Securing the Rights of Data Subjects with Blockchain Technology

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

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

Johannes Brottrager
Vienna University of Technology
Industrial Software (INSO)
Vienna, Austria
johannes.brottrager@inso.tuwien.ac.at

Phillip Niemeier
Vienna University of Technology
Industrial Software (INSO)
Vienna, Austria
phillip.niemeier@inso.tuwien.ac.at

René Lamber
Vienna University of Technology
Industrial Software (INSO)
Vienna, Austria
rene.lamber@inso.tuwien.ac.at

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

***Abstract*—The European Union's General Data Protection Regulation (GDPR) has been effective for more than a year. Even though several million euros have been spent on GDPR projects, companies are insecure about being fully compliant. The status quo is that companies lack processes and infrastructure for several legal responsibilities regarding rights of data subjects. This leads to manual effort and long waiting times for users. Data protection authorities receive complaints about these waiting times, but affected people cannot legally submit a proof for request initiation since these requests are usually done via the companies' platforms or email. This paper presents a technical solution to this problem by installing a blockchain-based application to submit and track requests for data access securely whilst preserving data protection for the subjects to be able to file complaints and ultimately ensure the given data protection rights.**

Keywords-GDPR; Blockchain; eGovernment; Data Protection

I. Introduction

Data protection and data privacy, especially regarding personal data, has become increasingly important as developments in information technology have raised concerns about information privacy and its implications [1].

With the European Union (EU) regulation 2016/679 General Data Protection Regulation (GDPR), data protection has received a legal foundation concerning the rights of natural persons (data subjects) whose data is processed [2, Art. 12-23] that received international reputation and spawned similar local laws, such as the California Consumer Privacy Act (CCPA) [3]. With it also come obligations of processors of personal data and controllers, who ultimately decide on the purposes and means of the processing [2, Art. 24-43].

The GDPR provides a large number of measures to protect personal data, which companies process, against misuse. This includes, among other things, the right of data subjects to prevent further processing of their data, not only by the controllers but also by entities that received the data from the controller, the processors. Furthermore, data processing was made more transparent for the data subjects by giving them the right to request information about which data is processed, for which purposes, by whom, and may at any time submit an application for modification or deletion of the data. The GDPR applies to all companies in the EU that process personal data, as well as third-country companies if they offer services to EU citizens [2, Art. 3]. Compliance with the data protection measures is enforced by public data protection authorities, who also have extensive rights of access to the processing activities of personal data. Failure to comply with the data protection measures will result in fines of up to 20 million euros or, in the case of a business, up to 4% of its total worldwide annual turnover [2, Art. 83].

The execution of the rights of the data subject can be in written or oral form, provided that the subject can identify himself [2, Art. 12]. The execution via a digital request is not defined any further. Currently, most companies choose to either implement a data protection web form to be filled out online or provide an email address to their customers. This bares two major problems:

Proof of application	The data subject has no proof when and what was applied for (content and time)
Authentication	The data subject must be able to identify himself if the controller is not able to do so

These problems lead to time-consuming processes, for both the controller and the subject, and also, in most cases, insecure processes, with no evidence of submission present.

Blockchain technology, which became famous for its use in the crypto-currency Bitcoin, is now being used in other fields such as asset management, flight insurance, and fund-raising [4]. The technology makes it possible to create a transparent, immutable, decentralized record database created by multiple

978-1-7281-7283-5/20/$31.00 ©2020 IEEE
DOI 10.1109/ICICT50521.2020.00050

Authorized licensed use limited to: UNIVERSIDAD DE GRANADA. Downloaded on January 14,2025 at 16:48:54 UTC from IEEE Xplore. Restrictions apply.

parties. Generally, the benefit of Blockchain use occurs when these parties share a multi-lateral mistrust, but need to work together so that each party can rely on the accuracy of the data stored on the Blockchain while being able to analyze the details simultaneously.

The contribution of this publication is a structured analysis of the issue at hand and a solution proposal for the discussed problems. It introduces a technical concept and prototype implementation of a new solution that withstands the high expectations regarding data protection and privacy.

The paper is organized as follows. First, we present and analyze current research, solutions and background information (Sect. II). Then, we describe the EU eGovernment action plan to promote digitization within the EU, which the proposed solution follows (Sect. III). Afterwards, we describe processes and roles relevant to the proposed solution (Sect. IV) and discuss the current state of the prototype implementation and architecture (Sect. V). Next, we shed light on implications of the solution (Sect. VII). Finally, we reflect on the findings, draw the conclusion and reflect on future work (Sect. VIII).

II. Related Work

The research fields that had to be considered when implementing the data protection platform spread from the field of E-Government (E-Gov), the state of the art in Blockchain technology, especially stamping, and the current state of privacy laws in the considered jurisdictions. Regarding E-Gov, Chadwick [5] examined three models in 2003: the managerial, the consultative and the participatory model. In the context of the Secure idenTity acrOss boRders linKed (STORK) project, research was carried out on the exchange of electronical Identities (eIDs) within the EU [6]. The use of trust services and electronic identification through the eIDAS regulation is encouraged throughout Europe [7]. As of 29 September 2018, EU member states must recognize the notified eIDs of other member states [8]. [9] researched the efficiency and scalability of electronic IDentification, Authentication and trust Services (eIDAS) infrastructure. Federated Identity Management (FIM) in connection with a European eID system was discussed in detail by [10]. Services that enable contracts to be terminated have established themselves in Europe and the United States of America (USA) [11]–[13]. However, the data must be entered manually by the user. There is no official authority behind it, and costs vary depending on the provider. Blockchain-based timestamping is implemented as a variety of free or paid timestamping services such as OriginStamp[1] based on a paper by Gipp et al. [14], or OpenTimestamp[2], in order to prove that something (e.g. a transaction, a file, or a request) existed at a certain point in time. At its core, such a service would be trivial to implement, e.g. by embedding the hash of the document to stamp as a fake public key hash in the PubKeyHash field of a transaction. This is effectively a transaction to a non-existing address, storing the hash on the Blockchain. By using one of the aforementioned services, multiple hashes are stored with one single transaction (e.g. only once a day), making the stamping less wasteful. Regarding the general use and acceptance of Blockchain in legal spaces, multiple projects are serving as a precedent for the use of Blockchain by government entities, such as land registry services in Georgia as well as some African countries [15], or the documentation of civil administration in the Chancheng district in China [16]. Several researchers [17], [18] tried to estimate and predict the impact of the GDPR in advance of the regulation being in place. The reality showed that on the one hand "recorded pageviews and recorded revenues fall by about 10% for EU users after the GDPR's enforcement deadline" [19] and on the other hand the implementation was, one year after the GDPR came into force, not yet finished, and legal situations are still unclear for businesses [20].

Blockchain has shown solutions and issues regarding data protection. One the one hand processings of personal data on the Blockchain have legal issues with regards to the GDPR [21] and on the other hand, solutions for consent management, such as [22] and [23] support the implementation and enforcement of the GDPR in a Blockchain context.

Other nations and states such as Canada (PIPEDA) and California (CCPA) [24], [25] implemented similar data protection laws that will have an impact on the economy [26].

III. E-Government

In 2016, the EU eGovernment Action Plan [27] to promote digitization within the European Union was published. The vision of how public administrations and public institutions in the field of E-Gov should behave and change in the course of the next years can be summarised by the following principles:

- "Digital by Default": The public administration should primarily provide services digitally and also communicate digitally with citizens.
- "Once only principle": If possible, data should only be recorded once by the authority, multiple storage should be avoided.
- "Inclusiveness and accessibility": As many citizens as possible should be able to use services.
- "Openness and transparency": There should be an exchange of data between authorities.
- "Cross-border by default:": Certain data will be made available across borders to strengthen the EU's internal market.
- "Interoperability by default": A free exchange of data throughout the internal market should be possible. Public services should also support this approach.
- "Trustworthiness and Security": Legal security and technical security create trust in the authorities.

The EU eGovernment Action Plan 2016-2020 [27] also sets political goals. These are summarised as:

1) Modernising public administration with the help of ICT.
2) Digital services in the public domain are intended to guarantee cross-border mobility.

[1]https://originstamp.org/
[2]https://opentimestamp.org/

Authorized licensed use limited to: UNIVERSIDAD DE GRANADA. Downloaded on January 14,2025 at 16:48:54 UTC from IEEE Xplore. Restrictions apply.

3) Public services should offer high-quality services and enable easy digital interaction.

The solution presented by the authors is largely based on "interoperability by default" as a goal of the EU eGovernment Action Plan, and on goals 2 and 3 of the political goals. As such, it aligns with the EU E-Gov strategy.

IV. Processes and Roles

A. Roles

Based on the GDPR, the following roles were used for the prototype:

- Data Subject: An identified or identifiable natural person to whom personal data relates.
- Controller: Is responsible for what happens to the data. Provides information in accordance with the GDPR.
- Processor: Processes personal data on behalf of the controller.
- Data Protection Authority (DPA): The respective Data Protection Authority is the national supervisory authority for data protection in the country of the data subject or the controller. Sometimes forms can be accessed on the website of the data protection authority regarding the subjects' rights (e.g. [28]). Among other things, about data information [2, Art. 15], correction [2, Art. 16] or deletion [2, Art. 17] according to GDPR. Further, general complaints can also be submitted.

B. Issues with the rights of the subjects

The rights of a subject are highly dependent on a manual, undocumented, unstandardized process. Since several parties are involved in the usually paper-based processes, a certain administrative effort can be assumed. In the event of a complaint, documents and emails are sent in an unstructured way. The authentication process is also carried out manually (scanning the identity card or passport). These can be (illegally) used by the receiving party and are not a solid proof of identity. It also can be assumed that correspondence takes place via unencrypted media, such as email.

These factors lead to a process that is disastrous from a data protection and data security point of view. A system needs to be in place that helps data subjects to be able to easily exercise their rights without risking their data further.

The authors therefore propose a way as shown in Section V to communicate with the DPA in an encrypted and replicable way. The solution is not limited to one country, the solution can immediately be applied to every DPA of the EU.

C. Process

According to the GDPR, data subjects have several rights concerning their personal data. These are among other things the right to information, access, rectification, withdraw consent, object, right to be forgotten. The authors developed a data protection platform in the form of a prototype according to [2, Art. 15], namely the right of access by the data subject. The prototype itself could be extended for other data protection related inquiries in the future.

The data protection platform uses a simple standardized process for the data subject to create an inquiry faced to the controller or later in the process to the DPA if needed. The standard process is illustrated in Fig. 1 and can proceed as follows:

A data subject provided personal data (1) to the data controller. The data subject issues a request (2) to the data protection platform by selecting his/her country of residence and respective company he/she wants to initiate a request to. The data protection platform asks the user for details regarding his inquiry, such as name and identification names/numbers given by the controller (user name, contract number) and a proof of identity (3) to fill out a request form. The proof of identity differs from country to country. Ideally a country has a public identification system (see Section II). Otherwise, the fallback is a scan of an identification card. The data protection platform fills out a form dependent on the country or falls back to a simple email. The forms are usually given by the countries' DPA and therefore saved on the data protection platform. The data protection contacts are currently not publicly available via any database, therefore the data protection platform collects email addresses of data protection postboxes or data protection officers of companies. The filled-out form is sent to the data protection officer by email via a Simple Mail Transfer Protocol (SMTP) server (4a). If a Pretty Good Privacy (PGP) key for this email address exists, it will be used for encryption. The protocol of the communication between the servers, especially the confirmation of delivery (4b), is appended to the form and is later sent to the data subject. The form including the delivery protocol is hashed with a timestamp (proof) and persisted on the Blockchain (5). As a result, it can be proven later, that the email, with the provided content, was sent to the data protection officer. This information may be provided to the DPA in case of a dispute. This document will be emailed to the person next to a calendar entry file and then deleted from the privacy platform. The calendar entry contains a reminder to the data subject that a complaint can be lodged with the DPA after the expiry of the statutory deadline (according to Article 12 GDPR). The email contains a link that leads directly to the data protection platform. Then, a complaint can be filed with the DPA, in which the proof is stored and the DPA can carry out a review of the request. Included are the signature of the data subject, a proof of the application including the time and a proof of the delivery of the application to the data protection officer.

V. Architecture and Prototype

The data protection platform itself can be run by anyone. It does not necessarily need a direct interface to the DPA nor to the controller. All national data protection agencies are contactable via email[3] while the contact details of each acDPO must be published by the controller according to the GDPR, in many cases including an email address [2]. Therefore, the

[3]A list of all national data protection agencies of EU member states can be found on https://edpb.europa.eu/about-edpb/board/members_en

Authorized licensed use limited to: UNIVERSIDAD DE GRANADA. Downloaded on January 14,2025 at 16:48:54 UTC from IEEE Xplore. Restrictions apply.

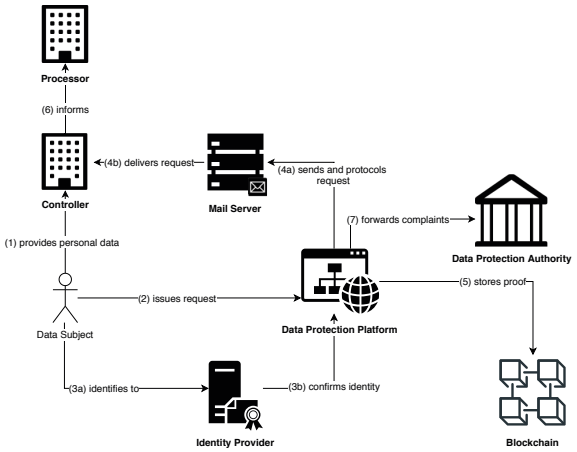

Fig. 1. Actors and processes of the context of the system.

interfacing of the platform with these entities is executed via email.

Since the data protection platform itself is processing personal data it must comply with data protection regulations and be a role-model regarding data protection implementation. It implements privacy by design and default and minimizes the processing and storage of data. The platform does not store any information entered by the data subject but rather hashes the inputs as a filled-out PDF form or an email and deletes the original information after sending it to the controller and data subject via email. The filled-out form then is only saved by the data subject, not on the platform. For convenience reasons, a link containing the entered information is sent to the user, so he/she does not have to enter it again in case of a complaint (see chapter IV).

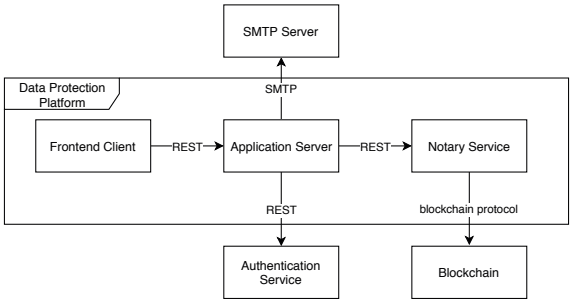

Fig. 2. Architectural overview of the system.

The prototype, that was created to demonstrate the potential of such a platform, consists of a server-side Java stack utilizing the Spring Framework[4] to provide basic functionalities regarding front-end content delivery, PDF generation, and SMTP communication. The prototype's front-end is realized via an Angular[5] client that provides the user-facing forms and sends requests to the application server. In order to publish hashes on the Bitcoin Blockchain, the OpenTimestamps [29] protocol is used by a separate notary service. The OpenTimestamps protocol achieves scalability through aggregation. Hashes that are to be stored on the Blockchain are collected on the OpenCalendar servers[6] and committed in bulk as a merkle tree[7] using a single OP_RETURN[8] transaction.

As visualized in Fig. 2, the three components of the platform communicate via restful HTTP requests amongst themselves and with the authentication service, i.e. the respective provider of the eID. The inquiries to the respective data controllers are sent out using the SMTP protocol, while communication with the Blockchain is executed via the corresponding Blockchain protocol.

VI. Data Protection

The platform itself processes the personal information entered by the requester. The information is temporarily stored during the execution of the signature and E-Mail processing and afterwards deleted. The blockchain stamping service only receives a hash of the signed document and stores (as described in chapter V) the root of a merkle tree of document hashes. Therefore the platform implements "Privacy by Design".

VII. Implications

The current research shows the importance and necessity of data protection. Countries around the world are starting to tackle the challenges occurring with data protection. After finally defining the rights of the people (data subjects), current models, such as the European GDPR have one problem in common: Enforcement of the data subject rights. The implemented prototype showed the feasibility of a centralized, blockchain-backed data protection platform that enables a data subject to execute their rights toward strong entities such as controllers and the government.

The prototype showed that a data protection platform can be operated based on existing identification and stamping services. Only the hosting costs of the simple web application consisting of a web server and a mail server (see Section V) have to be paid since the other services are either state-owned or free. One time-consuming task was the collection of company information and their data protection officer, the implementation of the existing identification service and collection of complaint forms of data protection agencies.

It is possible that such a platform would be operated by a government, especially the data protection authorities, but could be run by anyone.

The implementation furthermore showed, that there are deficiencies in the current GDPR-relevant processes, such as:

[4]https://spring.io

[5]https://angular.io

[6]Such as https://alice.btc.calendar.opentimestamps.org/, which currently commits every 1.8 hours on average.

[7]A merkle tree is an abstract data type in form of a tree that stores objects, in our case the hashes of the stamped documents in its leaf nodes. All none leaf nodes are hashes of their respective child nodes. This means, that changing any hash would invalidate the root hash, which is therefore the only thing that has to be stored, saving greatly on storage requirements.

[8]OP_RETURN results in a transaction that burns the sent bitcoins and stores output data on the Blockchain.

Authorized licensed use limited to: UNIVERSIDAD DE GRANADA. Downloaded on January 14,2025 at 16:48:54 UTC from IEEE Xplore. Restrictions apply.

- No standardized forms for application at the authorities
- Missing data protection and secure identification for authentication and authorization of requests
- Lack of available information regarding data processing companies and their data protection officers
- No standardized interface (barring email) for complaints or requests to the controller

These can be overcome by a step by step migration to and introduction of a new platform. Starting with the data protection platform, interfaces to data protection authorities for data access (companies and data protection officers) and data submission (complaints) could be created as a further step. Furthermore, national or multinational identification systems could be integrated. Finally, a mandatory interface for every online operating data processor with a website could be enforced in order to be able to file requests.

VIII. Conclusion

With the GDPR being in effect for more than a year, companies are still in desperate need of more efficient ways to handle GDPR requests, all while ensuring compliance to the data protection rights given to data subjects. Research identified prerequisites and challenges for an efficient multinational implementation such as secure identification, standardization, and availability of information about data processors. The authors showed how a central platform for supporting the protection of data subjects' rights using Blockchain technology can be realized. The presented approach contributes to solving the issue of trust and replicability in data protection requests and ultimately the enforceability of peoples' legal rights. As such a solution, the prototype may be implemented as a multinational platform to assist data subjects, data processors and controllers to more efficiently comply with regulatory guidelines in a standardized way across multiple territories.

References

[1] R. E. Crossler, "Privacy in the digital age: a review of information privacy research in information systems," *Management Information Systems Quarterly*, vol. 35, no. 4, pp. 1017–1041, 2011.

[2] Council of European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," *Official Journal of the European Union*, vol. L119, May 2016. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC

[3] T. Ehret, "Data privacy and GDPR at one year, a U.S. perspective. Part One - report card," *Reuters Financial Regulatory Forum*, 2019. [Online]. Available: https://www.reuters.com/article/bc-finreg-gdpr-one-year-report-card-part/data-privacy-and-gdpr-at-one-year-a-u-s-perspective-part-one-report-card-idUSKCN1SS2K5

[4] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: current status, classification and open issues," *Telematics and Informatics*, 2018.

[5] A. Chadwick and C. May, "Interaction between States and Citizens in the Age of the Internet: "e-Government" in the United States, Britain, and the European Union," *Governance*, vol. 16, no. 2, pp. 271–300, 2003. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-0491.00216

[6] V. Koulolias, A. Kountzeris, H. Leitold, B. Zwattendorfer, A. Crespo, and M. Stern, "STORK e-privacy and security," in *2011 5th International Conference on Network and System Security*, Sep. 2011, pp. 234–238.

[7] European Parliament and Council of European Union, "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," *Official Journal of the European Union*, vol. L257/73, 7 2014. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2014/910/oj

[8] eID User Community, "Overview of pre-notified and notified eID schemes under eIDAS." [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

[9] D. Berbecaru and A. Lioy, "On integration of academic attributes in the eIDAS infrastructure to support cross-border services," in *2018 22nd International Conference on System Theory, Control and Computing (ICSTCC)*, Oct. 2018, pp. 691–696.

[10] 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.

[11] T. Landauer, "Online-Kündigen." [Online]. Available: https://www.online-kuendigen.at

[12] Aboalarm, "Aboalarm." [Online]. Available: https://www.aboalarm.de

[13] Law Depot, "Free Legal Documents, Forms and Contracts." [Online]. Available: https://www.lawdepot.com

[14] B. Gipp, N. Meuschke, and A. Gernandt, "Decentralized trusted timestamping using the crypto currency bitcoin," *arXiv preprint arXiv:1502.04015*, 2015.

[15] N. Kshetri and J. Voas, "Blockchain in developing countries," *IT Professional*, vol. 20, no. 2, pp. 11–14, 2018.

[16] H. Hou, "The application of blockchain technology in E-government in China," in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2017, pp. 1–4.

[17] C. Tankard, "What the GDPR means for businesses," *Network Security*, vol. 2016, no. 6, pp. 5–8, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1353485816300563

[18] J. P. Albrecht, "How the GDPR will change the world," *Eur. Data Prot. L. Rev.*, vol. 2, p. 287, 2016.

[19] S. Goldberg, G. Johnson, and S. Shriver, "Regulating Privacy Online: The Early Impact of the GDPR on European Web Traffic & E-Commerce Outcomes," *Available at SSRN 3421731*, 2019.

[20] J. Heidrich, "Wirklich wichtig," *iX*, vol. 6, pp. 80–83, 2019.

[21] D. Schmelz, G. Fischer, P. Niemeier, L. Zhu, and T. Grechenig, "Towards using public blockchain in information-centric networks: challenges imposed by the European Union's general data protection regulation," in *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*. IEEE, 2018, pp. 223–228.

[22] K. Rantos, G. Drosatos, K. Demertzis, C. Ilioudis, and A. Papanikolaou, "Blockchain-based Consents Management for Personal Data Processing in the IoT Ecosystem," in *ICETE (2)*, 2018, pp. 738–743.

[23] C. Wirth and M. Kolain, "Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data," in *Proceedings of 1st ERCIM Blockchain Workshop 2018*. European Society for Socially Embedded Technologies (EUSSET), 2018.

[24] D. Lackey and N. Beaton, "The current state of data protection and privacy compliance in Canada and the USA," *Applied Marketing Analytics*, vol. 4, no. 4, pp. 355–359, 2019. [Online]. Available: https://www.ingentaconnect.com/content/hsp/ama/2019/00000004/00000004/art00009

[25] CCPA, "The California Consumer Privacy Act of 2018." [Online]. Available: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

[26] Forbes, "How CCPA Will Impact The World's Digital Economy." [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2019/10/31/how-ccpa-will-impact-the-worlds-digital-economy/

[27] 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

[28] DSB, "Austrian Data Protection Authority," 2019. [Online]. Available: https://www.data-protection-authority.gv.at

[29] P. Todd, "OpenTimestamps: Scalable, Trustless, Distributed Timestamping with Bitcoin (2016)," 2016. [Online]. Available: https://petertodd.org/2016/opentimestamps-announcement

Authorized licensed use limited to: UNIVERSIDAD DE GRANADA. Downloaded on January 14,2025 at 16:48:54 UTC from IEEE Xplore. Restrictions apply.