ISSN 1831-9424

European Commission

The landscape of consent management tools – a data altruism perspective

Lähteenoja, V., Himanen, J., Turpeinen, M., Signorelli, S.

2024

Joint Research Centre

EUR 40084

Contact information

Name: Alexander KOTSEV
Address: Via E. Fermi 2749, 21027 Ispra (VA) – Italy
Email: Alexander.KOTSEV@ec.europa.eu

Name: Serena SIGNORELLI
Address: Via E. Fermi 2749, 21027 Ispra (VA) – Italy
Email: Serena.SIGNORELLI@ec.europa.eu

EU Science Hub

https://joint-research-centre.ec.europa.eu

JRC137572

EUR 40084

PDF ISBN 978-92-68-21145-8 ISSN 1831-9424 doi:10.2760/0852673 KJ-01-24-089-EN-N

Luxembourg: Publications Office of the European Union, 2024

How to cite this report: European Commission, Joint Research Centre, Lähteenoja, V., Himanen, J., Turpeinen, M., and Signorelli, S. *The landscape of consent management tools - a data altruism perspective.* Publications Office of the European Union, Luxembourg, 2024, doi:10.2760/0852673, JRC137572.

Layout: Carmen Capote de la Calle

The landscape of consent management tools – a data altruism perspective

Lähteenoja, V., Himanen, J., Turpeinen, M., Signorelli, S.

2024

Contents

Abstract

The report discusses the landscape of consent management tools, with a focus on the specific needs of Registered Data Altruism Organisations (RDAOs). The study is aimed at policymakers that may want to develop or procure consent management digital tools to enable data altruism, as well as at current and/or aspiring RDAOs that may want to learn about the typologies of solutions available on the market. The study categorizes the solutions into two types: consent-focused and consent-included, and further identifies eight distinct patterns of consent management solution offerings currently on the market. Each pattern is evaluated on its suitability for RDAOs through a number of factors such as maturity, modularity, technical complexity, scalability, and comprehensiveness. A long list of 170 potential digital consent solutions identified is provided in Annex 1. The report concludes that there exist digital consent solutions on the market that could be relatively easily adopted by RDAOs and serve their core needs of consent management. Specifically, it recommends solutions that follow the 'core' consent management pattern, which focus exclusively on consent management and are flexible enough to cater to the diverse needs of RDAOs.

AUTHORS

- **Lähteenoja Viivi** – 1001 Lakes OY
- **Himanen, Joel** – 1001 Lakes OY
- **Turpeinen, Marko** – 1001 Lakes OY
- **Signorelli, Serena** – European Commission, Joint Research Centre (JRC)

1. Introduction

The sharing of data presents a huge potential for economy and society: it can enable new products and services based on novel technologies, make production more efficient, and provide tools for combatting societal challenges. One of the mechanisms that can increase the sharing of data is data altruism, intended as the willingness of individuals and companies in giving their consent or permission to make available data that they generate – voluntarily and without reward – to be used in the public interest.

The European Strategy for data [1], and the Data Governance Act (DGA) [2], among other goals, aims to foster data altruism (intended in the DGA as 'the voluntary sharing of data [...] without seeking or receiving a reward [...] for objectives of general interest' Art. 2(16)) by introducing a framework for 'data altruism organisations recognised in the Union' and mandating the creation of a European data altruism consent form.

In particular, Chapter IV of the DGA is dedicated to organisations establishing data altruism initiatives of various kinds, which will have the possibility to register as 'data altruism organisations recognised in the Union' or Registered Data Altruism Organisations (RDAOs). RDAOs must be not-for-profit entities and their registration under the DGA is voluntary. Only organisations that meet a set of transparency requirements (Art. 20), that offer specific safeguards to protect the rights and interests of individuals and companies who share their data (Art. 21), and that comply with a future data altruism rulebook (Art. 22 and Delegated Act) once adopted will be able to register as RDAOs. A European data altruism consent form (Art. 25) will be adopted to allow the collection of consent or permission across Member States in a uniform format.

As data altruism is consent-based and as individuals increasingly expect digital solutions for processes, consenting the use of personal data for objectives of general interest on the basis of altruistic motivations should also be possible through a digital process. The 'European data altruism consent form' should thus be 'digital by design'. Such a digital solution should also allow for receiving and withdrawing consent, meant in the GDPR [3] sense as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her' (Art. 4).

The purpose of this report is to support data altruism organisations on the adoption of digital solutions for consent management. Currently, there exists no standard digital solution for the implementation of consent management in general, nor is there one specifically for consent in the context of data altruism.

The current study is a joint collaboration between the Joint Research Centre of the European Commission and 1001 Lakes, in the context of an Administrative Agreement of the former with the Directorate-General for Communications Networks, Content and Technology (CNECT) entitled 'Data Sharing: Economic, Technological and Societal dimensions (DataSETS)'.

The aim is to offer a bird's-eye view on what is currently available on the market to aspiring and existing data altruism organisations, in

order for them to understand their needs and to identify the best solution suitable for their activities. The intention of the study is not to evaluate the utility of the identified consent management tools in general and the European Commission has neither the mandate, nor the ambition to do so.

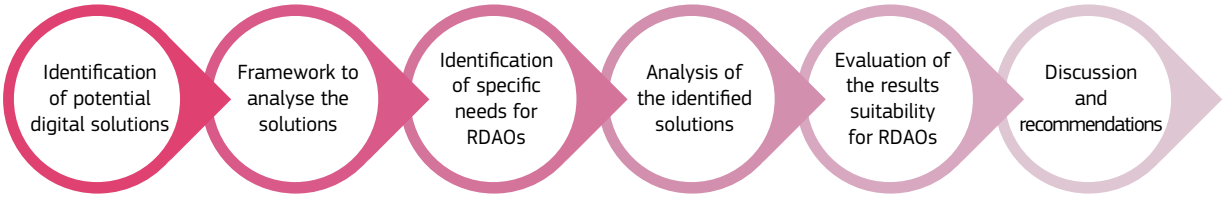
The intended audience for this report is twofold: policymakers and current and/or aspiring RDAOs. Policymakers may be interested in getting to know the consent management digital solutions available on the market for possible use by data altruism organisations, with the aim of knowing the landscape and to possibly intervene with the direct development of a digital tool or the procurement of one. Current and/or aspiring RDAOs may be interested in getting to know the specific needs that RDAOs have and decide which the typology that better suits their needs is.

This report begins with a detailed description of the methodology and steps taken to reach the objectives of the study (Section 2). It then presents summary data on and brief discussions of 170 identified potential consent management solutions in terms of their provider types, geographical spread, and operational status to illustrate that there is a sizable and varied landscape of solutions on the market or being developed currently (Section 3). Then, to help make sense of this mass and variety of solutions, an analysis framework of consent solutions in general is described together with an anticipated set of features especially relevant for RDAOs (Section 4). Next, what is needed for the management of consent in the specific case of RDAO is introduced (Section 5), followed by a typology of consent solutions deriving from the application of the analysis framework, each type discussed in terms of how suitable solutions of that pattern might be for RDAOs (Section 6). Finally, the findings of the study are briefly discussed in light of the overarching research question and recommendations are offered (Section 7). Appended to this report is the full identified list of solutions and their providers (Annex 1).

2. Study approach

This study was conducted using a mix of desk research, qualitative interviews and expert analysis. It consisted of the six steps summarised in Figure 1 that will be deepened in dedicated sections of the report:

FIGURE 1. Methodology steps.



Source: authors' elaboration

1. **Casting a wide net to identify as many digital solutions as possible that could potentially be used for consent management in general.** In this desk research phase, a long list of 170 solutions (Annex 1) was compiled using data from Langford et al. [4], the list of MyData operator awardees from 2020-2023 [5] and additional research. This simple list of solutions was enriched with some additional information[1] (like website, type of provider, etc.) and each solution was further analysed in terms of their operational status and assigned one of the labels 'operational', 'idle', 'defunct', or 'no data'. This analysis resulted in 134 operational organisations or solutions. A summary and short discussion of the results are presented in Section 3.
2. **Developing a framework for analysing these solutions for their suitability for consent management in general.**

A series of qualitative interviews were conducted with seven solution providers. These interviews focused on four themes that were anticipated in order to be common to all relevant consent solutions, namely:

a. compatibility with EUDI [6] wallets;
b. ability to handle dynamic consent;
c. ability to handle consents about sensitive data (in the sense of Article 9 of the GDPR [3]);
d. the relevant technical standards used, if any.

Also, three different scenarios for data altruism were discussed from the solution provider's point of view:

- Scenario 1. **One-to-one consent relationships**, where a data subject gives both consent and data to a requesting party that then collects the data from the data subject.
- Scenario 2. **Three-party situations**, where a data subject gives only consent to a requesting party, which party then collects the data

1. Solution website, solution provider name, provider website, provider type ('company', 'research institute', 'project', 'non-profit', 'public entity'), and provider domicile country.

consented, with proof of consent, from its present controller (and not directly from the data subject themselves).

- Scenario 3. **One-to-many consent relationships**, where a data subject gives both consent and data to a requesting party who is a data altruism organisation, which party further gives data and proof of consent to additional requesting parties, such as research organisations.

The interviews[2] were conducted as 45–60-minute online meetings and served primarily the purpose of understanding, first, if there existed some standard functional workflow for consent management and, second, if there were no such commonly used models, what elements would one look like and contain. The results of these interviews, in the shape of an analysis framework for digital consent solutions, are described in Section 4.

3. **Identifying and hypothesising the more specific needs of RDAOs.** An additional qualitative interview was conducted with an existing RDAO, DATALOG[3], to understand their current practices of managing consents. As these were found to be non-digital, a set of hypothetical considerations were developed for future RDAOs requiring a digital solution. An initial set of considerations was developed to determine whether a digital consent solution was relevant for RDAOs at all, and a further set of considerations was added of especially desirable features for a consent solution for RDAOs. These sets of considerations are described in Section 5.

4. **Conducting analysis of identified solutions based on the framework and anticipated specific needs and clustering them in typical patterns that different solutions may follow.** The 134 operational solutions identified in step 1 were further analysed in terms of meeting the basic considerations for relevance to RDAOs. This analysis resulted in each solution being assigned one of the labels 'relevant', 'unsure' (for some idle solutions), 'not relevant' ('N/A' was assigned to all defunct solutions or solutions with no data on their operational status) and yielded 70 solutions labelled as 'relevant'. 20 of these relevant solutions were subjected to more detailed study. Based on this and the previous steps, it was possible to identify and describe different though partially overlapping types or patterns that consent solutions tend to fall into or follow. These descriptions are included in Section 6.

5. **Evaluating the resulting patterns for their suitability for RDAOs.** The patterns identified in the previous steps were further analysed in terms of the desired features of RDAOs identified in step 3. The results of these evaluations are included in the pattern descriptions in Section 6.

6. **Discussing and providing recommendations based on this study as a whole.** Finally, the findings from the above research are discussed in terms of the overarching research question of whether there exist digital consent solutions currently on the market that could be easily adopted by and serve the needs of RDAOs. Based on this summary discussion, recommendations are offered that are presented in Section 7 of this report.

2. The processing of personal data in the context of this report was conducted in accordance with Regulation (EU) 2018/1725 and is described in the data protection record DPR-EC-01011, available at: https://ec.europa.eu/dpo-register/detail/DPR-EC-01011.

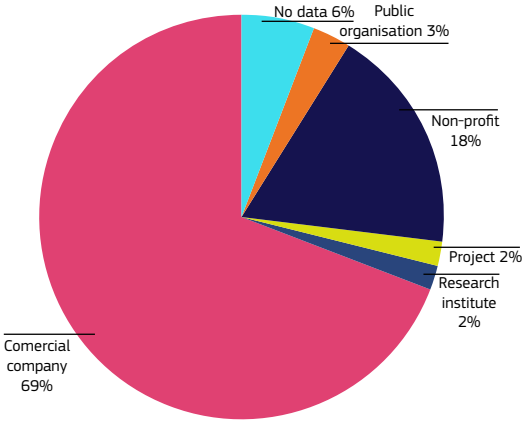
3. https://datalog.es/

3. Identification of potential digital solutions for consent management

The first step of our methodology consists into the identification of existing digital solutions currently on the market for consent management in general. Before delving into the specific available solutions for data altruism organisations, it is necessary to chart whether there is a market for digital consent solutions at all, and if there is, who is part of it. For this purpose, we cast a wide net to identify as many digital solutions as possible that could potentially be used for consent management in general. In the end, a long list of 170 potential digital consent solutions (available in Annex 1) was collected and analysed in terms of their provider types, domicile countries, and current operational status. This section provides some summary data on the collected list of solutions to give the reader an idea of the potential market.

As shown in Figure 2, a great majority (69%) of the 170 identified solutions are offered by **commercial companies**. Due to the limited scope of this study, other types of providers may exist in greater numbers than identified here. However, it can be argued that the most marketed solutions, and thereby the easiest to identify, are provided by private companies. Arguably, the role of the compliance requirements imposed by the GDPR [3], and the market sensing an opportunity to fill it, will have had a nontrivial effect on this aspect of these findings.

FIGURE 2. Potential solutions breakdown by type of provider.

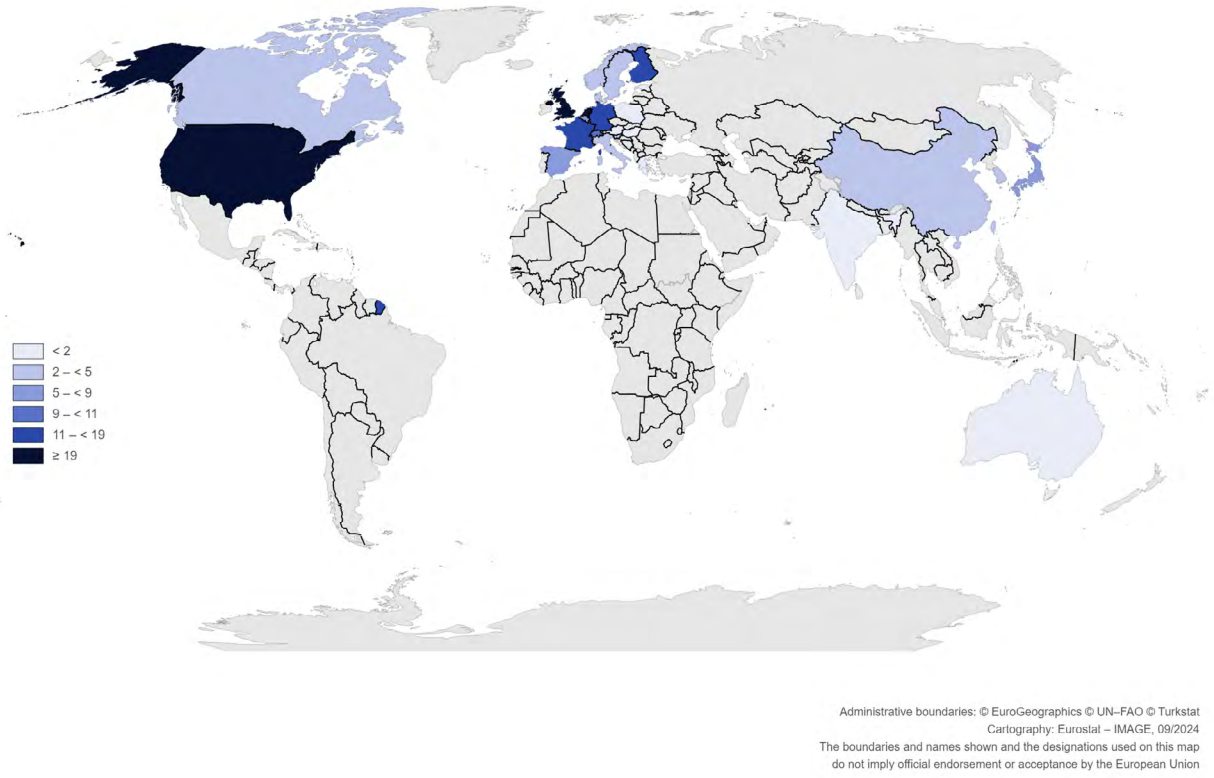


Source: authors' elaboration

Looking at the geographical distribution of the identified solutions (Figure 3), we identified solutions by providers in 29 countries, with 56% of the solutions provided in EU Member States. The most 'active' countries in this regard were the Netherlands (28 solutions), Finland (15), France (11), and Germany (11) in the EU, and the US (24) and the UK (19) outside of the EU. The relatively large number

of US-based solutions may be explained by the large number of US-based companies offering services in the EU market and thus facing GDPR [3] compliance requirements.

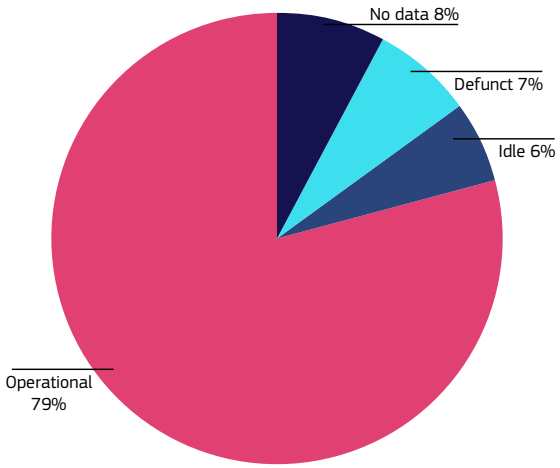
FIGURE 3. Domicile countries of the solutions providers.



Source: authors' elaboration

Finally, we decided to classify the identified solutions based on their operational status and summarise them in Figure 4; in particular, 'Operational' refers to solutions that are currently actively offered as products or services, or actively maintained as completed project or research outputs. 'Idle' refers to solutions with an online presence but which indicates that they are not actively supported or maintained. 'Defunct' refers to solutions that have been discontinued, and 'No data' refers to cases where online presence no longer exists. The share of 'idle', 'defunct', and 'no data' solutions in the list of identified solutions reflects the rapid evolution of the landscape, as the oldest dataset used to compile the initial list of solutions (Appendix 1 in [4]) is from 2020, less than four years ago.

FIGURE 4. Potential identified solutions breakdown by operational status.



Source: authors' elaboration

In summary, casting a wide net for potential digital consent solutions yielded a substantive list of providers with solutions. We find that the majority of these solutions are offered by commercial companies and that the majority of providers of these solutions are based in the EU. It is reasonable to assume based on these findings that there exists in the EU and elsewhere a demand for digital consent solutions and at the very least a strongly emerging field of commercial providers attempting to cater for this demand. In other words, there exist digital consent solutions currently on the market. So far, however, it is not clear which, if any, of the identified solutions could be easily adopted by and serve the needs of RDAOs. The next section begins to address this latter consideration.

4. Framework for the analysis of the identified solutions

The digital management of the entire lifecycle of consents is a complex process that has dependencies on and implications for other processes of any organisation. To assess whether a digital consent solution is suitable for RDAOs, we must understand two aspects. First, we need to understand **the high-level functional elements of a consent management flow** in general. Describing these functional elements will allow us to evaluate in more detail which solutions currently on the market offer which elements and to identify among the solutions typical patterns of included and excluded elements.

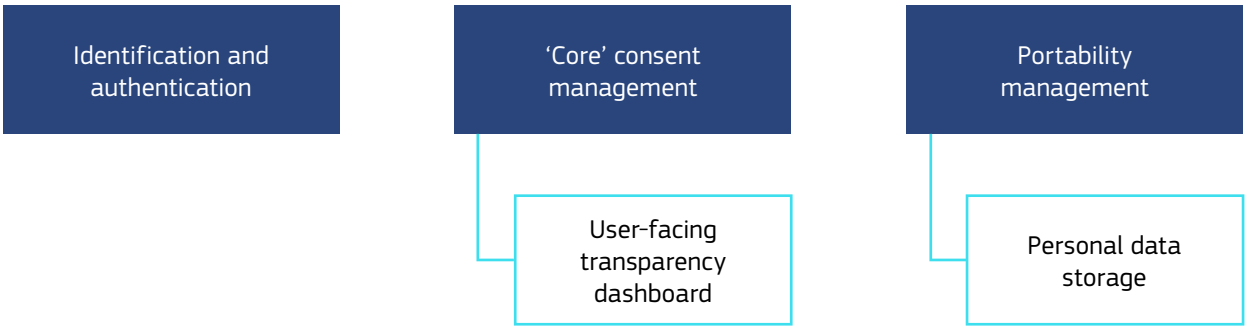
For example, consider the hypothesis of a consent management lifecycle that requires the functional elements A, B, C, and D. Identifying and describing these elements will allow us to analyse specific solutions in terms of whether they provide which element. From this, we can expect patterns to emerge, where we find different solutions all providing, for example, elements A, C, and D but not B, or a set of solutions specialising in providing specifically and only element C, and not A, B, or D.

The second thing we need to understand to assess whether a digital consent solution is suitable for RDAOs is **what are the functional elements** and other features of these solutions that are **especially relevant and desirable for RDAOs** in particular. This will allow us to evaluate the different patterns (and individual solutions that follow them) against a set of criteria of those elements and features that make solutions particularly suitable for RDAOs.

This section presents the working analysis framework we have developed in order to understand the first aspect, the high-level functional elements of a consent management flow in general. The second aspect, the functional elements and other features of these solutions that are especially relevant and desirable for RDAOs in particular, are described in Section 5.

Through our research and interviews with providers of different digital consent solutions, we constructed the following breakdown of the high-level functional elements of digital consent management: 1) **Identification and authentication**, 2) **'Core' consent management**, of which a part can be 2a) User-facing transparency dashboard, and 3) **Portability management**, of which a part can be 3a) Personal data storage. These elements (Figure 5) are described in more detail in the following sections.

FIGURE 5. High-level functional elements (and sub-elements) of digital consent management.



Source: authors' elaboration

4.1 Identification and authentication

A critical element related to consent management under the GDPR [3] is the establishment of a mechanism by which a person can be identified, authenticated, and sufficiently reliably re-identified after the initial consent event. Without the possibility of re-identifying an individual, it won't be possible for them to revoke or modify the consents they have already given.

Identification and authentication can be as light as a username and password combination or a social media login, or as strong as via the future EUDI [6] wallets, bank IDs, and other strong authentication methods. The most suitable method for use in connection with a digital consent solution will depend on how important it is to verify the real identity of the person consenting.

The decision on which kind of identification and authentication to require should be based on legal evaluation (GDPR [3] and other relevant regulation at EU and national level) and consider the different aspects of consent being asked for and given. These include which type of data are being processed and whether it falls under the category of sensitive data in the sense of Article 9 of the GDPR [3], where the data are sourced from and the requirements there may be for the person to grant third-party access to them, and the purposes of processing the data consented.

This element can be built into a digital consent solution, or offered by the same provider in conjunction with a consent solution, but it may also be provided independently of any consent solution. In other words, consent solutions may come with an in-built mechanism for identification and authentication which is designed as an integral and inseparable feature of these solutions. Alternatively, consent solutions may come with an optional feature or add-on for identification and authentication that is designed specifically for that consent solution but which is non-essential for the functioning of the consent solution proper. Consent solutions may also be designed to be agnostic and purposefully support multiple common methods and solutions for identification and authentication.

4.2 'Core' consent management

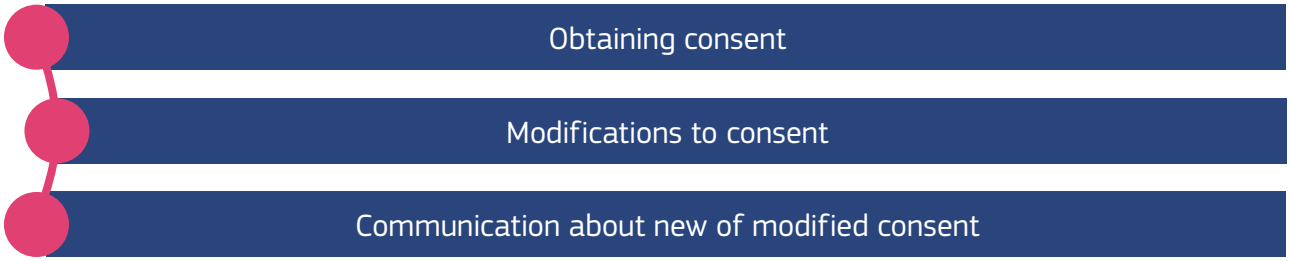
The management of consents throughout their lifecycle, including its subsequent revocation as well as modifications made by the data subject or by the party collecting consents, can be a complex process with dependencies and implications throughout the

technical and service architecture of the entire organisation. Likewise, consent management can be considered from multiple points of view from different vantage points within the organisation: as a set of compliance processes or user experience design requirements, a branding and image issue, a source of customer insights or an employee access management consideration, and so on.

For the purposes of this analysis framework, in this section we describe what we consider the simplest, sufficiently comprehensive set of considerations for 'core' consent management without much consideration for what this implies for the whole set of other, adjacent considerations that can exist in a given organisation. The purpose of this approach is to describe the core element of any consent management solution, which we have seen implemented in various ways by different solutions currently on the market.

From the point of view of the organisation collecting and managing consents, there are three events that are relevant: **obtaining consent** in the first place, which implies the creation of a record of this consent with the relevant information included, **modifications to this consent** (which include its revocation), which implies modification to the contents of the record of the same consent, and **communication of new or modified consent records** to the relevant systems and parties.

FIGURE 6. Relevant events for 'core' consent management.



Source: authors' elaboration

Obtaining consent. The process of obtaining consent requires a user-facing consent screen that should make clearly intelligible to the person consenting the data types, the sources for those data, and purposes of processing that the consent covers. Together with the timestamp of the affirmation of consent given, these are the 'consent data' that populate the new consent record that is created each time a new consent is obtained for the first time. Consent records can be formatted according to a standard such as ISO/IEC TS 27560:2023[4], which describes the information structure of a consent record.

A consent record is also associated with the account or similar of the person that had been identified and authenticated as being the holder of that account in the 'identification and authentication' step.

Note here that this process describes simply and only obtaining a consent. It is entirely agnostic to both the mechanisms by which the individual is identified and by which the data that is being consented is obtained. We discussed the former in Section 4.1 and will discuss the latter in Section 4.3 on portability management.

Modifications to consents. The simplest way to manage the modifications to a consent that we have found during this study is to treat

4. Privacy technologies — Consent record information structure https://www.iso.org/standard/80392.html

consents as 'just' records, albeit with a specific function in an organisation.

The ISO 15489-1:2016[5] standard defines records as 'information created, received, and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of business'. Treating consents as a special class of records means that there exists a robust body of standards, best practices, and research on how they can be managed throughout their lifecycle, including 'identifying, classifying, storing, securing, retrieving, tracking and destroying or permanently preserving' [7] them. Examples of such standards are the ISO 16175-1:2020[6], which describes functional requirements and associated guidance for any applications that manage digital records, and MoReq2010[7], an open EU records management specification.

Treating consents as records enables processing each subsequent event after the creation of the record as a modification of that record that is logged and timestamped in a kind of version history. The revocation of the consent by the person means that the 'validity' field in the consent record is modified from indicating 'valid' to indicating 'invalid' and a new version of the record is created with the timestamp of the new version. In this way, each time the person grants, modifies in any way, or revokes their consent, a new version of the record is created and timestamped and the old version is marked invalid.

Likewise a new version of the consent record is created and the old marked invalid any time the organisation obtaining and managing consents needs to alter the consent record to, for example, add a purpose for processing data or a third party to whom the data may be disclosed. In this case, the person must re-grant the consent, including the modifications made, before it is marked and considered valid. Records can also be set to have retention periods, meaning they expire and are marked as invalid at a specific time or after a set period of time.

Communication about new and modified consents. Finally, any 'core' consent solution must have the ability to automatically push notifications of all changes in a given consent record in multiple directions. It must be able to notify the data subject that a change has been initiated by the organisation and that they must re-grant their consent for data processing to resume. It must be able to notify the organisation managing consents that the data subject has revoked or in another way modified their previous consent. And, in some cases, it must be able to notify third parties who process data that the consent was modified. In addition, any new attempts to process the data consented must be able to pull the latest version of the consent record with its status of valid or invalid.

A 'core' consent management solution should not be expected to be able to enforce action based on the notifications it pushes or are pulled from it. It should be considered sufficient that the solution is capable of delivering these notifications in real time. More elaborate consent solutions may offer integrations with systems that process data that are able to execute actions based on the notifications of granted or revoked consent.

4.2.1 User-facing transparency dashboard

A user-facing transparency dashboard is a feature sometimes provided as part of a 'core' consent management solution. This refers to the interface for people that contains a view of all the consents that they have at some point given. A user-facing transparency dashboard allows for 'self-service' consent revocation or modification, as opposed to

5. Information and documentation — Records management https://www.iso.org/standard/62542.html

6. Information and documentation — Processes and functional requirements for software for managing records https://www.iso.org/standard/74294.html

7. https://moreq.info/

models whereby the individual consenting must contact the data controller via email or similar complicated way to notify them of revocation of consent.

Opening a consent in a dashboard view will show the information about the consent, that is, a representation of the contents of the consent record like the data types, sources, purposes etc. The dashboard will also present the person with options to modify each consent record or entirely revoke each consent. Such transparency dashboards are especially common in contexts where a person is asked for multiple consents for different data types, sources, processing purposes, and/or third parties processing the data.

By default, a transparency dashboard does not need to include any actual data consented for processing, but rather merely the consent records which describe the data. For example, a consent record may show that I have consented to the processing of my mailing address for the purpose of sending me a magazine. However, it does not contain the data of what that address actually is. Dashboards that 'contain' data in this way and also allow its editing are of course possible, though not necessary, for 'core' consent management solutions because they require elements in addition to 'core' consent management, such as data storage. We discuss data storage in the next section in connection with portability management.

4.3 Portability management

Portability management refers to the different ways in which data is accessed and/or transferred after or in connection with granting consent. Portability management can be described as the third high-level element of digital consent solutions (in addition to identification – Section 4.1 - and consent management – Section 4.2) and is sometimes bundled with one or both the other elements, though it is not necessary to do so.

Portability management can mean that, in the same process as consenting, a person also provides data by, for example, filling out a form. Other scenarios involve data acquired by a portability request because it is held by another party and uploaded by the data subject. Alternatively, the data subject may be directed to download and install an app that collects data from their device. It may also be possible that the data subject gives legal mandate to the organisation requesting consent to access data from a third party and/or to port data on their behalf into its own systems. Any of these mechanisms can be built into a consent management solution, or a consent solution can be designed to support multiple tools and mechanisms for managing data portability. None of them are required for a 'core' consent solution.

4.3.1 Personal data storage

In cases where data subjects consent multiple times – for different specific research purposes, for example – and at least part of the data consented for processing are repeatedly the same – their date of birth, for example – it may be beneficial to associate the account of the data subject with their personal data storage that hosts the most commonly requested data. In this way, these data can be populated in a form or added to a dataset in a more simple and quick way than by manual re-entry each time. This functionality may also be bundled with the identification element if, for example, a digital wallet is used.

To summarise, the aim of this section is to understand the high-level functional elements of a consent management flow in general. We were able to describe in some detail three conceptually distinct elements: identity and authentication, 'core' consent management, and portability management. Additionally, we described the sub-element of 'core' consent management, user-facing transparency dashboards, and the sub-

element of portability management, personal data storage. This was done with the objective that describing these elements will allow us to evaluate in more detail which digital consent solutions currently on the market offer which elements and to identify among the solutions typical patterns of included and excluded elements. Before we proceed to this task, it is worth briefly describe the features of digital consent solutions that are especially relevant and desirable for RDAOs.

5. The special case of Registered Data Altruism Organisations (RDAOs)

This section enriches the understanding of what is needed for the management of the lifecycle of consents from the specific point of view of RDAOs. This enriched understanding enables us to evaluate identified solution patterns, and specific solutions that follow those patterns, for their suitability specifically for RDAOs.

Although there currently exists only one RDAO[8], and as of time of writing it does not use digital means for consent management, we can hypothesise more or less generic needs that future RDAOs who wish to use a digital consent management solution may have. We can also refer to requirements in the DGA and the GDPR for some basic needs to comply with regulation.

We have categorised the elements and features specifically relevant for the case of RDAOs into two types (Figure 7): considerations affecting whether a solution could be considered relevant for easy adoption by numbers of future RDAOs, and considerations describing elements and features that make a solution pattern or an individual solution especially suitable for RDAOs.

8. DATALOG https://datalog.es/

FIGURE 7. Elements and features specifically relevant for the case of RDAOs.

Considerations affecting the overall relevance for RDAOs

- Maturity of the solution
- Modularity of the elements of consent management
- Technical complexity
- Scalability
- Comprehensiveness

Considerations indicating particular suitability for RDAOs

- Simplicity and consent in the focus
- Flexible ability to reliably re-identify individuals
- Flexible ability to work with portability management tools

Source: authors' elaboration

Concerning the overall relevance for RDAOs, the **maturity** of the solution represents one of the key aspects, as a relevant solution should be in production and beyond conceptual, alpha, or beta versions.

Another important element is the **modularity** of the elements of consent management, or how 'enmeshed' the consent management functionality is with the rest of the provider's offering. A relevant solution should not require the purchase or use of a set of elements or features that are not strictly needed by RDAOs.

Then the **technical complexity**, or whether a significant amount of technical expertise would be necessary for initial setup or maintenance, has to be considered. A relevant solution should not require substantial technical competences in-house.

Another fundamental element is **scalability**, or whether each instance of a solution would be built bespoke to an organisation or would need substantial adjustments to accommodate varied purposes of data processing. A relevant solution should be able to cater to as many and as many varieties of RDAOs as possible.

Finally, **comprehensiveness**, or whether the solution could handle consents in diverse situations like when handling consents for different types of data (including sensitive data in the sense of article 9 of the GDPR [3]), dynamic granting and revocation of consents, timely downstream notification of (withdrawal of) consents, and levels of specificity of purposes for processing included in consents. A relevant solution should be as comprehensive as possible.

Regarding the **particular suitability for RDAOs**, we need to have **simplicity and consent in the focus**. Consent management is a critical and complex task of RDAOs and the digital solution to use for it should ideally be built specifically to manage consents, rather than having a different primary purpose.

Another key element is the **flexible ability to reliably re-identify individuals**. A feature enabling reliable re-identifying individuals may be included in the consent solution itself (i.e., the solution may include the identification and authentication element) or the consent solution can be designed in such a way that it can work with one or more other, ideally multiple, solutions that provide this ability. As RDAOs are expected to be of diverse kinds and needs, it is expected that the latter approach is more appropriate for a generic consent management solution that could be used by as many RDAOs as possible.

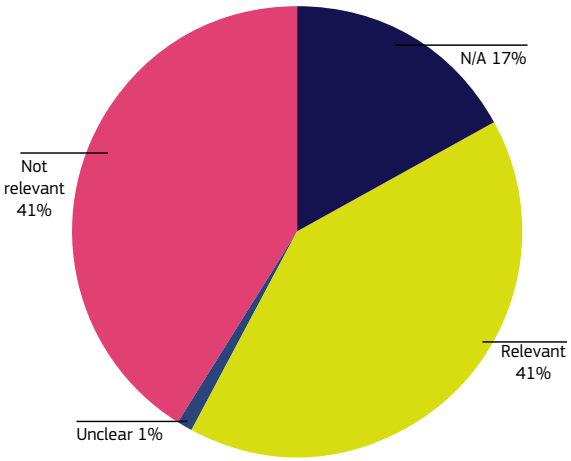
Finally, we need to consider the **flexible ability to work with portability management tools**. It can also be hypothesised that RDAOs will have a range of different methods for data collection and so diverse data portability needs. Any consent solution should be able to accommodate a variety of different ways for RDAOs to manage the portability of the data they use.

Now that we have identified factors affecting the overall relevance of a solution to RDAOs, or potential 'disqualifying' factors, as well as those indicating particularly suitability for RDAOs, we are ready to analyse further the 134 operational solutions that were identified in the earlier steps of this study, using the analysis framework provided in Section 4.

6. Typology and suitability for Registered Data Altruism Organisations (RDAOs)

We applied the considerations listed in Section 5 to the long list of identified potential solutions in order to identify a subset of particularly promising, relevant digital consent solutions. The labels 'N/A' and 'unclear' were assigned respectively to defunct solutions and to those where there was very little information available online. The labels 'relevant' and 'not relevant' were assigned based on a review of publicly available material and solutions analysed as 'relevant' were a combination of relatively high maturity, high modularity, low technical requirements for the organisation using it, high scalability and replicability, and high comprehensiveness. Figure 8 describes the results of this analysis.

FIGURE 8. Potential solutions breakdown by operational status.



Source: authors' elaboration

Next, using the three elements and two sub-elements identified and described in Section 4, this study identifies eight more or less distinct patterns of consent management solution offerings currently on the market.

These patterns, or types of offering, can further be clustered into two types: **consent-focused** and **consent-included** (Figure 9). Solutions of the first type set out to solve a consent management issue (usually a business problem) whereas solutions of the second type set out to solve some other issues, for which consent management is also relevant. These patterns are described and examples are listed for each in the following sections. The suitability of different patterns for RDAOs consent management purposes is assessed against the considerations specifically relevant for RDAOs introduced in Section 5: Simplicity and consent in the focus, Transparency dashboard for individuals, and Flexible ability both to reliably re-identify individuals and to work with portability management tools.

FIGURE 9. Identified patterns of consent management solutions currently on the market.

Consent-focused patterns	Consent-included patterns
■ Simple cookie consent ■ 'Core' consent management	■ Enterprise customer relationship management (CRM) ■ E-commerce and analytics solutions ■ Research focused data collection ■ Identity management solutions ■ Data exchange platforms ■ Personal data vaults

Source: authors' elaboration

6.1 Consent-focused patterns

6.1.1 Simple cookie consent

Simple cookie consent solutions used in collecting information about a person's web browsing tend not to authenticate people and usually identify them only based on IP address and its location. They offer website or app users the option for more or less granular consent for different types of cookies and trackers, and (if GDPR-compliant) a transparency dashboard type functionality to revoke these consents. They tend not to include portability management functionalities or personal data storage. In addition to the elements of a consent management solution, they tend to offer organisations the ability to scan their own websites for cookies and trackers and automate their categorisation and/or inclusion in the interfaces for managing consents.

Examples: CookieYes, CookiePro.

Suitability for RDAOs

Cookie consent tools are one of the more common types of consent management solutions, and although they tend to be very simple, they seem unlikely to be suitable for RDAOs since they tend not to be built to support reliable re-identification of the people interacting with them.

- Simplicity and consent in the focus: *Yes.*
- Flexible ability to reliably re-identify individuals: *Unlikely.*
- Flexible ability to work with portability management tools: *Unlikely.*

Suitability assessment for RDAOs: *Likely not suitable.*

6.1.2 'Core' consent management

Solutions that follow the 'core' consent management pattern tend to focus exclusively on the 'core' consent management element, usually including the provision of user-facing transparency dashboards, and tend to scope out identity and authentication as well as portability management, including personal data storage elements. They tend to be designed in a way that allows for these other elements to be handled by different solutions in a variety of ways. In other words, they remain agnostic as to both the need for these elements as well as how they are managed. At their best, consent management solutions that follow this pattern can be integrated or interoperable with a wide range of solutions in a manner that can successfully avoid the kinds of vendor lock-in effects to which more 'wholesale' solutions can be susceptible. Two subtypes of 'core' consent management solutions can be discerned: empowered focused and compliance focused, discussed below.

Empowerment focused. Consent management solutions that are primarily motivated by giving data subjects the tools to manage their GDPR [3] rights such as giving and revoking consent to their personal data being processed, tend to be provided by smaller, more conceptual and less mature EU-based providers. These solutions tend to approach consent management from the perspective of individual users and focus their offering and value proposition specifically for Business-to-Consumers (B2C) companies and other organisations that prioritise empowering their customers. They may also incorporate in their offering elements of identification and authentication, portability management, and personal data storage depending on their primary use cases.

Compliance focused. Compliance focused consent management solutions differ from the above, empowerment focused solutions, in that the primary problem they seek to solve for their corporate clients is that of regulatory compliance. This is reflected in their tendency not to prioritise or provide an individual-facing transparency dashboard and rather focus their offer on the needs of the company employees who need to process personal data and the officers who are responsible for the compliance of that processing with applicable laws. They tend to remain agnostic as to whether or how identification and authentication and portability management elements are implemented. In addition to managing consents, these types of solutions can include other compliance-related elements such as automations for reporting obligations.

Examples: Traq ('core' consent); Right Consents by Fair&Smart (part of LuxTrust) and iGrant.io (empowerment focused); Signatu (compliance focused).

Suitability for RDAOs

'Core' consent management solutions that focus (near) exclusively on managing the core element of a consent management seem particularly fitting and flexible to be of service to diverse kinds of RDAOs.

- Simplicity and consent in the focus: *Yes.*
- Flexible ability to reliably re-identify individuals: *Yes.*
- Flexible ability to work with portability management tools: *Likely yes.*

Suitability assessment for RDAOs: *Likely very suitable.*

6.2 Consent-included patterns

6.2.1 Enterprise customer relationship management (CRM)

Enterprise CRM solutions tend not to authenticate people but rather assign

company-internal IDs for customers whose data is managed. They tend not to prioritise or even provide a customer-facing transparency dashboard for managing their consents, but rather focus on company-internal users and their needs. Consents recorded in the CRM solution can be collected via the solution itself or via other means and imported into the system. Solutions can also offer portability management functionalities, such as data collection forms. They tend not to provide customers their own personal data storage. In addition to the elements for a consent management solution, they tend to be heavily integrated with messaging and other relationship management functionalities, including analytics services.

Examples: Salesforce, SAP.

Suitability for RDAOs

These solutions in which consent management is built into a larger customer relationship management system seem unlikely to suit the needs for RDAOs, as their core offering are the advanced functionalities for analytics, marketing, communication preference management and so on, and the consent management is merely built in to support the core offering.

- Simplicity and consent in the focus: *No.*
- Flexible ability to reliably re-identify individuals: *Yes.*
- Flexible ability to work with portability management tools: *Likely yes.*

Suitability assessment for RDAOs: *Likely not very suitable.*

6.2.2 E-commerce and analytics solutions

The solutions following this pattern tend to be motivated by the marketing, sales and analytics needs of a company, typically categorisable as a B2C e-commerce venture of some kind. Because meeting these needs requires processing personal data, and operating within the EU requires GDPR [3] compliance, these types of solutions tend to incorporate cookie and consent management in their offering. Because the primary problem these solutions address is the business-internal need for insights on customer behaviour and preferences, they tend to prioritise providing tools for maximising consents given, opt-ins and other methods for increasing conversion rates. They also tend to follow a pattern similar to simple cookie consent solutions in not including an identification and authentication element and offering similar individual-facing transparency dashboards, but differ in additionally offering analytics and conversion optimisation elements.

Examples: One Trust, Trust Arc.

Suitability for RDAOs

Solutions that follow this pattern tend to be focused on behavioural data collection and processing, and as such seem unlikely to be able to serve numbers of RDAOs with diverse needs.

- Simplicity and consent in the focus: *Unlikely.*
- Flexible ability to reliably re-identify individuals: *Likely limited.*
- Flexible ability to work with portability management tools: *Likely limited.*

Suitability assessment for RDAOs: *Likely not suitable.*

6.2.3 Research-focused data collection

Solutions that are designed with the research community in mind tend to adopt a pattern of focusing primarily on portability management, as the main issue these solutions are designed to address is data collection. Personal data collection for research purposes tends to

rely on consent as the legal grounds for processing, and so these solutions usually have quite specific and elaborate ways of specifying purpose for processing personal data. They can also include quite sophisticated methods of data collection including software that participants have to install on their own device. The software then extracts certain data locally before sending them to the environment in which researchers can access them. These solutions tend to focus on serving the researcher and thus do not include identification and authentication elements (unless required by the researcher) nor offer transparency dashboards or similar for the individuals participating in the study.

Example: PORT.

Suitability for RDAOs

Research-focused data collection tools that incorporate consent management might possibly be suitable for some numbers of research-oriented RDAOs. They are often based on open source components, but some may not exist as 'enterprise grade' or commercial solutions.

- Simplicity and consent in the focus: *No.*
- Flexible ability to reliably re-identify individuals: *Potentially.*
- Flexible ability to work with portability management tools: *Possibly.*

Suitability assessment for RDAOs: *Possibly suitable.*

6.2.4 Identity management solutions

Identity management solutions originate from attempting to address problems such as service-independent login and the provision of eID wallets for credentials and attestations that can be shared or given access to for identification and authentication purposes. The consent management elements included in solutions that follow this pattern tend to be secondary and primarily apply to the person identification data that the solution uses and for which they usually provide a personal data storage solution. They are usually user-centric as their purpose tends to be giving individuals more granular control over which personal attributes they share in which identification and/or authentication instance, and they may provide transparency dashboards for viewing logs of attempts to access certain person identification data. However, due to the nature of these instances being one-off identification or authentication events rather than leading to continuous or continued processing of personal data, they usually do not not include methods for revoking consent once given for a specific instance.

Examples: Affinidi, LuxTrust.

Suitability for RDAOs

It is possible that solutions that follow the identity management pattern may be suitable for use by some RDAOs. However, since they were likely not primarily designed for consent management, it may be that customisation would be necessary for solutions of this pattern to serve the core consent needs of RDAOs.

- Simplicity and consent in the focus: *No.*
- Flexible ability to reliably re-identify individuals: *Not always flexible but reliable.*
- Flexible ability to work with portability management tools: *Possibly.*

Suitability assessment for RDAOs: *Possibly suitable.*

6.2.5 Data exchange platforms

Solutions that follow the data exchange platform pattern tend to focus on solving issues around personal data monetisation or valorisation. They tend to include an identification and authentication element to

be able to support monetary transactions, such as making and receiving payments. The data portability management elements can include retrieval of data on the authority of the individual using the solution. Data exchange platforms can offer some personal data storage for frequently accessed (or sold) data. Solutions following this pattern tend to offer limited capacities for managing consents beyond the initial granting and not to focus on mechanisms for revoking consents, as most transactions are usually one-off events rather than lead to continuous or continued processing of the data consented. In this way, solutions following this pattern are somewhat similar to those following the identity management solution pattern. Transparency dashboards likewise tend to be similar and present as a log of concluded transactions.

Example: itsmydata.

Suitability for RDAOs

These solutions that are associated with data exchange platforms or marketplaces are unlikely to be suitable for RDAOs because their providers' business models tend to be based on commission on executed (paid) data transactions. In the case of RDAOs, however, the transactions are purely voluntary and no money exchanges hands from which a commission could be charged.

- Simplicity and consent in the focus: *No.*
- Flexible ability to reliably re-identify individuals: *Yes.*
- Flexible ability to work with portability management tools: *Likely yes.*

Suitability assessment for RDAOs: *Likely not very suitable.*

6.2.6 Personal data vaults

Solutions providing personal data vaults are often discussed in connection with personal data sharing but they do not always include the possibility for others to access or otherwise process data contained in them, and they usually do not contain mechanisms for consenting to the use of the data stored by third parties. At their most basic, personal data vaults only receive data, and the person that owns the vault is the only party who can (technically) access the data stored. However, solutions branded as personal data vaults or similar (the vocabulary around these is quite diverse) can also include ways in which the person with the vault can consent to others accessing data stored there. For a deep dive on personal data spaces, see [8].

Solutions that follow this pattern tend to be individual and privacy focused and to be best able to handle mostly fairly static data. In some ways, a personal data vault and solutions offering them are very similar to eID wallet solutions of the Self Sovereign Identity (SSI)-flavour that follow the identity management pattern, where the individual has maximal control over the technical access to the data contained. These solutions tend to provide at least basic data management elements for individuals to import data, but transparency dashboard specifically for consents tend only be included in the more complex solutions where the possibility of consent-based third-party access is built into the solution.

Examples: Cozy, Solid-based solutions.

Suitability for RDAOs

Personal data vaults tend to recognise the importance of consent but, since it's not at the core of the issue they're addressing, their mechanisms to manage consents tend to be immature or non-existent. For the purposes of RDAOs, asking all individuals who engage in data altruism first to install a personal vault, then populate it with the data requested by the RDAO, and finally consent to the

RDAO accessing or otherwise processing them, seems like an unlikely successful and scalable solution. If governments decide to grant personal data vaults to all citizens, the likelihood for RDAOs to use such consent management tools would increase.

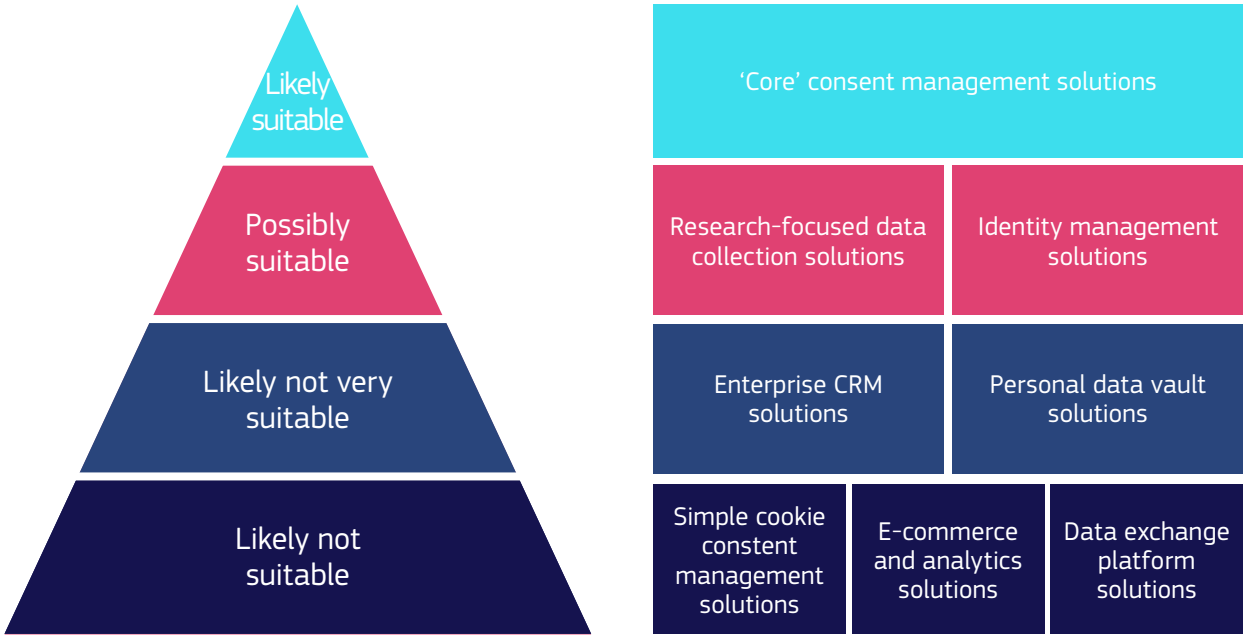
- Simplicity and consent in the focus: *No.*
- Flexible ability to reliably re-identify individuals: *Likely yes.*
- Flexible ability to work with portability management tools: *Yes.*

Suitability assessment for RDAOs: *Likely not very suitable.*

The tables below summarise the main features of the different patterns that consent solutions follow (Table 1) and the assessments of their suitability specifically for RDAOs (Table 2). Consequently, we propose a tentative ranking of different consent solution patterns in terms of how likely they are to be suitable for adoption for numbers of RDAOs (Figure 10). This ranking is the following:

- Likely suitable: 'Core' consent management solutions;
- Possibly suitable: Research-focused data collection solutions and Identity management solutions;
- Likely not very suitable: Enterprise CRM solutions and Personal data vault solutions;
- Likely not suitable: Simple cookie consent management solutions, E-commerce and analytics solutions, and Data exchange platform solutions.

FIGURE 10. Features of the identified consent management solutions and their suitability for RDAOs.



Source: authors' elaboration

TABLE 1. Summary of identified consent solution patterns.

Pattern			1. Identification and authentication usually included	2. 'Core' consent usually included	2A. User-facing transparency dashboard usually included	3. Portability management usually included	3A. Personal data storage usually included
Consent focused patterns	Simple cookie consent management		No	Yes	Yes	No	No
	'Core' consent manage-ment	Empowerment focused	No	Yes	Yes	No	No
		Compliance focused	No	Yes	Not always	No	No
Consent included patterns	Enterprise CRM		No	Yes	No	Yes	No
	E-commerce and analytics		No	Yes	Yes	No	No
	Research-focused data collection		No	Yes	No	Yes	No
	Identity management		Yes	Yes	Yes	No	Yes
	Data exchange platform		Yes	Yes	Yes	Yes	No
	Personal data vault		Yes	Sometimes	Sometimes	Yes	Yes

Source: authors' elaboration

TABLE 2. Summary of solution patterns' RDAOs suitability assessments.

Pattern		Simplicity and consent in the focus	Flexible ability to reliably re-identify individuals	Flexible ability to work with portability management tools	Suitability assessment for RDAOs
Consent focused patterns	Simple cookie consent management	Yes	Unlikely	Unlikely	Likely not suitable
	'Core' consent management	Yes	Yes	Likely yes	Likely suitable
Consent included patterns	Enterprise CRM	No	Yes	Likely yes	Likely not very suitable
	E-commerce and analytics	Unlikely	Likely limited	Likely limited	Likely not suitable
	Research-focused data collection	No	Potentially	Possibly	Possibly suitable
	Identity management	No	Not flexible but reliable	Possibly	Possibly suitable
	Data exchange platform	No	Yes	Likely yes	Likely not suitable
	Personal data vault	No	Likely yes	Yes	Likely not very suitable

Source: authors' elaboration

7. Conclusions

The purpose of this report is to support data altruism organisations on the adoption of digital solutions for consent management. After a landscape analysis (Section 3), we found that there exist a number of digital consent solutions currently on the market but it is still not entirely clear which, if any, of the identified solutions could be easily adopted by and serve all the needs of RDAOs.

After elaborating our own analysis framework (Section 4) and describing the specific needs of RDAOs (Section 5), we were able to discern from the landscape eight patterns into which several consent solutions follow. We were also able to evaluate these patterns against the specific needs of RDAOs (Section 6).

As a result of our analysis, **we find it likely that there exist digital consent solutions currently on the market that could be relatively easily adopted by RDAOs and serve at least the very core needs of consent management for them**. Below we summarise some of the shared characteristics of these examples.

The solutions likely to be most suitable for RDAOs tended to follow the 'core' consent management pattern (see Section 6.1.2 for details and examples). This means that *the primary problem they are built to solve for customers and users is specifically consent management*. Because of this feature, it is plausible that these kinds of solutions are particularly well-equipped to handle the critical aspects of consent management: obtaining consents and creating a record of them, making modifications to those records (including withdrawal of the consent in part or entirely), and ensuring real-time notifications to all necessary parties and systems when a consent is obtained or modified (see Section 4.2. for more details on the core consent processes as we understand them).

The likely suitable solutions available on the market also tend not to include or be bundled with identification and authentication or portability management functionalities. They also usually include a user-facing transparency dashboard and not a personal data storage feature.

This pattern of consent solutions was evaluated as likely suitable also because the hypothesised digital needs of RDAOs are more extensive than merely consent management but diverse beyond it. This is why any consent solution for RDAOs should be *flexibly able to work with different types of identification and authentication mechanisms and tools, as well as with different types of portability management solutions.* We find it therefore not advisable to bundle one or both of these elements into the same solution that is proposed for numbers of RDAOs to handle the core processes of their consent management.

In addition, we find that *well-established record lifecycle management approaches and standards provide a solid basis for consent management.* In order not to reinvent the wheel, it is possible to treat consent records as a special case of records, apply the relevant standards and best practices, and end up with a functional core consent management system. Because of the simplicity of relying on existing, tested methods from records management and applying them to consents, we consider consent management solutions that adopt this approach are especially suitable for RDAOs.

In summary, when searching for digital consent solutions currently on the market that could be relatively easily adopted by RDAOs and serve at least the very core needs of consent management for them, we recommend checking potential solutions for the following:

- The primary problem the solution attempts to solve is core consent management, and not something else. Afterwards, you are able to dig deeper to ensure all the core processes of consent management throughout its lifecycle are in place.
- The solution is not tied in some way to a specific way of handling identification and authentication, or portability management. This will mean the solution is flexible enough to cater to the anticipated diversity of future RDAOs.
- The solution preferably does not entail the use of bespoke or proprietary protocols and methods but rather relies on some established standards and standard approaches. An example of such standards that can be used is the ISO standard for consent records[9], and an example of a standard approach that can be adopted is that of records management[10]. Moreover, the secure middleware platform Simpl[11] aims to enable interoperability by promoting common data standards and could provide additional components to the solution for consent management of RDAOs.

As we know from the examples we have identified, these kinds of solutions currently exist on the market and as we have been able to assess in this study, they are likely suitable for adoption by RDAOs.

9. ISO/IEC TS 27560:2023 Privacy technologies — Consent record information structure https://www.iso.org/standard/80392.html

10. ISO 15489-1:2016 Information and documentation — Records management https://www.iso.org/standard/62542.html

11. https://simpl-programme.ec.europa.eu/

References

[1] European Strategy for Data, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

[2] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0868

[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), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679

[4] Langford, J., Poikola, A., Janssen, W., Lähteenoja, V. and Rikken, M. (Eds.) (2020) 'Understanding MyData Operators', MyData Global. https://mydata.org/wp-content/uploads/2020/04/Understanding-Mydata-Operators.pdf

[5] https://mydata.org/participate/awards/

[6] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1183

[7] ARMA International. 'Glossary of Records and Information Management Terms, 3rd Edition'. ARMA International.

[8] European Commission, Joint Research Centre, Lähteenoja, V., Leonard, M. and Langford, J., Personal Data Spaces: Workshop series, Publications Office of the European Union, Luxembourg, 2024, https://data.europa.eu/doi/10.2760/748099, JRC138783

List of abbreviations and definitions

Abbreviations	Definitions
B2C	Business-to-Consumer
CRM	Customer Relationship Management
DGA	Data Governance Act
eID	Electronic Identification
EIDAS	Electronic IDentification, Authentication and trust Services
EU	European Union
EUDI	European Digital Identity
GDPR	General Data Protection Regulation
RDAO	Data altruism organisations recognised in the Union
SSI	Self-Sovereign Identity

List of figures

List of tables

Annexes

Annex 1. Full list of identified potential solutions

The following table does not have the ambition of being comprehensive and cover all solutions available on the market at the time of writing. Additionally, it does not aim at evaluating the identified solutions nor at being binding for the European Commission.

Solution name	Solution provider(s)	Provider type	Provider country
ACROSS platform	ACROSS	Project	Greece
Affinidi Login	Affinidi	Company	Singapore
Affinidi Vault	Affinidi	Company	Singapore
ArcBlock	ArcBlock	Company	China
BankID	BankID	Company	Sweden
Bankin'	Bankin	Company	France
BE SWARM	BE SWARM SAS	Company	France
BitsaboutMe	BitsaboutMe AG / Ltd	Company	Switzerland
Buddy Payment	Buddy payment	Company	Netherlands
CANDiY	Sakak	Company	South Korea
CaPe	Engineering Ingegne-ria Informatica SpA	Company	Italy
Capture	Numbers Co., Ltd.	Company	Taiwan
CCM19	Papoo Software & Media GmbH	Company	Germany
Ciitizen	Ciitizen	Company	US
CitizenMe	CitizenMe	Company	UK
Click2Share	Click2Share	N/A	Netherlands
Coelition	Coelition	Company	UK
Consent Receipt Suite	Datafund d.o.o.	Company	Slovenia
Consent Wallet	NTT Data Corporation	Company	Japan
CONSENT-as-a-ser-vice	DATA for GOOD Foun-dation	Non-profit	Denmark
ConsentGrid	Cloud Privacy Labs	Company	US
Consento	Consento	Company	Japan
Consentua	Consentua	Company	UK
Cookiebot	Usercentrics GmbH	Company	Germany
CookiePro	OneTrust LLC	Company	US

Solution name	Solution provider(s)	Provider type	Provider country
CookieYes	CookieYes Limited	Company	UK
Cozy	Cozy Cloud SAS	Company	France
Crownpeak CMP	Crownpeak	Company	US
Dappre	Dappre	Company	Netherlands
Data Equity Bank	Data Equity Bank	N/A	US
Data Unions	Streamr Network AG	Company	Switzerland
DataCave	Tribal Data Limited	Company	UK
Datacoup	ODE Holdings, Inc	Company	US
DataGuard Consent and Preference Management	DataCo GmbH	Company	Germany
DataKeeper	DataKeeper	Company	Netherlands
DATALOG	Universitat Pompeu Fabra Barcelona,Ideas for Change	Research institute, Company	Spain, Spain
Datamixer	Datamixer	Non-profit	Belgium
DataPal	DataPal	Company	UK
DataPassports	DataPassports	Company	Canada
Dataplaza	Dataplaza	N/A	Netherlands
Dataspace protocol	IDSA	Non-profit	Germany
Dataswyft	Dataswyft Group	Company	UK
DataVillage	DataVillage	Company	Canada
Datavillage	Datavillage SRL	Company	Belgium
DataYogi	DataYogi	Company	UK
Datum ID	Datum Network GmbH	Company	Switzerland
Diabetes Services	Diabetes Services ApS	Project	Denmark
digi.me	Digi.me Limited	Company	UK
Digital Lab	Younode	Company	Japan
DTLab WHISSPR Report Service	Digital Transparency Lab	Non-profit	UK
Dyme	Dyme	Company	Netherlands
Eclipse Dataspace Components (EDC)	Eclipse Foundation AISBL	Non-profit	Belgium
Ecolyo	Metropole Grand Lyon	Public body	France
Enfuce	Enfuce	Company	Finland
Evidon	Evidon	Company	US
Ewise	Ewise	N/A	US

Solution name	Solution provider(s)	Provider type	Provider country
Expanded Password System	Mnemonic Identity Solutions	Company	UK
EYD consent management	EYD AS	Company	Norway
Fairdrive	Swarm Association	Non-profit	Switzerland
Fairdrop	Datafund d.o.o.	Company	Slovenia
Fikks	Fikks	Company	Netherlands
Financieel Paspoort	Stichting Financieel Paspoort	Non-profit	Netherlands
Fiware	FIWARE Foundation, e.V.	Non-profit	Germany
Gaia-X	Gaia-X AISBL	Non-profit	Belgium
Geens	Geens NPO	Non-profit	Belgium
Gravito CMP	Gravito	Company	Finland
Healthbank	Healthbank cooperative	Non-profit	Switzerland
Heely	Heely	Company	Finland
HelloConsent	HelloConsent	N/A	N/A
Helsinki MyData operator	City of Helsinki	Public body	Finland
Hestia.ai	Hestia.ai	Company	Switzerland
HHDC	Holland Health Data Co-operative	Non-profit	Netherlands
iGrant.io	LCubed AB	Company	Sweden
illow	illow	Company	US
Information Answers	Information Answers Ltd	Company	UK
IRMA	Privacy by Design Foundation,SIDN Business BV	Non-profit, Company	Netherlands, Netherlands
iSHARE Trust framework	iSHARE	Non-profit	Netherlands
itsmydata.	itsmydata GmbH	Company	Germany
iWize	iWize B.V.	Company	Netherlands
JanusID	JanusID B.V.	Company	Netherlands
JLINC	Portable Data Corporation	Company	US
JoinData	JoinData	Non-profit	Netherlands
Jolocom	Jolocom	Project	Germany
Kivra Business	Kivra	Company	Sweden
Linxo	Linxo SAS	Company	France

Solution name	Solution provider(s)	Provider type	Provider country
Luotettava työntekijä	Vastuu Group Ltd	Company	Finland
Lympo	LATGALA OÜ	Company	Estonia
MedMij	MedMij	Non-profit	Netherlands
Meeco	Meeco Group Pty Ltd	Company	Belgium
MIDATA	MIDATA	Non-profit	Switzerland
Mijnapp Eindhoven	Mijnapp	Public body	Netherlands
MijnGeldzaken	Finnation bv	Company	Netherlands
MijnOverheid	Logius	Public body	Netherlands
MijnPensioenoverzicht	MijnPensioenoverzicht	Public body	Netherlands
miKS-it	Meeco Group Pty Ltd	Company	Belgium
MunJob	MunJob Oy	Company	Finland
My Data Intelligence	My Data Intelligence	Company	Japan
my:D	SNPLab Inc.	Company	South Korea
MyDataIsRich.com	MEDICORASSE CORREDURÍA DE SEGUROS DEL CMB S.A.U.	Company	Spain
MyDataMood	MYDATAMOOD	N/A	Spain
MyDataShare	Vastuu Group Ltd	Company	Finland
Mydex	Mydex Data Services CIC	Company	UK
MyLife Capsule	Life Capsule Pty Ltd	Company	Australia
MyLife Digital	MyLife Digital Limited	Company	UK
MyQii	Qii	Company	Netherlands
N/A	Qiy Foundation	Non-profit	Netherlands
N/A	Prometheus-X	Non-profit	France
N/A	Innovalor	Company	Netherlands
N/A	Findy	Non-profit	Finland
N/A	iSPIRT	Non-profit	India
N/A	MyData Global	Non-profit	Finland
N/A	Pondersource	Non-profit	Netherlands
Ockto	Ockto B.V.	Company	Netherlands
OmaPosti Pro	Posti	Company	Finland
Omat ostot	S-Group	Company	Finland
Onecub	Onecub	Company	France
OneTrust	OneTrust LLC	Company	US
OpenConsent	OpenConsent	N/A	UK

Solution name	Solution provider(s)	Provider type	Provider country
OwnYourData	Verein zur Förderung der selbstständigen Nutzung von Daten	Non-profit	Austria
paspit	DataSign Inc.	Company	Japan
Peercraft	Peercraft	Company	Denmark
People.io	People.io	N/A	UK
Personal consent manager	PIMCity Project,Politecnico di Torino	Project,Research institute	Italy
PersonalData.io	Personaldata.io	Non-profit	Switzerland
Personium	Fujitsu Limited	Company	Japan
Piwik PRO	Piwik PRO SA	Company	Poland
PlanetCross	Planetway	Company	Japan
PlanetID	Planetway	Company	Japan
Pocket	Pool Data Limited	Company	Gibraltar
Pocket	Pool Data Ltd	Company	UK
Pollen	OKP4	Company	France
polypoly	pc polypoly coop SCE mbH	Company	Germany
PORT	University of Utrecht,University of Amsterdam,Eyra	Research institute	Netherlands
Powr of You	Powr of You	Company	UK
Prifina	Prifina	Company	US
PrivacyCloud	PRIVACYCLOUD SL	Company	Spain
reData.me	E-Group	Company	Hungary
Right Consents Community Edition	Fair&Smart,LuxTrust	Company	Luxemburg, Luxemburg
RUDI	City of Rennes	Public body	France
Salesforce	Salesforce	Company	US
SAP Customer consent	SAP	Company	Germany
Schluss	Foundation development Schluss	Non-profit	Netherlands
Schluss	Schluss	Non-profit	Netherlands
Self Innovations	Self Innovations, Inc.	Company	US
Sensotrend	Sensotrend Oy	Company	Finland
Signatu	Signatu	Company	Norway
Smart Species	Digital Transparency Lab	Non-profit	UK
Solid	MIT	Research institute	US
SOWL	esatus AG	Company	Germany

Solution name	Solution provider(s)	Provider type	Provider country
Spartacus	Spartacus	N/A	US
Startup Commons Global	Digiole	Company	Finland
Termly	Termly Inc.	Company	US
Tink	Tink	Company	Sweden
Traq	Traq	Company	Norway
TribalData	Global Tree Initiative	Non-profit	US
Trinity Identity Provider	comuny GmbH	Company	Germany
Tritom	DataSpace Europe	Company	Finland
Tru	Tru Social Inc.	Company	US
TrustArc	TrustArc Inc	Company	US
Trustee	HIE of One	Company	US
UBDI	UBDI, Inc.	Company	US
UBDI	UBDI, Inc.	Company	US
USBOS	Indie Computing Corp	Company	US
use.id	Digita.ai	Company	Belgium
UUnivers	REVENA sa	Company	Switzerland
VALENCIADATA	Instituto de Biomecánica de Valencia (IBV)	Research institute	Spain
Valtti+	Vastuu Group Ltd	Company	Finland
Visions Galaxy	Visions	Company	France
VisionsTrust	Visions	Company	France
Yivi	Privacy by Design Foundation,SIDN Business BV	Non-profit, Company	Netherlands, Netherlands

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:
— by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
— at the following standard number: +32 22999696,
— via the following form: european-union.europa.eu/contact-eu/write-us_en.

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

Open data from the EU

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

Science for policy

The Joint Research Centre (JRC) provides independent, evidence-based knowledge and science, supporting EU policies to positively impact society

EU Science Hub
joint-research-centre.ec.europa.eu

Publications Office
of the European Union