Self-sovereign identity systems and European data protection regulations: an analysis of roles and responsibilities

Andrés Chomczyk Penedo [1]

Abstract: Decentralized identity systems have taken a key role in the identity management landscape. Self-sovereign identity management systems have promised to return control over identity to individuals. However, these promises still need to be assessed against the existing regulatory framework. As identity attributes can be considered personal data, rules such as the General Data Protection Regulation are applicable. The existing legal literature has still not delivered an analysis of who is a controller and who is a processor in the context of a self-sovereign identity system for the process of identity creation. As such, the purpose of this contribution is to tackle this challenge.

Keywords: digital identity, self-sovereign identity, identity management, data protection, privacy.

1 Introduction

Decentralized systems have taken the centre stage in the identity management landscape in the last couple of years [Bl19, Ab16, Al16]. Although identity can be considered as a human right [Al18], it is also possible to consider that the elements that compose an identity, as noted by Wang and De Filippi [WD20], are also personal data. With the rise of decentralized solutions for identity management, several legal scholars have devoted themselves to the analysis of the legal and regulatory compliance of such systems [WD20, Fi19, Wa18]. However, their analysis has focused mainly on whether blockchains and private distributed ledgers, that provide the technical infrastructure for these systems, can be compliant with data protection regulations. In this respect and to the best of our knowledge, an analysis, from a data protection perspective, of how these systems operate is still missing. Therefore, this contribution seeks to address this point.

[1] Vrije Universiteit Brussel, Department of Interdisciplinary Studies of Law (Metajuridica), Law, Science, Technology and Society (LSTS) Research Group, Pleinlaan 2, Elsene, Brussel, 1050,
andres.chomczyk.penedo@vub.be, https://orcid.org/0000-0002-6820-999X

The author has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No 813497.

2 Identity, digital identity, and the case for self-sovereign identity

Identity can be characterized as "(…) an experience of the essential consistency and continuity of the self in time and space, as well as observations and acknowledgments of existence by others" [DG18]. Identity is built upon information that allows an individual to separate itself from the rest of society and individualized itself above the whole. While there are certain aspects of an individual's identity that might be possible to construct on a solitary basis, a considerable portion of it is built upon interactions between the individual and third parties.

2.1 Identity's legal framework

The information that constitutes an identity "(…) is a collection of individual attributes that describe an entity and determine the transactions in which that entity can participate" [Ab16]. In this respect, Wang and De Filippi [WD20] argue that following the definition of personal data provided by Article 4.1[2] General Data Protection Regulation[3] ("GDPR"), the attributes of identity could be deemed as personal data. Moreover, Al Tamimi [Al18] mentions that it is also possible to consider identity to be protected as a human right[4].

2.2 What is a digital identity and its relevant legal framework?

As Kim Cameron points out, a digital identity is a set of statements that a digital subject makes about itself or another digital subject [Ca05]. These digital subjects can be either a natural or legal person as well as a thing -mainly hardware-, such as an IoT sensor. These statements are called claims, i.e., an assertion regarding the veracity of something which is usually under discussion or doubt, and are associated with a digital subject using an identifier. In this regard, and following Wang and De Filippi [WD20], if these statements are related directly or indirectly to an identified or identifiable natural person, then they would be considered as personal data.

[2] " (…) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; (…)"

[3] 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)

[4] While his research focuses solely on European case law and regulations, his approach applies to other regional human rights systems that protect the same aspects of identity, such as the Latin American system organized, mainly, under the San José de Costa Rica Treaty as well as national regulations. Al Tamimi focuses on the rights to private life, religious freedom, and free association which are present in the San José de Costa Rica Treaty under articles 11, 12, and 16, respectively. Moreover, other rights provided in this international treaty could also serve as a base for the protection of human identities such as the right to a name or the right to a nationality in articles 18 and 20, respectively.

However, identifiers are not directly linked to claims but instead are stored in a credential, which in return can have one or more declarations [Al16] and even regarding one or more digital subjects [Ca05]. Using these identifiers, it is possible to distinguish an entity from the rest. Identifiers should fulfil two fundamental requirements for them to be effective and useful: identifiers should be unique and limited in amount per field [WD20]. To achieve this, centralization has long been the answer to make identity systems useful in their purpose [Al16].

2.3 What is self-sovereign identity and its relation to identity's legal framework?

The process of creating a digital identity depends on how the identity system is designed; most of the current systems rely greatly upon the interaction with a centralized entity that acts as an identity provider, as Allen remarks [Al16]. As such, users were and still are, vulnerable to actions that could compromise either the confidentiality, the integrity, or the availability of the information since their data, i.e., the attributes that are part of their identities, is controlled by other entities.

To solve the perils that centralization poses, the idea of self-sovereign identity ("SSI") systems was proposed by Christopher Allen in his paper titled "The Path to Self-Sovereign Identity" [Al16]. This idea puts the individual at the centre of an identity system and all actions related to identity need to be authorized by that person by consenting to that data processing activity. Giannopoulou and Wang argue that SSI systems are "(…) rooted in the belief that individuals have the right to an identity independent of reliance on a third-party identity provider, such as the state or any other central authority" [GW20].

Within this context, Allen, building upon previous work, put forward 10 principles that SSI systems should follow to be considered as such, namely: (i) existence; (ii) control; (iii) access; (iv) transparency; (v) persistence; (vi) portability; (vii) interoperability; (viii) consent; (ix) minimalization; and (x) protection. Several of the principles that Allen proposes are aligned, if not expressly recognized, with data protection principles and rights provided for by the GDPR and similar regulations. While compliance with data protection principles is mandatory for any identity management system, SSI systems can leverage the fact that their development has started after the enactment of regulations such as the GDPR. Therefore, their design and implementation can already be made following these principles rather than adapting and adjusting to them. In this respect, legal scholars, such as De Filippi and Wang [Fi19], and different reports drafted regarding SSI systems, mainly from the European Union Blockchain Observatory and Forum [Bl19], have also recognized that SSI systems could become an important tool, if properly deployed, to enhance and foster the rights and safeguards prescribed in data protection regulations, such as the GDPR.

Controllers could leverage the SSI system to achieve compliance with the data protection regulations. For example, the SSI system might have a template where the mandatory

information of Article 13 GDPR, or any other relevant data protection regulation, could be provided before any data collection takes place. Also, SSI systems developed with the privacy by design principle in mind could help to achieve a proper informed consent[5], following the requirements set by the Article 29 Working Party ("WP29") and the European Data Protection Board ("EDPB") [Gu20a]. Moreover, SSI system developers proclaim that these systems could foster data subject's rights exercise although no evidence has yet been produced regarding this.

Beyond the identity creation process, the use of the data associated with that identity constitutes a data processing activity that is subject to data protection regulations. If an individual is requested for certain information regarding its identity to provide a service, that activity triggers the applicability of, for example, the GDPR. If the SSI system works properly, the individual would have greater control over how their data is used because they will know in greater detail which data was requested as well as for which purposes but compliance with GDPR still is necessary for the data processing activities carried out by the relying parties on such identity.

The use of blockchain and distributed ledger technologies is not necessary for the development of an SSI system although its use is aligned with some of the guiding principles stated by Allen [GW20]. However, if these technologies are used, then all identified issues, and proposed solutions, regarding data protection regulations should also be considered to make the system and its use compliant with the GDPR

3 How are roles in an SSI system assigned under European data protection regulations?

Recital 79 GDPR states that "[t]he protection of the rights and freedoms of data subjects (…) requires a clear allocation of the responsibilities under this Regulation (…)". The question proposed in the headline is, therefore, of the uttermost importance and should be the starting point for any debate around how the SSI system should comply with European data protection regulations or any other piece of legislation related to data protection.

The answer to this question could help policymakers, practitioners, and academics in addressing other data protection-related issues regarding SSI systems. Identity management systems are complex; there are several data processing activities taking

[5] Since a great deal of importance is placed on fostering consent-based interactions through SSI systems, it is possible to further overload data subjects with consent requests, albeit in a different format, that could result in a situation not that different from the current crisis that consent is undergoing or, even worse, further deepen it, as well as causing information fatigue [SC14]. Following with this, information, according to the existing interpretation from authoritative bodies [Gu18], needs to be tailored in several manners: from timing to wording as well as structure, keeping always in mind the intended audience. SSI systems proclaim that, through them, data subjects can have complete knowledge about how and who will make use of their data. However, the effectiveness of this mechanism for this purpose still needs to be tested.

place at the same time and, often, they are interconnected [Ab16]. To properly answer this question, it is possible to differentiate between the roles performed for the creation and operation of digital identities, mainly credentials and identifiers, and, on the other hand, the roles of the infrastructure used to operate the SSI system. Since the latter has been addressed by legal scholars, see e.g. [Fi19], focus for this contribution shall be placed on the former. Moreover, and as mentioned above, the specific usage of an identity created and operated through an SSI system can also be analysed under the lens of data protection regulations, but that analysis is beyond the purpose of this contribution.

3.1 Roles in the creation and operation of a digital identity within an SSI system

SSI systems do not function statically as they are intended to operate relying upon a horizontal model of equality between all participating actors [Wa18]; in this regard, it is possible to say that SSI systems intend to escape the hierarchical relationship with which the GDPR, and many other similar regulations, was conceived, i.e., the controller/data subject structure. By looking into some of the most relevant projects and technical standards under development [DI20] and taking into consideration the previously mentioned principles, it is possible to outline some common features among SSI systems to answer the proposed question.

In this regard, and for this contribution, the following operational structure for the identity creation process of a hypothetical SSI system is proposed: (i) any individual might make claims about themselves and add such claims into a credential issued by them; (ii) individuals and legal entities might make claims about other individuals and add such claims into a credential issued by them; (iii) the credential might be held by a different entity than the individual that the credential refers to; (iv) the credential is stored in a medium under complete control of the holder (v) individuals are allowed to self-issue identifiers, in particular, decentralized identifiers; and (vi) a verifiable data registry using a public distributed ledger is used for facilitating the managing of identifiers and claims. The proposed structure could be used by both trusted identity providers as well as individuals interacting on a peer-to-peer basis.

3.2 Who can be a controller in an SSI system?

Identifying the controller within the context of certain data processing activity is of the uttermost importance since "(…) they are the primary bearers of the obligations set by such law towards data subjects" [Kr20]. To answer this first question, it is possible to start with the definition of data controller provided by Article 4.7 GDPR[6].

[6] "(…) means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its

To interpret this concept, EDPB has recently published the update to WP29's Opinion No. 1/2010 regarding the concepts of controller and processor in the GDPR [Gu20b][7]. As it is pointed out in that guidance, there are 5 core elements to the concept of controller: (i) the entity that determines the processing; (ii) the actual determination of the processing; (iii) whether the determination is done solely or jointly with other; (iv) which purpose and means are determined; and (v) the determination of the process itself. WP29 characterized the role of the controller by stating that it was the entity that dictated the information lifecycle, from its collection to its destruction [Op10]; although this characterization with those exact words is missing in EDPB's guidelines, the idea remains present due to the relevance of the determination.

The process of determining who is a controller demands a fact-based answer where a considerable number of factors play into account [Kr20]. SSI systems intend to put people in control of their identity. Following EDPB's criteria, the information lifecycle would be dictated by the individual, i.e., the purposes and means for processing personal data would be selected by a person. In this context, the only one legally authorized to arrange the creation, maintenance, and operation of a digital identity would be that individual. As mentioned above, EDPB follows closely the criteria set forth by WP29 and expands upon it due to recent developments in the caselaw from the Court of Justice of the European Union ("CJEU")[8].

Regarding the first criteria, Article 4.7 GDPR allows for natural persons to be controllers; therefore, an individual might be considered as such. Being able to determine a processing activity implies that an entity has influence, either legal or factual, to choose why data are processed. In this respect, an individual meets both criteria. Identity is a right that is recognized to an individual and only that individual is legally authorized, unless a specific provision applies to the case such as the case of parents over their children, to act over such identity. On a factual basis, only that person should be in the position to decide about their own identity.

As for the last two criteria -the purposes and means, and the processing itself- the EDPB elaborates on the ideas drafted by WP29. In this regard, EDPB upholds that purposes and means, from a data protection perspective, constitutes why and how a data processing activity takes place; therefore, to qualify as controller, it is necessary to choose the objective for which data shall be processed and, also, the technological resources that shall be used to that end [Gu20b]. However, not all means are equally important and, as

nomination may be provided for by Union or Member State law (…)"

[7] As of the date hereof, the document is still under public consultation period and changes could occur.

[8] In this respect, we are referencing to the following cases: Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV., ECLI:EU:C:2019:629 (Court of Justice of the European Union (Second Chamber) 2019); Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta, ECLI:EU:C:2018:551 (Court of Justice of the European Union (Grand Chamber) 2018); and Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, ECLI:EU:C:2018:388 (Court of Justice of the European Union (Grand Chamber) 2018).

such, only those that could be deemed as essential would be important enough to meet the standard to qualify as controller [Gu20b].

Nevertheless, individuals are in the perfect position to choose why their identity data becomes part of a credential and then, attach it to a decentralized identifier -determination of purposes- and it is up to them the selection of the tools, i.e., picking a platform, selecting a wallet to store credentials, etc., that would be essential to this activity -determinations of means-. Finally, as for the processing itself, data subjects would be the ones choosing whether to enrol in this identity management solutions and, as such, determining the activity to be performed upon their data.

However, and as the literature points out, if an individual merely processes their personal data, then the GDPR -as well as any other data protection regulations based upon it or with a similar structure- would not be applicable; this is because data protection regulations, such as the GDPR, need the existence of two separate entities that act as controller and data subjects, respectively, to be applicable, see e.g. [Kr20]. It is appropriate to ask and try to answer whether an individual is a controller, therefore rendering the inapplicability of the GDPR or similar data protection regulations, or if other entities involved in these data processing activities, would-be controllers.

As for the first question, while it is possible for an individual to become a controller of personal data and the case law from the CJEU seems to be inclined in the direction of expanding the consideration of individuals as controllers [Ed20], it is not so clear that data subjects can become controllers of their data. In a sense, as Bygrave and Tosoni point out, the whole purpose of data protection regulations is "(…) to protect others' interest (i.e., those of data subjects), not their own (…) In essence, it would seem logical that a controller must be some party other than the data subject" [BT20a]. As such, at least what respect to the identity creation process under analysis herein, individuals would not be considered as controllers regarding their own identities. The WP29 pointed out that the assignment of the role of the controller should be to help data subjects to have a clear entity to demand their rights [Gu20b]. In this regard, a question that could be asked is if the shift of controllership to an individual, i.e., traditional data subject in any other identity system, is acceptable or not, but this falls beyond the scope of this contribution.

It is possible to wonder if other entities, including other individuals, can be controllers in the identity creation processes. In contrast to the situation presented above, the alternation needed to trigger the applicability of the GDPR exists. Therefore, any other person who intends to do that -create and operate a digital identity- would incur into a data processing activity as it would be determining purposes and means. However, an individual might be a controller but could be exempt from complying with the GDPR. In this regard, Article 2.2.c.[9] GDPR -the personal or household exemption- could be used in certain situations. For example, a legal representative of a child could be considered as a

[9] "(…) 2. This Regulation does not apply to the processing of personal data: (…) (c) by a natural person in the course of a purely personal or household activity; (…)"

controller as the individual, i.e., the child, would not be processing its data to construct its identity but instead, this would be done by a third party, e.g., their legal representative. This exemption needs to be interpreted when it is applied to a particular case. To do so, it is possible to rely on Recital 18 GDPR[10].

According to it, it shall be necessary to pay particular attention to the legal relationship between the individuals involved in the processing activity to address the type of data protection relationship which they will have. In other words, and as Recital 18 GDPR states, if the bond between controller and data subjects does not imply a commercial or professional relationship, the personal or household exemption would be applicable. Legal literature commenting on the existing caselaw of this exemption under the former European data protection directive, whose wording is mimic by the GDPR and therefore its analysis relevant to it, is inclined in this respect [Kr20]. In this sense, a parent managing the digital identity of their child may fall within the household exemption while the management of digital identity by the guardian of an insane would not and, therefore, it would be a controller that shall need to comply with the GDPR.

Generally, it is possible to conclude that the individual would not be considered a data controller regarding the issuance of their credentials. When it comes to the issuance of credentials and the association of such credentials to a decentralized identifier for those with whom it shares a family bond, the household exemption would be applicable. As for other entities that process personal data related to an individual's identity, that processing operation would constitute a data processing activity that would imply considering that entity as a controller as it is defining purposes and means.

3.3 Who can be a processor in an SSI system?

While the core data processing activity in an SSI system would be the operation of credential issuance and pegging to a decentralized identifier, it is possible to mention that other activities are secondary to that: from the validation of claims to the storage of credentials or their presentation. However, the main shared characteristic among these is that none of them, in principle, implies the determination of purposes and means. Any entity conducting those activities could be considered as a processor. As EDPB denotes, "[t]he role of a processor does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context (…) In practice, where the provided service is not specifically targeted at processing personal data or where such processing does not constitute a key element of the service, the service provider may be in a position to independently determine the purposes and means (…)" [Gu20b].

[10] "This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities."

As for this second question, it is possible to follow the same path as before by relying on the definition of data processor as prescribed in Article 4.8 GDPR[11]. EDPB rightly points out that what matters to determine if an entity is a processor is a decision of by a controller -in this case the individual- to delegate into a third-party certain processing activity per its instructions, i.e., there needs to be some act of delegation by the controller in favour of the processor [Gu20b]. As Bygrave and Tosoni mention, to consider an entity as a processor, there needs to be an entity acting as a controller to impose processing conditions [BT20b]. However, if the processor, going against the mandate given by the controller, determines for what and how will data be processed, then that entity would have crossed the threshold and would become a controller [Op06].

If the controller is not the data subject or an individual that can rely on the exemption provided for in Article 2.2.c, there is no doubt that the full extent of the GDPR applies and that the processor would have to comply with the GDPR. However, if the data subject or an individual that can rely on that exemption is the controller, does the processor still has to comply with the GDPR? The fact that the controller is exempt from complying with the GDPR does not imply that exemption should be extended to the processor as the exception must be interpretive restrictively and as it only covers the controller, as noted by Recital 18 GDPR [Kr20].

Certain regulated activities, such as the services covered by the eIDAS Regulation[12], have a logical connection with SSI systems [Al20]. The question of how the eIDAS Regulation should be applied to the SSI system is on itself a topic that exceeds this contribution and one which there is no answer yet from authoritative bodies. Nevertheless, it is possible to ask if a trust service provider can be considered as a processor for the controller or whether it is a controller due to the determination of purposes and means. The literature is inclined towards considering trust services providers as controllers as a trust service provider is the sole responsible for how its business shall be run, i.e., it is the one that determines purposes and means for the processing of data [Ts16]. However, given that within an SSI system context, data processing activities are constraint to what the individual allows, trust service providers would have their autonomy severely limited but also due to what the developers of the software have permitted within the code over which an SSI system runs.

3.4 Are the developers of an SSI system controllers, processors, or something else?

Software developers are in a particular situation in *peer-to-peer* solutions[13]. Therefore, it

[11] "(…) the natural or legal person, public authority, service or other body that processes personal data on behalf of the controller (…)".

[12] 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

[13] In the field of decentralized finance, there is an ongoing discussion on whether developers have to comply with applicable financial regulations if they can be considered as the prime responsible for it [Va19].

is possible to ask if developers are determining means and purposes from a data protection perspective in the case of an SSI system. Although software developers through their code condition and limit what users can do with the software in question by only making it useful for certain activities done in a certain way, such limitation is not sufficient to consider that purposes and means have been selected for the user. For example, none would even think about considering Microsoft as a controller over users for the provision of a copy of Word installed on a home computer. Users of SSI systems are free, first, to use them and, second, to select which attributes of their identity would be uploaded.

However, if developers operate in any manner the SSI system, this argumentation falls short as there is some form of determination of processing activities as well as purposes and means. As such, a middle ground solution could be considering the existence of a joint controllership with the data subject. The CJEU has already ruled in certain cases that individuals can be joint controllers with other, either persons or legal entities [Ed20]. The trouble with this approach is twofold. On one hand, the fact that the individual cannot be the controller of their data is still on the table, as noted above. On the other hand, and according to EDPB, joint controllership must result from a converging decision, i.e., the purposes and means selected by each entity have a symbiotic relationship between each other and result in a single larger data processing activity [Gu20b]. This solution might be relevant for those cases where the controller is someone besides the person that their credentials refer to, as described above.

Developers could be considered as data processors by proving resources to the individual to carry out all activities related to the creation and maintenance of the credential. In this regard, as pointed out by Recital 18, software developers might be processors. As for guidance on this matter, the EDPB has not addressed the situation in their guidelines regarding the concepts of controller and processor; the only piece of advice given by EDPB that could be somehow used for further interpretation is provided as an example of an IT consultant that incidentally process personal data and where the entity that request the provision of such software development activity assumes any liability arising from such performance by a third party [Gu20b].

4 Conclusions

Decentralization and peer-to-peer relations have shaken regulations as most of our legal systems are structured around the identification of an accountable entity. In the case of existing European data protection regulations, the question regarding how SSI systems can reach compliance, if possible at all, with them is still an open question. While these types of identity management systems are intended to foster users' control over their identity personal data, the actual details on how to implement them in a compliant manner demand further analysis and, most important, guidance from authority bodies.

In this contribution, some insights were provided for this endeavour regarding the process of identity creation: (i) individuals can build and operate their own identity and would not be data controllers of such process; (ii) individuals and legal entities building and operating other people identities can be both data controllers or processors, depending on the situation, although in certain cases exempt from having to comply with these regulations, as in the case of parents for their children identity; and (iii) SSI systems developers would most likely be exempt from the application of data protection regulations as data controllers or processors unless they engage in building or operating those identities in any manner whatsoever.

Although the discussion is still open, there is one thing that is clear among the overall uncertainty: any action taken needs to put individuals at the front and avoid making existing, functioning, and tested pieces of regulation not applicable. In this respect, any SSI system should keep its focus on the founding principles of them: individuals should be able to seek legal remedy against any wrongdoing over their identity and not putting burdens on them.

Bibliography

[Ab16] A Blueprint for Digital Identity. World Economic Forum, Aug. 2016.

[Al16] Christopher, Allen. The Path to Self-Sovereign Identity. Life With Alacrity, 25 Apr. 2016, http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html, date accessed February 15, 2021.

[Al18] Yussef, Al Tamimi: Human Rights and the Excess of Identity: A Legal and Theoretical Inquiry into the Notion of Identity in Strasbourg Case Law. Social & Legal Studies, vol. 27, no. 3, pp. 283–98, June 2018.

[Al20] Ignacio, Alamillo Domingo. How EIDAS Can Legally Support Digital Identity and Trustworthy DLT-Based Transactions in the Digital Single Market. European Commission, Apr. 2020.

[Bl19] Blockchain and Digital Identity. EU Blockchain Observatory and Forum, 2 May 2019.

[BT20a] Lee, A., Bygrave, and Luca, Tosoni. Article 4(7). Controller. The EU General Data Protection Regulation (GDPR) A Commentary, edited by Christopher, Kuner et al., 1st ed., Oxford University Press, pp. 145–56, 2020.

[BT20b] Lee, A., Bygrave, and Luca, Tosoni. Article 4(8). Processor. The EU General Data Protection Regulation (GDPR) A Commentary, edited by Christopher, Kuner et al., 1st ed., Oxford University Press, pp. 157–62, 2020

[Ca05] Kim, Cameron. The Laws of Identity. May 2005.

[DG18] Dragana, Deh and Danica Glođović: The Construction of Identity in Digital Space. AM Journal of Art and Media Studies, vol. 16, pp. 101–11, 2018.

[DI20] Decentralized Identity, https://github.com/decentralized-identity/decentralized-identity.github.io/blob/master/assets/map-of-adjacent-orgs-and-specs--sept-2020--one-

sided.pdf, date accessed February 15, 2021.

[Ed20] Lilian, Edwards, et al. Data Subjects as Data Controllers: A Fashion(Able) Concept? Internet Policy Review. *policyreview.info*, https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400, date accessed April 9, 2021.

[Fi19] Michèle, Finck. Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?, European Parliament, 2019.

[Gu18] Guidelines on Transparency under Regulation 2016/679. WP260 rev.01, Article 29 Working Party, 11 Apr. 2018.

[Gu20a] Guidelines on consent under Regulation 2016/679. 05/2020, European Data Protection Board, 2 Sept. 2020.

[Gu20b] Guidelines on the Concepts of Controller and Processor in the GDPR. 07/2020, European Data Protection Board, 2 Sept. 2020.

[GW20] Alexandra, Giannopoulou and Fennie, Wang. Self-sovereign identity. Glossary of distributed technologies. Internet Policy Review. *policyreview.info*, https://policyreview.info/glossary#node-1524, date accessed April 9, 2021.

[Kr20] Herke, Kranenborg. Article 2. Material Scope. The EU General Data Protection Regulation (GDPR) A Commentary, edited by Christopher, Kuner et al., 1st ed., Oxford University Press, pp. 60–73, 2020.

[Op06] Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). WP128, Article 29 Working Party, 22 Nov. 2006.

[Op10] Opinion 1/2010 on the Concepts of 'Controller' and 'Processor'. WP 169, Article 29 Working Party, 16 Feb. 2010.

[SC14] Bart, W., Schermer, and Bart, Custers. The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection. Ethics and Information Technology, vol. 16, no. 2, p. 12, June 2014.

[Ts16] Niko, Tsakalakis, et al. What's in a Name: The Conflicting Views of Pseudonymisation under EIDAS and the General Data Protection Regulation. Gesellschaft für Informatik, 2016, pp. 167–74.

[Va20] Peter, Van Valkenburgh. Electronic Cash, Decentralized Exchange, and the Constitution. CoinCenter, Mar. 2019.

[Wa18] Kai, Wagner, et al. Self-sovereign Identity A position paper on blockchain enabled identity and the road ahead. Identity Working Group of the German Blockchain Association, 23 Oct. 2018.

[WD20] Fennie, Wang and Primavera, De Filippi: Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. Frontiers in Blockchain, vol. 2, p. 28, Jan. 2020.