

# Streamlining governmental processes by putting citizens in control of their personal data

Raf Buyle<sup>1</sup> , Ruben Taelman<sup>1</sup>, Katrien Mostaert<sup>2</sup>, Geroen Joris<sup>2</sup>, Erik Mannens<sup>1</sup>,  
Ruben Verborgh<sup>1</sup> and Tim Berners-Lee<sup>3</sup>

<sup>1</sup> imec IDLab - Ghent University, Ghent, Belgium  
raf.buyle@ugent.be

<sup>2</sup> Informatie Vlaanderen, Flemish Government, Brussels, Belgium

<sup>3</sup> Department of Computer Science - University of Oxford, Oxford, UK

**Abstract.** Governments typically store large amounts of personal information on their citizens, such as a home address, marital status, and occupation, to offer public services. Because governments consist of various governmental agencies, multiple copies of this data often exist. This raises concerns regarding data consistency, privacy, and access control, especially under recent legal frameworks such as GDPR. To solve these problems, and to give citizens true control over their data, we explore an approach using the decentralised Solid ecosystem, which enables citizens to maintain their data in personal data pods. We have applied this approach to two high-impact use cases, where citizen information is stored in personal data pods, and both public and private organisations are selectively granted access. Our findings indicate that Solid allows reshaping the relationship between citizens, their personal data, and the applications they use in the public and private sector. We strongly believe that the insights from this Flemish Solid Pilot can speed up the process for public administrations and private organisations that want to put the users in control of their data.

**Keywords:** Personal data, decentralisation, GDPR, Solid, Linked Data.

## 1 Introduction

With the introduction of the General Data Protection Regulation (GDPR), the European Commission has provided a legal framework that aims to empower individuals in taking control of their personal information [10]. Such control is not necessarily a disadvantage to parties processing personal information: when used properly, GDPR can actually facilitate data flows that used to be much more complicated. GDPR, however, is mostly known for its complex legal effects on European companies dealing with large-scale personal data and may cost them significant resources in order to achieve and maintain legal compatibility. While international and multinational companies also have to respect GDPR rights for European data subjects, even when they do not have a physical European presence, several large players are—to put it light-

ly—slow with a correct adoption of GDPR. This has created a perverse reverse effect, where European companies that try to respect GDPR become less preferred as business partners, losing revenue to non-European companies that are more “relaxed” with GDPR adoption [14].

Not all organisations that are subject to GDPR have questionable or malicious intent: some of them experience genuine difficulties in trying to adhere to the legal obligations. This is definitely the case for local, regional and national governments, which need personal data to provide the services their citizens require. Governmental structures consist of multiple layers, and every layer consists of its agencies with their own data needs and processes that have grown historically. As a result, citizen data is spread across many places in many copies, leading to complex legal questions as well as numerous inconsistencies and repeated requests for data that is already present in other government administrations. These governments are a demanding party for a legally compliant technical solution to simplify all of their data needs.

The majority of data processes at the government level nowadays essentially aim to tackle the problem of how to move data as frictionless as possible from point A to B. Not only does this create a lot of technical challenges between the many different points, it also becomes a complex legal matter when a governmental “data train” needs to pass by stations A, B, C, and D, where B and C are not legally allowed to see all of the data that A and D can. As such, complex processes exist to verify precisely what the access rights of B and C are, and to then reintegrate their results when pushing the data to D. A telling example is a low-emission zone (LEZ) in which certain vehicles are not allowed in a city centre, or only under certain conditions, because they emit too many harmful substances. In Flanders, a vehicle is linked to a natural person. When entering a LEZ, federal information linking the license plate to the owner is combined with regional data indicating whether a person has a disability; finally the data is processed and the decision whether the vehicle is allowed is passed on to the city.

The Solid ecosystem [2, 15, 21] provides an answer by proposing a personal data pod for every citizen, such that all of their public and private data remains in one place. Instead of moving data between A and D, each of the agencies asks for permission to view a highly specific part of the data. That way, data does not have to be moved around, and GDPR compliance can be assessed automatically for every single data request. Control over personal data in our online and offline lives is a trending topic and therefore researched intensely [7, 16, 17, 19, 20, 22, 23, 26]. The key concept is that people can choose where they store their personal data, which build upon the principles of decentralisation. Blockchain is regularly referred to in this context as a solution for the management of personal data [7, 26]. Blockchain is a way for different parties who do not know each other to come to an agreement without the need for a referee or a trusted third party. This principle is essential, for example, for organising payments without a central bank or central manager, as the decentralised digital currency Bitcoin does [5]. Blockchains replicate data across many nodes. However, often, initiatives use Blockchain when this trusted third party is not required at all. If you have a central player or if the different parties trust each other, then you don't need a blockchain. Also, the immutability character of Blockchain,

which implies that data cannot be deleted, might be a challenge in the context of article 17 of the GDPR that gives people the right to erase their personal data [7, 8]

In this article, we explore the perspectives of control over personal data, and discuss two particular use cases that we have implemented using Solid. Solid provides a Web-based ecosystem that builds upon open standards and conventions [24]. According to Harrison, Pardo & Cook [12] an ecosystem is a metaphor often used to “convey a sense of the interdependent social systems of actors, organisations, material infrastructures, and symbolic resources that must be created in technology-enabled, information-intensive social systems” [p. 900]. A telling example of digital ecosystems are open data ecosystems [25]. Open Data refers to the obligation of the government to make their non-privacy-sensitive and non-confidential data freely available on the Web [13]. The open data reusers depend on the data and metadata from the data providers, while the providers depend on the feedback of the reusers to increase the data quality [18, 25]. Albeit all the actors in the open data ecosystem are interdependent to develop their business efficiently and effectively, public administrations and policy-makers are in the best position to bootstrap these open government ecosystems [12]. Zuiderwijk, Janssen & Davis state that the open data ecosystem challenges are related to “policy, licenses, technology, financing, organisation, culture, and legal frameworks and are influenced by ICT infrastructures” [25]. The challenges of open data ecosystems, which rewired the “one-way street” into a “bidirectional communication”, could be paralleled to the challenges to put the citizen in control of their personal data [12, 18]. By applying the Solid ecosystem approach to two high-impact use cases, the Flemish Government aims to build up the skills and capacity to put the citizen in control.

This article is further structured as follows. In the next section, we present the challenges that we aim to tackle. After that, we explain the basics around Solid in Section 3. Next, in Section 4, we discuss our approach for tackling the challenges using Solid, followed by a discussion of our implementation in Section 5. Finally, we conclude and present our lessons learned in Section 6.

## 2 Challenges

Local and regional governments in Flanders, the northern federated state of Belgium<sup>1</sup>, aim to empower citizens in reusing their personal information online in different contexts such as public services, banking, health insurance, and telecom providers. Governments are often the custodian of authoritative personal data, such as a domicile address or medical information, which are administered by public administrations in various information systems. Government administrations in Flanders share and reuse authoritative personal data between their various back-office applications to reduce the administrative burden for citizens [3], which is an implementation of the European

---

<sup>1</sup> <https://www.vlaanderen.be/en/discover-flanders>

‘once-only principle’<sup>2</sup>. However, public administrations are struggling to put the citizen in control.

A first challenge is that government administrations struggle to keep personal data such as email addresses, telephone numbers or bank account numbers up to date. As some citizens rarely have contact with their government, personal data is often outdated in the various information systems.

A second challenge concerns to allow citizens to reuse their data in a different context, such as a diploma when applying for a new job. The GDPR regulation 2016/679 states that “*In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.*” (European Commission, 2016, Article 43). To put it differently, the relationship between a government and a citizen is commonly considered as an imbalanced relationship, since the government wields more power than their citizens<sup>3</sup>. Therefore, a consent given by a citizen to reuse the authoritative data managed in government information systems in the private sector, cannot be considered as freely given [8, 9]. Sharing data between government administrations in Europe is not based on a given consent, but has a specific lawful basis.

Therefore, our main research question is: how governmental processes can be streamlined by putting citizens in control of their authoritative personal data, within the context of the GDPR regulation? This research question has two perspectives. On the one hand, how can citizens share their data with government administrations? On the other hand, how can citizens reuse their data stored in government information systems in a different context?

This project evaluates how the decentralised principles of Solid [2, 19, 21, 24] can tackle these hurdles. Solid is an ecosystem that enables individuals to store data in their data pods. This gives users true control over their data, as they can choose where their data resides, and who can access it. The outcome, based on the principles of Linked Data and decentralisation, is valuable for putting the user back in control with respect to public administrations and private organisations.

### 3 Solid

Solid [2] is a Web-based ecosystem that separates data from their applications, by providing people with their *personal data pod*, in which they can store data independently of the applications that they or others use to access that data. People can decide at a granular level which actors and applications can read from or write to

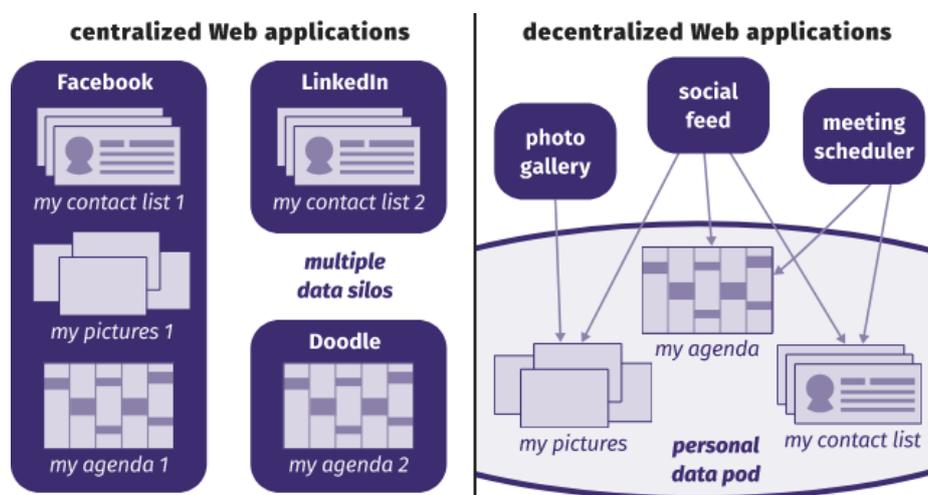
---

<sup>2</sup><https://ec.europa.eu/digital-single-market/en/news/ministerial-declaration-egovernment-tallinn-declaration>

<sup>3</sup> [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-my-employer-require-me-give-my-consent-use-my-personal-data\\_en#references](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-my-employer-require-me-give-my-consent-use-my-personal-data_en#references)

specific parts of their data. The contrast with current application architectures is illustrated in Figure. 1: instead of depending on a few applications that act as a gatekeeper of the data of large groups of people, the citizen is put in control of their personal data. Applications need to request access from the citizen in order to be able to operate on their data.

Importantly, Solid is not an application or platform, but a protocol: a collection of open standards and conventions. It builds upon existing Web standards, including the Linked Data stack [2], which can be implemented by anyone.



**Fig. 1.** Current applications are a combination of app and data. Thereby, the app becomes a centralisation point, as all interactions with that data have to go through the app. By introducing the concept of a personal data pod, Solid pushes data out of applications, such that the same data can be managed with different applications. This removes the dependency on a centralised application, as data can be stored independently in a location of the citizen's choice.

A data pod is a personal storage space that can exist anywhere on the Web, such as on your server, a shared community server, or a government-provided storage space. Within this data pod, the owner has full permissions regarding data creation, editing, and control management. The owner can decide to give specific permissions to other people, such as allowing family members to see their holiday pictures or allowing colleagues to read conference notes. Also, people, organisations and applications can post a request to the public inbox of a pod to gain access to personal data. Within Solid, people have at least one data pod for themselves, but they can additionally have multiple other pods, for instance, for home data, work data, medical data, etc.

Whereas typical centralised applications require users to store their data within the application, Solid turns this around by making data personal and allows users to use any application on top of their data after granting explicit access. While simple applications work with just a single data pod, the real power of Solid becomes clear when applications *combine data* from multiple data pods, giving way to *decentralised ap-*

*plications*. For example, social network applications on Solid can store personal information such as posts, friends, comments, and likes in a personal data pod, while their visualisation will require combining data across different data pods. This solves two essential problems. First, data no longer needs to be *copied* in different applications, since applications will point to the single copy. Second, as a consequence thereof, synchronisation problems no longer occur: because there is only one copy of the data, applications can no longer have inconsistent versions of data.

Solid enables several capabilities that are typically missing in the current centralised Web applications:

- **Independent identity:** people choose how they are identified and where their identity resides. In Solid, a personal identifier (WebID) is a URL<sup>4</sup>.
- **Control over data:** people can grant and revoke fine-grained access permissions to specific parts of their data.
- **Choice of application:** the danger of vendor lock-in is avoided as data can flexibly be used by different applications.

For our purposes, Solid solves the aforementioned “data train” problem, precisely because data does not move anymore between different government agencies. Instead, each government agency goes directly to the original source of the data, which is the data pod of the citizen. This addressed the problem of multiple copies and synchronisation, as well as the GDPR question of which agency has the right to access what data attributes of a citizen since each agency makes an individual request to the data pod. As such, the many processes focused on transporting data from one hop to the next, will be refocused on reading and writing data from a pod.

---

<sup>4</sup> Solid uses the WebID-OIDC specification for authentication:  
<https://github.com/solid/webid-oidc-spec>

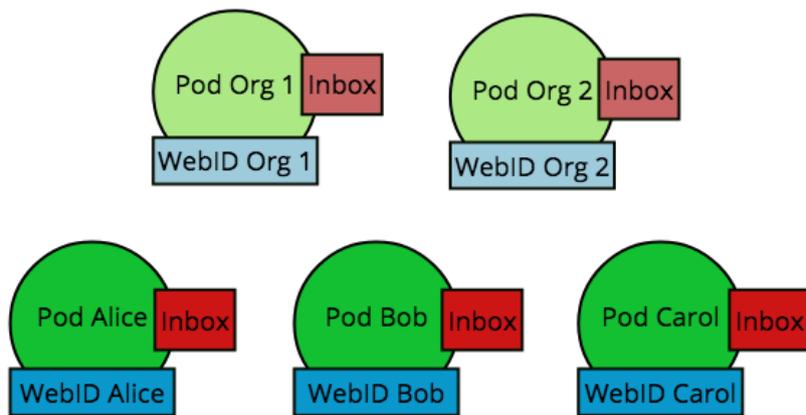
## 4 Approach: exchanging personal information using Solid

In this section, we explain our approach for allowing citizens to share information with their government and vice versa using Solid. We first start by explaining the requirements of this approach. After that, we discuss two real-world scenarios that make use of this approach: (1) citizens sharing data, such as contact preferences (e.g. email address, telephone number), stored in a pod and (2) reusing authoritative government data in the private sector, such as diplomas, where the citizen keeps the diploma that has been digitally signed by the university and the government holds an indelible copy.

### 4.1 Requirements

For our use cases, we assume that all citizens can be identified uniquely with a globally unique Uniform Resource Identifier (URI), referred to as a WebID<sup>5</sup>. This WebID points to a Linked Data document with more details about the citizen, in particular, a pointer to the personal data pod. Furthermore, we assume that all government departments and organisations have a WebID and data pod. An overview of the required components can be seen in Figure 2.

Typically, Solid data pods have a public inbox where anyone can post messages for the owner, where the messages can then only be read, modified, and removed by the owner. We assume this convention is met for all data pods, as we make use of this functionality for the communication between users.



**Fig. 2.** The required components for our use cases. All governmental organisations (first row), all citizens (second row) have a data pod, WebID, and inbox.

<sup>5</sup> <https://www.w3.org/wiki/WebID>

## 4.2 Use case: Citizens sharing personal information

The Flemish government has developed a digital assistant that offers an integrated user experience when citizens interact with the different government administrations. A telling example is to provide citizens with notifications regarding the status of their public service, via a preferred channel. As the majority of the citizens have few digital interactions with their government, compared to interactions with the private sector, contact information and information about their preferences are often outdated. Therefore the roles are swapped, and the citizen's pod becomes the source for primary contact information and preferences. This use case addresses the first challenge and avoids that users have to keep their data up-to-date in the various portals of public and private organisations, which has an impact on the timeliness of the data.

We use an email address to illustrate this use case, which applies to any personal information.

**Preconditions:** citizen Alice (A) can be identified uniquely by her WebID. Also, A has a personal online data store (pod), hosted on a Solid Server (S). Likewise, organisation (O) has a WebID and a pod.

**Use Case 1.1:** Share personal data. A authenticates to O, using secure delegated access. After successful authentication, A can grant O access to her email address by adding the WebID from O. O can read the email address from the pod after successful authentication. Extension: A can withdraw O the access to her email address.

**Use Case 1.2:** Manage personal data. A authenticates to her pod, using secure delegated access. After successful authentication, A can add her email address to her pod via a user interface. Extension: A can modify or delete her email address.

**Use Case 1.3:** Request access to personal data. O posts a request to the public inbox of A to gain access to the email address of A. After seeing this request, A grants O read access to her email address and send a notification to the public inbox of O. O receives the notification with a link to the original request. O can now read the email address from A.

## 4.3 Use case: Citizens sharing authoritative information

Governments aim to empower citizens to reuse their personal information, stored in authoritative data sources on different governmental levels. Telling examples are sharing a diploma when applying for a new Job as can be seen in Figure 3, or obtaining information about their income and government debts when applying for a loan. This use case evaluates a student that obtains a certificate from the university and addresses the second challenge. As a citizen cannot give the government consent to share their data with private partners, we put the user in control by storing the diplo-

ma in the citizens' pod. To put it differently, in the context of GDPR, the data subject becomes the controller of the data. This scenario indicates that Solid allows reshaping the relationship between citizens', their authoritative data and the applications they use in the public and private sector. If the citizen becomes an authentic source, legal agreements must be made to ensure that the authorities have easy access to the data. If the citizen refuses, the government can exercise this right as it does today in the tax context [1].

**Preconditions:** citizen Alice (A) can be identified uniquely by her WebID. Also, A has a pod, hosted on a Solid Server (S). Likewise, university (U) has a WebID and a pod. An employer (E) of A also has a WebID.

**Use Case 2.1:** registering as a student. A registers as a student at U, and has to provide her WebID. This will allow the university to send certificates after graduating.

**Use Case 2.2:** maintaining provenance until graduation. U maintains the whole provenance chain until the graduation of A. The provenance chain describes the history of a digital asset, in this case, a diploma, via a time-ordered sequence of provenance records. This includes all followed courses, grades, teachers, ... This information is not publically accessible, only A has read access to this.

**Use Case 2.3:** obtaining a certificate. A asks for a (summarised) copy of the certificate, so that she can share it with third parties. U will produce a summary of this certificate (not including the whole provenance chain), and send this to the inbox of A's data pod. This certificate is digitally signed by U using asymmetric encryption.

**Use Case 2.4:** sharing a diploma. Now that A has a copy of her diploma in her inbox, she can share it with anyone. For example, she can publish this on her data pod and give read access for her employer's WebID.

**Use Case 2.5:** checking the validity of a diploma. If E wants to check if the diploma of A is valid, E has to check the signature of U on this diploma. E does this by extracting the signature from the diploma, determining the authority (U). This can be done using existing document signing mechanisms, such as XAdES [4].

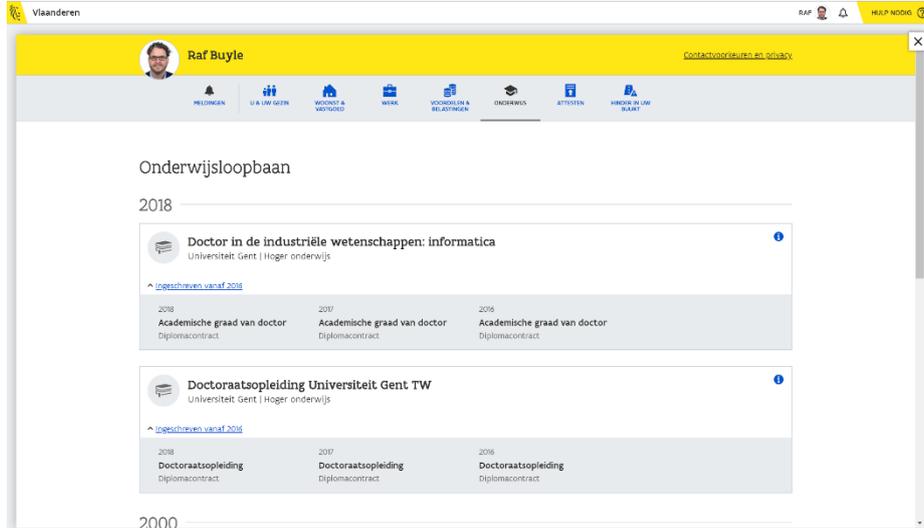


Fig. 3. Authoritative government data on diplomas, valuable for reuse in the private sector.

## 5 A digital assistant for Flemish citizens

In this section, we discuss the implementation of our approach into ‘Mijn Burgerprofiel’<sup>6</sup> (My Citizen Profile), which is a smart digital assistant for Flemish citizens [3] with an overview of all their authentic information and status information of their interactions with the government. The authentication method of My Citizen Profile depends on whether the citizen is using services that process information under GDPR. The European security standard<sup>7</sup> ‘electronic IDentification, Authentication and trust Services’ (eIDAS) defines a substantial degree of confidence in the claimed or asserted identity of a person to substantially decrease the risk of misuse or alteration of the identity<sup>8</sup>. Users can access personal data via the My Citizen Profile by using their Belgian electronic identity card via a smart card reader or via their mobile phone, with a SIM card and their installed itsme<sup>®</sup> application<sup>9</sup>.

As an example, we elaborate on the first use case that was discussed in the previous section, namely citizens sharing personal information (e.g., an email address). We leave the other use case as future work. As mentioned in section 3, Solid detaches application from data. As such, the implementation of our approach requires two components: (1) storage for data pods, and (2) an application for viewing and using relevant personal information. We discuss both components hereafter.

<sup>6</sup> <https://overheid.vlaanderen.be/mijn-burgerprofiel>

<sup>7</sup> <https://www.eid.as/home/>

<sup>8</sup> <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32014R0910>

<sup>9</sup> <https://www.itsme.be/en/security>

## 5.1 Storage for data pods.

For our implementation, we make use of the Node Solid Server (NSS)<sup>10</sup> (version 5.0.1) to create and host data pods. If the user already has a pod, this can be used to share personal information. NSS implements the required specifications to allow users to register for a WebID and data pod, after which the server hosts this data pod and allows interaction using the Web Access Control specification<sup>11</sup>. NSS allowed us to create Solid pods for any citizens and governmental organisations. As such, the government provides data pods for all citizens by default. However, if citizens desire more control over their pod, they can choose to host a data pod themselves, for example by running NSS privately on their server.

## 5.2 Application for interacting with personal information

In order to allow governmental organisations to request access to specific information of a citizen, or to view the actual information when access has been granted, we extended My Citizen Profile, where all Flemish citizens have a profile. Currently, this information is stored centrally within the databases of My Citizen Profile. For this work, we created a modified version of My Citizen Profile that instead stores information within the data pod of each citizen. The Flemish Government that hosts My Citizens Profile is a governmental organization, will also have one WebID, just like each citizen.

For our use case, we focus on storing the email address of a citizen. To achieve this, we implemented three components: a Solid linker, an email extractor, and an email visualizer. These components will be explained hereafter.

## 5.3 Solid linker

Within the profile settings of My Citizens Profile, we added a field where people can link their account with any Solid WebID, as can be seen in Figure 4. This involves logging in with any WebID via a pop-up window. By default, each profile is linked with the default government-provided WebID.

## 5.4 Email extractor

If a citizen has a valid Solid WebID linked to its My Citizens Profile account, the application can attempt to extract its email address by following the links to the file in its data pod that contains an email address. Based on a WebID, the email extractor component can determine the URL through which the file is available in the user's

---

<sup>10</sup> <https://www.npmjs.com/package/solid-server>

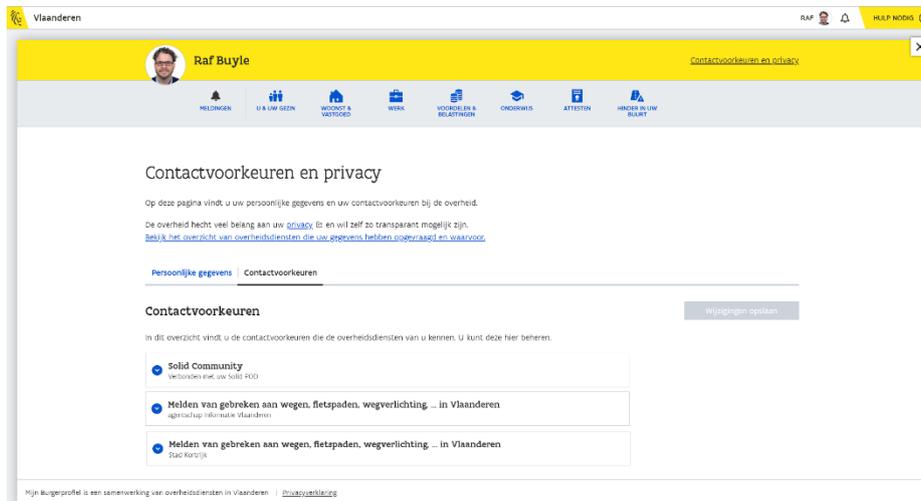
<sup>11</sup> <https://github.com/solid/web-access-control-spec>

data pod. With this URL, the extractor will perform an HTTP GET request, together with the authentication token of My Citizen Profile WebID.

If My Citizen Profile has been granted read-access to this file by the citizen, the content of this file will be returned; otherwise an authorisation error will be returned by the data pod of the citizen. If no errors were encountered, the email extractor component will return the discovered email address.

## 5.5 Email visualizer

On the personal My Citizen Profile overview page, a field is added that shows the email address of the user if this could be found. For this, the email extractor component is invoked based on the WebID that is linked to the current user. This information is always extracted on-the-fly, which means that this fact is never stored on any other location other than the citizen's data pod. This also means that when the citizen modifies the value, that My Citizen Profile, and any other authorised organizations, will be able to see the updated value immediately. This visualizer can be used in automated processes, such as sending reminders on, e.g., upcoming elections.



**Fig. 4.** The front-end design of the Digital Assistant, including the citizen's consent for reusing data from their personal data store.

## 6 Conclusions

In this paper, we presented insights on the implementation of Solid in the Region of Flanders. The Flemish government adapted the My Citizens Profile to be interoperable with the Solid ecosystem to put the citizen in control of their data. We addressed

two compelling challenges; firstly that government administrations struggle to keep personal data up to date, and secondly to allow citizens to reuse their data stored in government information systems in a different context. This initiative demonstrated that the Solid ecosystem provides an answer to the challenges by proposing personal data pod for every citizen, which enables them to share their data.

New avenues for future research include investigating methods to keep the most recent version of a (summarised) copy of the authoritative data, such as a domicile address, in the users' data pod. This should ensure that the information that is shared by citizens with the private sector is always up-to-date. Another obvious extension to this research is to inform the user with the nature of the given consent to reuse data from their pod, including: the identity of the reuser, the purpose, the fact that data only will be used for automated decision-making, and/or information whether the consent is related to an international transfer of data [6]. This concept is referred to as 'informed consent' and could be implemented as a set of templates in combination with the users' preferences, which should be exchanged through a standardised vocabulary [11]. Also, all actions should be logged transparently in the pod, including access to data, data modifications, giving consent and revoking of the rights, comparable to expenses on our bank account [24]. This fine-grained and structured log can also be used to detect anomalies and data breaches by using machine learning algorithms. To complete, future research should certainly focus on the different challenges of open government ecosystems applied to the Solid ecosystem, more specific on policy, the role of the different actors and sustainable economic models.

Solid builds upon existing Web standards and methods such as Linked Data and decentralisation, therefore Solid can be seen as process innovation rather than technological innovation. As the Flemish My Citizen Profile also builds upon Web standards, including the Linked Data stack, integration with Solid pods was straightforward. We have used an email address to illustrate this case, but the intention is to broaden this to all personal data. The right as a citizen to have control over personal data could be paralleled with other basic needs. However, it is a challenge to ensure that people have at least one data pod. The Flemish Government provides a guaranteed, uninterrupted and minimal supply of electricity, gas and water for household use<sup>12</sup>. This principle could be extended by offering the citizens a free amount of data storage at a supplier of their choice.

We expect that the insights from this Flemish Solid Pilot can speed up the process in public administrations and private organisations that face the same complexity when trying to put the user back in control.

---

<sup>12</sup> <https://www.vlaanderen.be/vlaamse-overheid/persberichten/recht-op-minimumlevering-elektriciteit-gas-en-water>

## References

1. Belgisch Staatsblad. Wijzigingen met betrekking tot de onderzoeksmiddelen van de administratie. (2011). [http://www.ejustice.just.fgov.be/cgi\\_loi/change\\_lg.pl?language=nl&la=N&table\\_name=wet&cn=2011041406](http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=2011041406) Accessed 9 July 2019
2. Berners-Lee, T.; Verborgh, R. Welcome to Solid. (2019). <https://rubenverborgh.github.io/Solid-DeSemWeb-2018/#title> Accessed 9 July 2019
3. Buyle, R., Van Compernelle, M., De Paepe, D., Scheerlinck, J., Mechant, P., Mannens, E., & Vanlিশhout, Z. Semantics in the wild: a digital assistant for Flemish citizens. In Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance (pp. 1-6). ACM (2018). doi: <https://doi.org/10.1145/3209415.3209421>
4. Cruellas, J. C., Karlinger, G., Pinkas, D., & Ross, J. Xml advanced electronic signatures (xades). W3C Recommendation (2003). <http://www.w3.org/TR/XAdES> Accessed 9 July 2019
5. Decker, C., & Wattenhofer, R. (2013, September). Information propagation in the bitcoin network. In IEEE P2P 2013 Proceedings (pp. 1-10). IEEE.
6. de Montjoye, Y. A., Wang, S. S., Pentland, A., Anh, D. T. T., & Datta, A. On the Trusted Use of Large-Scale Personal Data. *IEEE Data Eng. Bull.*, **35**(4), 5-8 (2012)
7. Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy?. *IEEE Cloud Computing*, **5**(1), 31-37.
8. European Commission. 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. *Official Journal of the European Union (OJ)*, **59**(1-88), 294 (2016)
9. European Commission. Guidelines on Consent under Regulation 2016/679 Luxembourg: Publications Office (2018) [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=623051](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051) Accessed 9 July 2019
10. European Commission. It's your data – take control. Luxembourg: Publications Office (2018). [https://ec.europa.eu/commission/sites/beta-political/files/data-protection-overview-citizens\\_en.pdf](https://ec.europa.eu/commission/sites/beta-political/files/data-protection-overview-citizens_en.pdf) Accessed 9 July 2019
11. Fatema, K., Hadziselimovic, E., Pandit, H. J., Debruyne, C., Lewis, D., & O'Sullivan, D. Compliance through Informed Consent: Semantic Based Consent Permission and Data Management Model. In Proceedings of the 5th Workshop on Society, Privacy and the Semantic Web - Policy and Technology (PrivOn2017), Vienna, Austria (2017)
12. Harrison, T. M., Pardo, T. A., & Cook, M. Creating open government ecosystems: A research and development agenda. *Future Internet*, **4**(4), 900-928. MDPI AG (2012). doi: <https://doi.org/10.3390/fi4040900>
13. Janssen, M., Charalabidis, Y., & Zuiderwijk, A. Benefits, adoption barriers and myths of open data and open government. *Information systems management*, **29**(4), 258-268 (2012). doi: <https://doi.org/10.1080/10580530.2012.716740>
14. Jia, J., Jin, G. Z., & Wagman, L. The short-run effects of GDPR on technology venture investment (No. w25248). National Bureau of Economic Research (2018). doi: [10.3386/w25248](https://doi.org/10.3386/w25248)
15. Mansour, E., Sambra, A. V., Hawke, S., Zereba, M., Capadisli, S., Ghanem, A., ... & Berners-Lee, T. A demonstration of the solid platform for social web applications. In Proceedings of the 25th International Conference Companion on World Wide Web (pp. 223-

- 226). International World Wide Web Conferences Steering Committee (2016). doi: <https://doi.org/10.1145/2872518.2890529>
16. Mun, M., Hao, S., Mishra, N., Shilton, K., Burke, J., Estrin, D., ... & Govindan, R. Personal data vaults: a locus of control for personal data streams. In Proceedings of the 6th International Conference on Emerging Networking Experiments and Technologies (p. 17). ACM (2010). doi: <https://doi.org/10.1145/1921168.1921191>
  17. Narayanan, A., Toubiana, V., Barocas, S., Nissenbaum, H., & Boneh, D. A critical look at decentralized personal data architectures. arXiv preprint arXiv:1202.4503 (2012)
  18. Pollock, R. (2011, March 11). Building the (Open) Data Ecosystem. <http://blog.okfn.org/2011/03/31/building-the-open-data-ecosystem/> Accessed 9 July 2019
  19. Solid. Welcome to Solid (2019). <https://solid.inrupt.com/> Accessed 9 July 2019
  20. Van Kleek, M., & OHara, K. The future of social is personal: The potential of the personal data store. In Social Collective Intelligence (pp. 125-158). Springer, Cham (2014)
  21. Verborgh, R. Ruben Verborgh on data & privacy. Imec Magazine (2019). <https://www.imec-int.com/en/imec-magazine/imec-magazine-january-2019/back-to-the-future-how-we-will-regain-control-of-our-personal-data> Accessed 9 July 2019
  22. Vescovi, M., Perentis, C., Leonardi, C., Lepri, B., & Moiso, C. My data store: toward user awareness and control on personal data. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (pp. 179-182). ACM (2014). doi: <http://dx.doi.org/10.1145/2638728.2638745>
  23. Whitley, E. A. Informational privacy, consent and the “control” of personal data. Information security technical report, **14**(3), 154-159 (2009). doi: <https://doi.org/10.1016/j.istr.2009.10.001>
  24. Yeung, C. M. A., Liccardi, I., Lu, K., Seneviratne, O., & Berners-Lee, T. Decentralization: The future of online social networking. In W3C Workshop on the Future of Social Networking Position Papers (Vol. 2, pp. 2-7) (2009)
  25. Zuiderwijk, A., Janssen, M., & Davis, C. Innovation with open data: Essential elements of open data ecosystems. Information Polity, **19**(1, 2), 17-33 (2014)
  26. Zyskind, G., & Nathan, O. Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE (2015). doi: [0.1109/SPW.2015.27](https://doi.org/10.1109/SPW.2015.27)