Operationalizing the law through the Solid environment: opportunities and challenges

Lola Montero Santos[1,*]

[1] *European University Institute, Via Bolognese, 156, 50139 Florence, Italy*

Abstract

This paper identifies the opportunities for the Solid environment in light of the new EU mandatory data sharing obligations under the Data Act. It also outlines several misalignments of current Solid specifications and specific EU legal requirements under the GDPR and the Data Act. Reflections are put forth on the current third party pod providers identified on the Solid Website.

Keywords

Mandatory data sharing, Data Act, Solid environment

1. Introduction

The legal framework for data sharing in the European Union (EU) is experiencing a profound transformation. The EU Data Protection Regulation (GDPR) mandates the portability of personal data (art. 20 GDPR) in some limited conditions, but only if technically feasible. Meanwhile, the Regulation on the Free Flow of Non Personal Data (FFNPDR) sets a voluntary framework for the sharing of non-personal data. Neither of these instruments achieved the desired increase in data availability in the EU market. Therefore, the EU's current strategy for data pursues a much more compulsory approach. Mandatory (also called statutory) data sharing includes all the circumstances that trigger the compulsory access (reading and/or transfer) of data. The recently adopted Data Act (DA) sets a general framework for the applicable conditions under mandatory data sharing (Ch. 3 & 4 DA) and mandates data sharing in two specific contexts: connected devices (Ch. 2 DA), and data processing services (Ch. 6 DA). The Solid environment can offer a technical solution that operationalizes these data sharing obligations.

This paper pursues two goals: 1) to identify the opportunities for the Solid environment to operationalize the statutory data sharing obligations contained in the DA, and 2) to outline the shortcomings or misalignments of current Solid specifications and the EU statutory data sharing requirements. In its conclusion, this paper reflects on the Third Party Solid Providers (the Pod Providers) currently available on the Solid Website.

Solid Symposium 2024, May 2–3, 2024, Leuven, Belgium

* Corresponding author.

lola.monterosantos@eui.eu (L. Montero Santos)

0000-0001-6069-6685 (L. Montero Santos)

This article is partially funded by the COST Action on Distributed Knowledge Graphs (CA19134), supported by COST (European Cooperation in Science and Technology)

2. The scope of the paper: Third Party Solid Pods for individuals

Solid constitutes an environment built through technical specifications facilitating a decentralized web in which users have control of their data, stored in pods. These are defined as "secure web servers for data" [1]. The pod owner controls the people or applications which can access or interact with the pod. Solid pods can be self-hosted or managed by a Pod Provider. Different legal frameworks apply if the pod owner is an individual acting on its own behalf, a business, or a public entity. The scope of this paper is constrained to individual pod owners (a person or data subject acting in a personal capacity) hosted by Pod Providers. This is the most viable option for individuals lacking programming knowledge to enter the Solid environment.

3. Solid and statutory data sharing

Empirical research shows that companies do not have a distinguishable incentive to transfer the data they hold [3]. Instead, the opposite occurs. If data sharing could harm a given competitive advantage, the business, generally driven by its commercial interests [4], is incentivized to hinder access to such data [3]. Even if the company cannot currently identify harm from sharing given datasets, the potential for future loss of a not yet identified strategic advantage can be sufficient to exclude enabling data sharing [3]. To tackle this phenomenon, the EU is increasing statutory data sharing. The Solid environment is a technical solution businesses can adopt to fulfil these mandatory obligations. This section highlights the opportunities for the Solid environment in light of several new mandatory data sharing obligations under the DA, particularly within the Internet of Things (IoT), Data Processing Service Providers (DPSPs), and data spaces.

3.1. Mandatory Data Sharing & the IoTs

The triggering circumstance for this mandatory data sharing is the presence of a connected product or related service (Ch. 2 DA). These belong to the increasingly popular world of the IoT. In the context of the IoT, product data is the "data, generated by the use of a connected product, that the manufacturer designed to be retrievable" (art 2.15 DA), and related service data is any recorded "data representing the digitization of user actions or events related to the connected product […] generated during the provision of a related service" (art 2.16 DA). These terms are grouped as 'readily available data' when they are or can be retrieved "without disproportionate effort going beyond a simple operation" (art 2.17 DA). Figure 1 below exemplifies the data flow. The individual using the given connected product or related service has the right to receive or access many of these IoT data points.

Figure 1: Solid environment for compliance with IoT mandatory data sharing under the DA (transfer to the individual).

The individual can also choose to transfer this data from one business to a third party (art 5 DA), i.e., a Solid App. In this context, the Pod Provider can facilitate a more granular decision for the individual to specify the data types that should be transferred. The DA states that this transfer needs to be conducted (1) without undue delay, (2) free of charge to the user, and (3) where relevant and technically feasible, continuously and in real-time. The data received by Business B must be of the same quality as the data collected by Business A and have an easy-to-use, secure, comprehensive, structured, commonly used, and machine-readable format (art 5.1 DA). These obligations can be incorporated within the Solid specifications (Figure 2). This way, all these obligations are met by any apps within the Solid ecosystem.

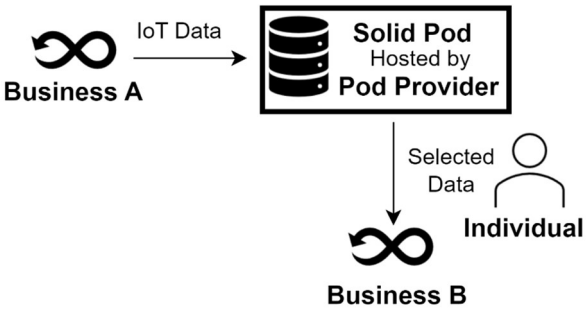

Figure 2: Solid environment for compliance with IoT mandatory data sharing under the DA (transfer to a third party).

Moreover, the granular decision-making by the individual in terms of which data is shared creates a clearer understanding of the data flow. This clarity can simplify the identification of unlawful data processing by Business B (art 6 DA), which would also benefit Business A and could act as an incentive for the Solid environment to flourish.

3.2. Data Processing Service Providers (DPSPs)

The DA also sets several obligations for DPSPs to facilitate switching among them (art 23 DA). DPSPs are entities delivering digital services to users, i.e. computing capabilities, such as the manipulation, storage, structuring, organizing, and analyzing of data (art 2.8 DA). Pod Providers are a type of DPSPs. According to the Solid technical specifications, Solid Pod Providers already meet the interoperability requirements to facilitate switching under the DA (art 30). Thus, if non-Solid DPSPs adopt Solid specifications, they would comply, by definition, with this DA obligation. However, the Solid environment sets much more stringent criteria for interoperability than mandatory DA conditions. For example, under the DA, interoperability is compulsory only for the same type of DPSPs (not all), and only if technically feasible (art 35 DA). Therefore, it is unlikely that businesses that want to disincentivize customers from using their data across different DPSPs will adopt Solid specifications. However, the gradual withdrawal of permitted switching charges, no longer allowed from 12 January 2027 (art 29 DA), may make Solid increasingly appealing over time for DPSPs, as Solid DPSPs would not need to devise new costly technical solutions to facilitate switching. Moreover, in enabling the simultaneous use of more than one DPSP (art 34 DA), the Solid architecture can be advantageous (Figure 3).

Figure 3: Solid environment for compliance with the DA's DPSPs mandatory data sharing.

3.3. Common European Data Spaces

The DA sets forth the interoperability requirements for participants in Common European Data Spaces (art 33 DA). A solid environment can enable companies to meet these interoperability requirements. However, this will require aligning the Solid specification to the requirements currently being developed for the different data spaces. The Solid pod architecture may be particularly useful for creating "cross-sectoral interoperable frameworks" (art 33.1 DA) to preserve the individual's choice in deciding which data can be used for what.

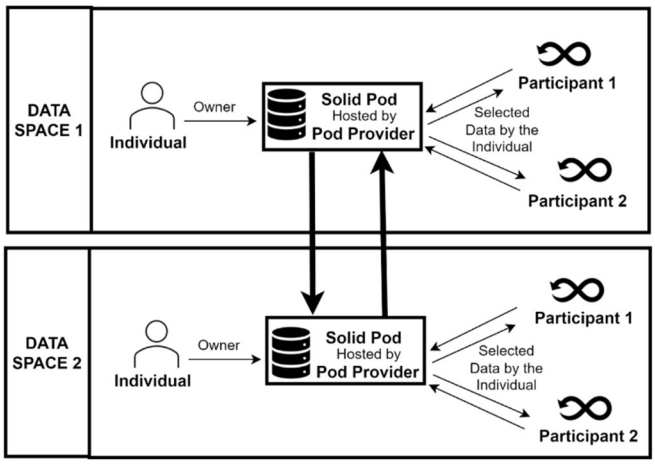

Figure 4: Solid environment for compliance with data spaces mandatory data sharing under the DA.

4. Misalignments of current Solid specifications and the EU statutory data sharing requirements

The Solid Protocol indicates that Solid pursues individuals to "maintain their autonomy, control their data and privacy, and choose applications and services to fulfil their needs" [5]. This goal aligns with the GDPR. However, making Solid-compliant solutions does not equate by default to EU-law-compliant solutions. Moreover, with the growing number of sector-specific or data space-specific data sharing frameworks, different technical specifications may be necessary for different contexts. To exemplify this issue, two specific misalignments of the Solid technical specifications with EU legal obligations are identified in the context of (3.1) Solid & the GDPR and (3.2) Solid data sharing & DA prohibitions. This is a non-exhaustive enumeration; many more misalignments could be noted.

4.1. Solid & GDPR misalignments

Solid pursues a decentralized web in which the individual controls their data. However, the technical solution in which Solid sets a user-centric control may cause issues when applying EU law. In the Solid environment, individuals choose the data they want to store in their pods and the access, use or write permissions they grant to other entities, such as Solid apps. Given the technical design of the Solid pod, Pod Providers and Solid Apps are likely to be considered data controllers. Pods are linked to an individual's WebID, one's "identity in the Solid ecosystem" [6]; thus, all the data held within one's Pod is personal data, regulated under the most stringent data protection regulations within the GDPR. As such, the Solid Apps receiving an individual's data hold legal responsibility to ensure that the data they receive is relevant and not excessive [7]. They are not supposed to accept or store "information [that] is not relevant with regard to the purpose of the new processing" [7], even if the individual decides to send this personal data to the Solid App. Similarly, Solid Apps are legally obliged to delete any unnecessary personal data they have received "as soon as possible" [7]. The mere hosting of excessive personal data is contrary to the GDPR.

4.2. Solid data sharing & DA prohibitions

The DA creates legal grounds prohibiting specific instances of data sharing. This is the case for gatekeepers, who cannot benefit from the DA, i.e. they cannot be data recipients (art 5.3 DA). Businesses designated as gatekeepers under the Digital Markets Act (DMA) have had, during a relevant period and for a foreseeable duration, a "significant impact on the internal market" and behave as a gateway for other businesses to carry out their operations (art 3.1.a DMA). This prohibition is unconditional and explicit. Therefore, the Solid technical specifications may need to be adapted to prevent gatekeepers from receiving or requesting data. Otherwise, the Solid specification would favor the breach of EU law.

Moreover, the DA sets a wide array of reasonable and nondiscriminatory terms and conditions that all mandatory data sharing must fulfil, as well as several assurances regarding liability and remedies (art 8 DA). These are aspects that the Solid specifications may need to incorporate to position themselves as abiding by EU law. The same can be said about the technical protection measures preventing unauthorized use or disclosure of the individual's data set by the DA (art. 11).

5. Reflection on Solid's future

The decentralized nature of the Solid environment may make the adaptation of Solid specifications for EU legal compliance difficult because of the lack of a central authority. This is especially true given the different data spaces that are being created in the EU, for which diverging legal or technical requirements may be adopted. To this end, different Solid branches may need to be created; that is, different Solid specifications, interoperable among one another, depending on the legal bases for the specific type of data sharing.

Nevertheless, few Pod Provider options currently exist for individuals. According to the Solid Website, most Pod Providers for individuals are presently prototypes. Inrupt pods are not usable, with its privacy policy stating that their pods are intended for research and that

users shall not use them to store personal data [8]. The same can be said for the Solid Community Prototype, which defines itself as "a fully functional server, but […without]" security or stability guarantees" [9]. The "teamid.live" Pod is also a prototype in an experimental phase [10], as is the case for Redpencilo Pods [11]. TrinPod may be the only one offering a "secure decentralized Solid compliant storage" [12]. However, it is based in the US, which creates additional legal requirements when servicing EU customers. The other pods enumerated in the Solid website (iGrant.io [13] and use.id[14]) seem to be designed for enterprises using Solid compliance digital services.

In 2021, Solid was described as being "in its infancy" [15]. This description still seems fitting. However, now is a prime time to develop the Solid environment. Solid can facilitate compliance with many new mandatory data sharing obligations set forth under the European Strategy for Data. This paper exemplifies some opportunities under the DA statutory data sharing obligations, but many more can be identified. Similarly, Solid is not a perfect fit for EU legal obligations. The technical versus legal misalignments need to be tackled for the adoption of Solid to flourish.

References

[1] 'Home' (Solid). URL: https://solidproject.org.

[2] H. Janssen, J. Cobbe, C. Norval, J. Singh, Decentralized Data Processing: Personal Data Stores and the GDPR, International Data Privacy Law 10 (2020) 356-384. doi: 10.1093/idpl/ipaa016.

[3] Deloitte and others, Study on Emerging Issues of Data Ownership, Interoperability, (Re-)Usability and Access to Data, and Liability: Final Report, European Commission, 2018. URL: https://data.europa.eu/doi/10.2759/781960

[4] Everis and others, Study on Data Sharing between Companies in Europe: Final Report, European Commission, 2018. URL: https://data.europa.eu/doi/10.2759/354943.

[5] Solid Protocol. URL: https://solidproject.org/TR/protocol.

[6] Get a Pod (Solid). URL: https://solidproject.org/users/get-a-pod.

[7] WP29, Guidelines on the Right to Data Portability (2017). URL: https://ec.europa.eu/newsroom/article29/items/611233.

[8] Inrupt Privacy Policy. URL: https://www.inrupt.com/privacy-policy.

[9] Solid Prototype. URL: https://solidcommunity.net.

[10] Teamid.Live. URL: https://teamid.live.

[11] Solid.Redpencil.Io. URL: https://solid.redpencil.io.

[12] TrinPodTM Server. URL: https://graphmetrix.com.

[13] iGrant.Io Data Pod. URL: https://igrant.io/datapod.html.

[14] use.id. URL: https://get.use.id.

[15] J. Krämer, P. Senellart, A. De Streel, Making Data Portability More Effective for the Digital Economy, Cerre, 2020. doi: 10.2139/ssrn.3866495