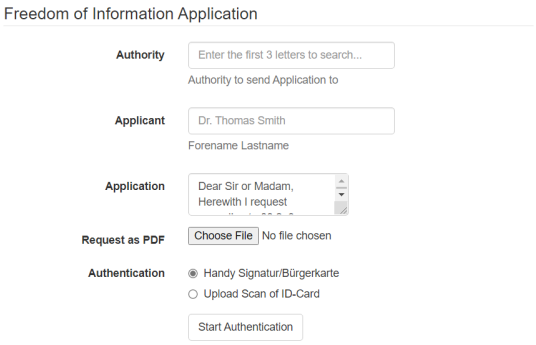

Figure 2. Freedom of information application form

Figure 2 shows the input screen from the perspective of a citizen of the prototype. The authority to which the arrival request is made can be specified as well as the request itself. The identification is done via electronic IDentification, Authentication and trust Services (eIDAS).

The receiving party, usually a government agency, receives the request and stores the data back in its private cloud, and sends a link to the requested private cloud system, which can mirror the data. Both parties can delete the data once the processing is complete. Using blockchain technology, both can also prove that the data has not been tampered with on either side. In addition, the requesting citizen can prove their request by providing the receiving party with proof of existence with a timestamp and hash. The data itself is not stored on the blockchain, nor is it distributed on the blockchain network. Only a hash, including a timestamp, is stored in a transaction on the blockchain.

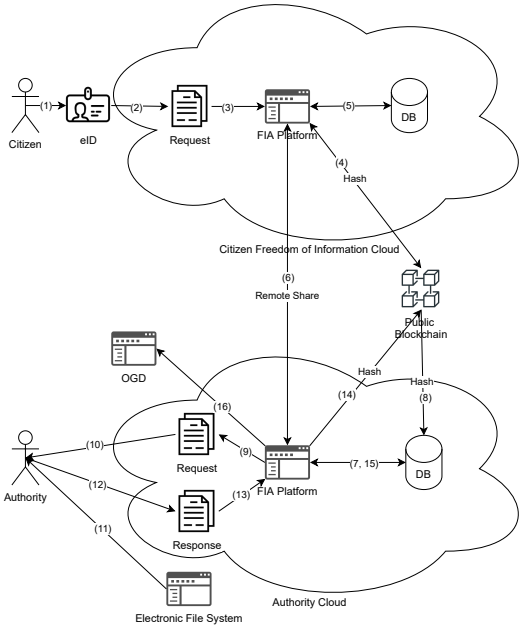

Figure 3. Architecture of the prototype

The general workflow can be described as followed, as shown in figure 3:

A citizen logs into the system (1), identifying himself by means of eIDAS. The citizen uploads his application, which is automatically digitally signed with his eIDAS identity (2). He or she is not bound to any particular form, as is already the case. However, the system does provide assistance. The citizen can select the addressee, i.e. the recipient authority, from a selection list (3). It is not necessary to know the specific address (either electronic or postal) to be able to make a request. Identification by means of eIDAS also eliminates the need for any queries regarding identity verification. A hash value of the request including the time is stored on a public blockchain (4) by the use

of a stamping service[1]. This means that the time and content of the request can be clearly traced and that the request cannot be manipulated on the way. The request (5) is stored in the private cloud of the citizen and forwarded to the public authority cloud (6) via remote share. The request is transmitted to the platform, which is located in the authority cloud (7). The authority checks the integrity of the request against the blockchain (8). The request is now visible to an authority employee (9) and can be processed. In the process, the request is assigned to the responsible caseworker (10). The request is processed (11). This happens in a specialised external system of the respective authority. The response from the authority (12) is transferred to the system (13) and digitally signed. A hash of the response is again persisted on the blockchain (14). The answer of the authority is stored in the authority cloud (15) and can be accessed by the citizen from his private cloud (6). Publication on the national OGD platform is envisaged by means of an interface, as in the present draft law (16) [40].

Besides data protection, usability was an important consideration of the prototype. Figure 4 shows the admin dashboard. It can be viewed by the respective Head of Service or Head of Authority. It is readily conceivable that this will be made available as an OGD dataset. The dashboard provides a quick overview of the workload to date and serves primarily as an information display. The individual inquiries are processed by the respective employee in charge.

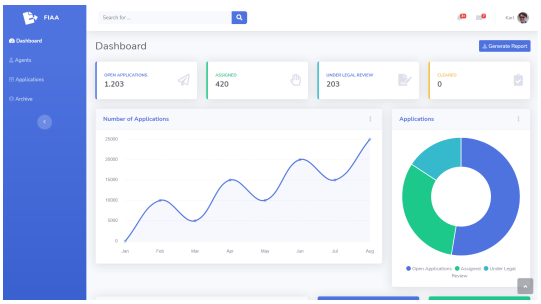

Figure 4. FIAA Dashboard

The prototype has been implemented to showcase the feasibility of a data protected and traceable freedom of information application. The frontend, as the backend has been developed in a common webframework (see Figure 5). The prototype uses the eIDAS implementation of A-Trust mobile signature and the opentimestamps[1] notary service. The underlying blockchain is the public Bitcoin blockchain.

[1] opentimestamps.org

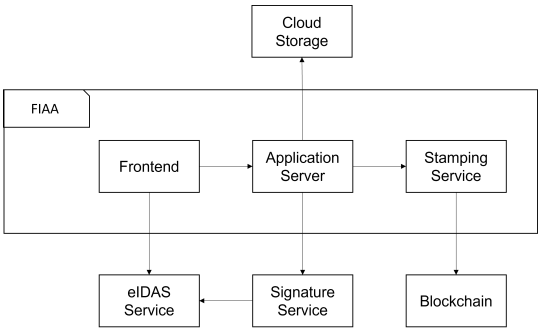

Figure 5. FIAA Architecture Overview

3.1. Architecture Roles

The relevant roles in the prototype are:

- Citizen: Any citizen who can obtain information from the authority according to the laws.
- Authority: A legally regulated entity appointed to perform certain public functions.

The roles are kept short for clarity. The role of an ombudsman is not envisaged in the current draft law and is therefore excluded as a role. The role of internal supervision has been intentionally omitted. The role of the data protection authority as an advisor is likewise excluded.

3.2. Blockchain

Blockchain technology can make a valuable contribution in areas such as payment, security, and logistics [46]. It provides a transparent, immutable, decentralized database used by multiple parties. The blockchain is used to document requests and responses in a forgery-proof manner for the purpose of transparency and reducing bureaucracy. If the parties involved share a mutual distrust, the use of this technology makes sense. Both partners can be confident that the information in the stored form is also correct respective not tampered with. In the case of the presented prototype, the added value results from the fact that each party (citizen and authority) can trace the communication in a secured manner. The blockchain is solely used as a “document stamping” system. Therefore no transaction data or personal data is stored on the blockchain.

3.3. eID Person Identification

The electronic ID (eID) is an electronic procedure to uniquely identify persons [47]. It ensures that this is also possible across borders within the EU. The eIDAS [48]

Regulation ensures that the entire EU area is subject to the same legal framework. Paper transactions are to be given the same legal status as electronic transactions.

The prototype developed by the authors provides for registration with the eID. For citizens who do not have an eID, a document upload is possible.

Since the "once-only" principle of E-Gov [49] is to be upheld, we propose to ensure universal access and provide a eID solution as the primary, but not the sole, identity provider.

The prototype was implemented by integrating the freely available Module for Online Application (MOA) modules [50].

3.4. Federated Servers

Federated cloud servers share resources, with users needing to authenticate only once. Sharing also works across products. This means that the stakeholders do not have to agree on a specific product.

Interoperability is required by the EU Government Action Plan [15] as discussed in section 1.3 and is one of the cornerstones of the present prototype. This is because interoperability is an important pillar for Open Cloud Mesh services [51, p. 1053]. For this purpose, Gracia-Tinedo, Cotes, Zamora-Gómez, *et al.* [52] developed a protocol that ensures that the different platforms can exchange data. Gracia-Tinedo, Cotes, Zamora-Gómez, *et al.* [52, p. 3] also point out that it is the currently prevalent vendor lock-in that poses a problem for real-world applications. The authors of this paper used a prototype to show that the problem can be tackled.

3.5. Government Cloud Services

Governments started building their own cloud services and applications years ago [53] [54]. This paper delineates that each agency or subordinate department could use its own services, such as electronic file services. Thereby, the presented system represents a specialized information system. The storage of data continues to take place in the respective electronic file system of the respective authority. Each state can therefore choose a variety of different providers and vendors. At the same time, this ensures that a changeover can proceed sequentially. This also ensures investment protection.

4. Conclusion and Implications

The prototype presented by the authors enables citizens to make secure and traceable requests to public authorities, especially regarding the Freedom of Information Act. In doing so, the platform follows all relevant guidelines [15].

From the citizen's perspective, this creates a useful and data-saving way to create and manage requests.

From the point of view of the authority, it is ensured at all times who is making the inquiry. At the same time, the data never leaves the public authority system. The electronic file management system used is entirely transparent [55].

The exchange among the authorities is possible via Elak-Trans [56]. This also means that information could be carried out across authorities in electronic form.

Neither the Tromsø Convention [39] nor the draft law on the Freedom of Information Act specifies how data exchange is to take place technically [40]. The authors are strongly concerned with the issue of how to provide citizens with a simple and secure method of sharing information under the Freedom of Information Act. The prototype presented here provides clarity.

Secure and documented data exchange has always been a challenge. Currently, government to citizen communication is handled by means of numerous channels - digital and analog. Among other things, these run via unencrypted paths, often also via numerous hops in other countries, and are therefore also subject to different legal systems.

It is worth mentioning once again that this is a country that continues to stand out from all other EU states due to its traditional official secrecy. Therefore, it is still not possible to reproduce the systems and procedures of other countries 1:1. The authors show that it is possible to transfer data in a way that is compliant with the GDPR in the context described above, and that this can increase convenience for both sides. The platform presented by the authors represents a step towards secure authority communication. The requirements of the Freedom of Information Act are met. This allows freedom of information to be satisfied while maintaining a high level of data protection.

References

[1] P. S. F. (auth.), *The Habsburg Monarchy, 1490–1848: Attributes of Empire*, ser. European History in Perspective. Macmillan Education UK, 2003, ISBN: 978-0-333-73728-6.

[2] L. A. Scaff, "Max Weber," in *Key Sociological Thinkers*. London: Macmillan Education UK, 1998, pp. 34–45, ISBN: 978-1-349-26616-6. DOI: 10.1007/978-1-349-26616-6_3.

[3] D. Graeber, *The utopia of rules : on technology, stupidity, and the secret joys of bureaucracy*. Brooklyn: Melville House, 2015, ISBN: 1612193749.

[4] M. Weber, *Economy and Society*, trans. by K. Tribe. Harvard University Press, 2019.

[5] S. O. Becker, K. Boeckh, C. Hainz, and L. Woessmann, "The empire is dead, long live the empire! long-run persistence of trust and corruption in the bureaucracy," *The Economic Journal*, vol. 126, no. 590, pp. 40–74, Jul. 2015. DOI: 10.1111/ecoj.12220.

[6] M. Bayer and G. Mordt, *Einführung in das Werk Max Webers* -. Berlin Heidelberg New York: Springer-Verlag, 2008, ISBN: 978-3-531-15392-6.

[7] *Hirtenbrief*. [Online]. Available: https://www.jku.at/fileadmin/gruppen/142/Erinnerung_an_seine_Staatsbeamten.pdf.

[8] *Wien Geschichte*. [Online]. Available: https://www.geschichtewiki.wien.gv.at/Beamte (visited on 07/12/2021).

[9] *Gesetz, betreffend das Dienstverhältnis der Staatsbeamten und der Staatsdienerschaft (Dienstpragmatik)*. [Online]. Available: https://alex.onb.ac.at/cgi-content/alex?aid=rgb&datum=19140004&seite=00000087.

[10] *Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Beamten-Dienstrechtsgesetz 1979, Fassung vom 11.03.2021*. [Online]. Available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10008470.

[11] *Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Vertragsbedienstetengesetz 1948, Fassung vom 11.03.2021*. [Online]. Available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10008115.

[12] C. S. Calude, G. Rozenberg, and A. Salomaa, Eds., *Rainbow of Computer Science*. Springer Berlin Heidelberg, 2011. DOI: 10.1007/978-3-642-19391-0.

[13] T. Janowski, "Digital government evolution: From transformation to contextualization," *Government Information Quarterly*, vol. 32, no. 3, pp. 221–236, 2015, ISSN: 0740-624X. DOI: 10.1016/j.giq.2015.07.001.

[14] G. S. Craveiro, J. A. S. Machado, and J. S. Machado, "The use of open government data to citizen empowerment," in *Proceedings of the 9th International Conference on Theory and Practice of Electronic Governance*, ser. ICEGOV '15-16, Montevideo, Uruguay: Association for Computing Machinery, 2016, pp. 398–399, ISBN: 9781450336406. DOI: 10.1145/2910019.2910076.

[15] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *EU eGovernment Action Plan 2016-2020*, 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0179&from=EN.

[16] *Bundes-verfassungsgesetz (b-vg) i.d.f. vom 15.03.2019*, BGBl. I Nr. 14/2019, 2019.

[17] M. Kaltenböck, "Ogd2011 – requirements analysis for an open data strategy (in austria)," in *Environmental Software Systems. Frameworks of eEnvironment*, J. Hřebíček, G. Schimak, and R. Denzer, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 64–69, ISBN: 978-3-642-22285-6.

[18] *Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Strafgesetzbuch, Fassung vom 12.03.2021*. [Online]. Available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296.

[19] *Global Right to Information Rating Map*. [Online]. Available: https://www.rti-rating.org (visited on 03/02/2021).

[20] *Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Auskunftspflichtgesetz, Fassung vom 12.03.2021*. [Online]. Available: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000916.

[21] A. Paulin, "E-gov theory and the role of design science in transforming public governance," in *Proceedings of the 18th Annual International Conference on Digital Government Research*, ser. dg.o '17, Staten Island, NY, USA: ACM, 2017, pp. 541–545, ISBN: 978-1-4503-5317-5. DOI: 10.1145/3085228.3085300.

[22] P. J. Andrisani, S. Hakim, and E. S. Savas, Eds., *The New Public Management*. Springer US, 2002. DOI: 10.1007/978-1-4615-1109-0.

[23] A. Maurer, Ed., *Wirtschaftssoziologie nach Max Weber*. VS Verlag für Sozialwissenschaften, 2010. DOI: 10.1007/978-3-531-92524-0.

[24] A. Bruno, *New Public Management (NPM) and the Introduction of an Accrual Accounting System*. Springer International Publishing, 2021. DOI: 10.1007/978-3-030-57386-7.

[25] M. Meyer, "Good governance," in *Liberal Democracy: Prosperity through Freedom*. Cham: Springer International Publishing, 2020, pp. 63–67, ISBN: 978-3-030-47408-9. DOI: 10.1007/978-3-030-47408-9_11.

[26] L. C. Reif, *The Ombudsman, Good Governance and the International Human Rights System*. Springer Netherlands, 2004. DOI: 10.1007/978-94-017-5932-8.

[27] A. Hodijah, "Analysing enterprise architecture model for service based e-government towards good government governance," in *2017 International Conference on Information Technology Systems and Innovation (ICITSI)*, 2017, pp. 114–119. DOI: 10.1109/ICITSI.2017.8267928.

[28] A. Perdana, "Ict, knowledge society, and good governance: Relationship and interation pattern," in *2010 International Symposium on Information Technology*, vol. 3, 2010, pp. 1571–1575. DOI: 10.1109/ITSIM.2010.5561597.

[29] B. Neamtu and D. C. Dragos, "Freedom of information in the european union: Legal challenges and practices of EU institutions," in *The Laws of Transparency in Action*, Springer International Publishing, Jul. 2018, pp. 11–70. DOI: 10.1007/978-3-319-76460-3_2.

[30] T. Zefferer, D. Ziegler, and A. Reiter, "Best of two worlds: Secure cloud federations meet eidas," in *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2017, pp. 396–401. DOI: 10.23919/ICITST.2017.8356430.

[31] *Sunfish*. [Online]. Available: http://www.sunfishproject.eu/sunfish/the-project (visited on 01/15/2021).

[32] J. Carretero, G. Izquierdo-Moreno, M. Vasile-Cabezas, and J. Garcia-Blas, "Federated identity architecture of the european eid system," *IEEE Access*, vol. 6, pp. 75 302–75 326, 2018. DOI: 10.1109/ACCESS.2018.2882870.

[33] A. Paulin, "Beyond bureaucracy," in *Beyond Bureaucracy: Towards Sustainable Governance Informatisation*, A. A. Paulin, L. G. Anthopoulos, and C. G. Reddick, Eds. Cham: Springer International Publishing, 2017, pp. 15–26, ISBN: 978-3-319-54142-6. DOI: 10.1007/978-3-319-54142-6_2.

[34] *Forum Informationsfreiheit*. [Online]. Available: https://www.informationsfreiheit.at (visited on 02/24/2021).

[35] *Ask the EU*. [Online]. Available: https://www.asktheeu.org (visited on 02/25/2021).

[36] *What do they Know*. [Online]. Available: https://www.whatdotheyknow.com (visited on 02/25/2021).

[37] R. Feik, *Die Amtsverschwiegenheit*. [Online]. Available: http://www.konvent.gv.at/K/DE/AVORL-K/AVORL-K_00303/fnameorig_017343.html.

[38] *Warum sich die Verhandlungen zum Amtsgeheimnis so lange ziehen*. [Online]. Available: https://www.derstandard.at/story/2000123429365/warum-sich-die-verhandlungen-zum-amtsgeheimnis-so-lange-ziehen (visited on 04/11/2021).

[39] *Council of Europe Convention on Access to Official Documents, CETS No.205*. [Online]. Available: https://www.coe.int/en/web/access-to-official-documents/home (visited on 02/13/2021).

[40] *Bundes-Verfassungsgesetz, Rechnungshofgesetz, u.a., Änderung; Informationsfreiheitsgesetz (95/ME)*, Mar. 8, 2021. [Online]. Available: https://www.parlament.gv.at/PAKT/VHG/XXVII/ME/ME_00095/index.shtml.

[41] *Analyse des Regierungsprogramms 2020-2024*. [Online]. Available: https://epicenter.works/sites/default/files/regierungsubereinkommen_analyse.pdf (visited on 01/28/2021).

[42] *Directive (EU) 2019/1024 of 20 June 2019 on open data and the re-use of public sector information*. [Online]. Available: http://data.europa.eu/eli/dir/2019/1024/oj.

[43] *Stellungnahme Ministerialentwurf betreffend Bundesgesetz, mit dem das Bundes- Verfassungsgesetz, das Rechnungshofgesetz 1948 und das Verfassungsgerichtshof- gesetz 1953 geändert und ein Informationsfreiheitsgesetz erlassen werden*. [Online]. Available: https://epicenter.works/document/3240 (visited on 06/04/2021).

[44] "Informationsfreiheit by design," *Datenschutz und Datensicherheit - DuD*, vol. 43, no. 8, pp. 466–466, Aug. 2019, ISSN: 1862-2607. DOI: 10.1007/s11623-019-1144-0.

[45] F. Gantner, *Theorie der juristischen Formulare*. Duncker & Humblot, 2010.

[46] S. Underwood, "Blockchain beyond bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, Oct. 2016, ISSN: 0001-0782. DOI: 10.1145/2994581.

[47] *eID Services*. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile (visited on 02/02/2021).

[48] *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. [Online]. Available: http://data.europa.eu/eli/reg/2014/910/oj.

[49] C. Akkaya and H. Krcmar, "Towards the implementation of the eu-wide "once-only principle": Perceptions of citizens in the dach-region," in *Electronic Government*, P. Parycek, O. Glassey, M. Janssen, H. J. Scholl, E. Tambouris, E. Kalampokis, and S. Virkar, Eds., Cham: Springer International Publishing, 2018, pp. 155–166, ISBN: 978-3-319-98690-6.

[50] *Joinup*. [Online]. Available: https://joinup.ec.europa.eu (visited on 01/23/2021).

[51] J. T. Mościcki and L. Mascetti, "Cloud storage services for file synchronization and sharing in science, education and research," *Future Generation Computer Systems*, vol. 78, pp. 1052–1054, 2018, ISSN: 0167-739X. DOI: 10.1016/j.future.2017.09.019.

[52] R. Gracia-Tinedo, C. Cotes, E. Zamora-Gómez, G. Ortiz, A. Moreno-Martínez, M. Sánchez-Artigas, P. García-López, R. Sánchez, A. Gómez, and A. Illana, "Giving wings to your data: A first experience of personal cloud interoperability," *Future Generation Computer Systems*, vol. 78, pp. 1055–1070, 2018, ISSN: 0167-739X. DOI: 10.1016/j.future.2017.01.027.

[53] *e-estonia*. [Online]. Available: https://e-estonia.com (visited on 03/10/2021).

[54] *Verwaltungscloud*. [Online]. Available: https://www.brz.gv.at/presse/20170804-verwaltungscloud-gestartet.html (visited on 01/11/2021).

[55] *Services*. [Online]. Available: https://www.bmdw.gv.at/Themen/Digitalisierung/Verwaltung/was-bedeutet-digitale-Verwaltung/E-Government-Bausteine-und-Services/Services.html (visited on 03/15/2021).

[56] *ELAK-Trans 3.0.1*. [Online]. Available: https://neu.ref.wien.gv.at/at.gv.wien.ref-live/documents/20189/95278/elak-trans_3-0-1_20160808.pdf/2b108477-f829-480a-a766-704163ea47e8?version=1.0 (visited on 03/19/2021).