



November 2018

# GDPR Data Portability and Core Vocabularies

**DIGIT**  
Directorate-General for Informatics

**ISA<sup>2</sup> Programme**  
[ec.europa.eu/isa2](http://ec.europa.eu/isa2)

**Disclaimer:**

The views expressed in this study are purely those of the Author(s) and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

*The study was prepared for the European Commission by Deloitte.*

EUROPEAN COMMISSION

Directorate-General for Informatics (DIGIT)

Directorate D – Digital Services

Unit D2 – ISA<sup>2</sup> Programme

Contact: [isa2@ec.europa.eu](mailto:isa2@ec.europa.eu)

*European Commission*

*B-1049 Brussels*

This publication has been drafted under the 2016.07 *SEMIC: Promoting semantic interoperability amongst the EU Member States*. ISA<sup>2</sup> is a EUR 131 million programme of the European Commission, supporting the modernisation of public administrations in Europe through the development of interoperability solutions. More than 20 solutions are already available, with more to come soon. All solutions are open source and available free of charge to any interested public administration in Europe.

## Table of Contents

<b>1. INTRODUCTION .....</b>	<b>4</b>
1.1. PURPOSE OF THE STUDY.....	4
1.2. STRUCTURE.....	4
<b>2. CONTEXT .....</b>	<b>5</b>
2.1. DEVELOPING SOLUTIONS TO INTEROPERABILITY CHALLENGES.....	5
2.2. THE GDPR AND DATA PORTABILITY.....	5
<b>3. CORE VOCABULARIES AS A SOLUTION FOR DATA PORTABILITY .....</b>	<b>10</b>
3.1. ISA <sup>2</sup> SPECIFICATIONS: CORE VOCABULARIES.....	10
3.2. CORE VOCABULARIES AND THE GDPR.....	10
<b>4. CONCLUSIONS AND RECOMMENDATIONS.....</b>	<b>15</b>
4.1. CONCLUSIONS.....	15
4.2. RECOMMENDATIONS FOR POSSIBLE ACTION.....	15
<b>ANNEX I. REFERENCES .....</b>	<b>17</b>

## Table of Tables

Table 1 – Overview of ISA <sup>2</sup> technical specifications and legal provisions of the GDPR.....	12
---	----

## 1. INTRODUCTION

*This section explains the purpose and scope of this short study on data portability and the use of Core Vocabularies and presents the structure of the report.*

### 1.1. Purpose of the study

The ISA<sup>2</sup> programme, established for the 2016-2020 period, seeks to provide interoperability solutions and common frameworks for European public administrations, businesses and citizens with the objective to modernise the European public sector<sup>1</sup>. Numerous distinct actions<sup>2</sup> are funded through the programme for the development of tools, services and frameworks in the area of interoperability.

This study is carried out in the context of ISA<sup>2</sup> Action 2016.07 *SEMIC: Promoting semantic interoperability amongst the EU Member States*. The SEMIC action seeks to promote the use of semantic tools and solutions to address interoperability challenges faced by Member States when exchanging data for the execution of European Public Services. To support this objective, it has produced semantic specifications and solutions which are available to public administrations in Europe free of charge.

This study aims to examine the use and application of Core Vocabularies and, more specifically, the Core Person vocabulary as a potential enabler for the *data portability* right contained in the General Data Protection Regulation (GDPR)<sup>3</sup> and to assess how public administrations in the EU could comply with these provisions using Core Vocabularies.

### 1.2. Structure

This document is structured as follows:

- **Section 1** introduces the study, its purpose and structure.
- **Section 2** describes the current policy and legal context governing *data portability* regarding European public administrations.
- **Section 3** provides an overview of the ISA<sup>2</sup> Core Vocabularies and the Core Person Vocabulary as a potential solution to address identified challenges.
- Finally, **section 4** proposes conclusions and recommendations.

---

<sup>1</sup> Decision (EU) 2015/2240 of the European Parliament and of the Council of 25 November 2015 establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA<sup>2</sup> programme) as a means for modernizing the public sector.

<sup>2</sup> In this context, 'actions' are defined as projects, solutions already in an operational phase and accompanying measure (Art. 2 Decision (EU) 2015/2240).

<sup>3</sup> 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 – GDPR).

## 2. CONTEXT

*In this section, an understanding of the policy and legal context is outlined: first, the policy framework for promoting semantic interoperability between public administrations is briefly summarised; second, provisions on data portability of the GDPR are highlighted.*

### 2.1. Developing solutions to interoperability challenges

The ISA<sup>2</sup> programme continues to demonstrate the long-standing commitment of EU institutions to foster interoperability between European public services and stimulate the digitalisation of European public administrations through the development of digital solutions.

Promoting such interoperability, digital public services and seamless data flows between European public administrations requires to address different layers of interoperability.

On the semantic level, it is critical to ensure that individual data elements exchanged between public administrations are automatically recognised thanks to unambiguous, shared meaning. As such, semantic interoperability guarantees that the precise format and meaning of exchanged data is maintained and understood throughout their flow between parties<sup>4</sup>. Several ISA<sup>2</sup> actions seek to contribute to such objectives. The SEMIC action, in particular, contributes to the promotion of semantic interoperability amongst the EU Member States by providing semantic interoperability solutions.

Core Vocabularies, defined as *'simplified, re-usable and extensible data models that capture the fundamental characteristics of a data entity in a context-neutral and syntax-neutral fashion'*<sup>5</sup>, are examples of such solutions. The Core Vocabularies developed through the SEMIC action include the Core Person, Core Business, Core Location, Core Public Service, Core Criterion and Core Evidence and the Core Public Organisation Vocabularies

The Core Person Vocabulary *'provides a minimum set of classes and properties for describing a natural person, i.e. the individual as opposed to any role they may play in society or the relationships they have to other people, organisations and property; all of which contribute significantly to the broader concept of identity. The vocabulary is closely integrated with the Location and Business Core Vocabularies'*<sup>6</sup>.

### 2.2. The GDPR and Data Portability

The General Data Protection Regulation (GDPR), which came into effect in May 2018, provides a new framework for harmonised governance of data privacy rules across the EU and the protection and empowerment of EU citizens regarding the use of their personal data.

The GDPR has three main objectives enshrined in Article 1: first, it prescribes rules *'relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data'* (Article 1(1)); second, it *'protects fundamental rights and freedoms of natural persons and in*

---

<sup>4</sup> Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2017) 134 final, 'European Interoperability Framework -Implementation Strategy

<sup>5</sup> European Commission, ISA<sup>2</sup> solutions, [https://ec.europa.eu/isa2/solutions/core-vocabularies\\_en](https://ec.europa.eu/isa2/solutions/core-vocabularies_en)

<sup>6</sup> JoinUp: <https://joinup.ec.europa.eu/release/core-person-vocabulary/100>.

*particular their right to the protection of personal data’ (Article 1(2)); and third, it ensures that personal data within the EU can flow freely without restriction nor prohibition ‘for reasons connected with the protection of natural persons with regard to the processing of personal data’ (Article 1(3)).*

The GDPR provides harmonised requirements for the processing of personal data, including in digital format, between different parties within the EU. Such harmonised requirements allow to ensure that individuals, companies or organisations can operate under the same rules and obligations when dealing with the personal data of individuals in the EU.

The GDPR contains definitions and provisions regarding data portability, the most relevant of which are presented below. It is noteworthy that GDPR places “data portability” at the highest level of personal data protection given that it recognises it explicitly as a “right” of the data subject.

As specified in Article 1 of the Regulation, relating to the subject matter and objectives of the legal act, individuals, as natural persons or data subjects are at the core of the GDPR and are the main beneficiaries of rights protected under the Regulation.

Article 2 of the Regulation frames the material scope of the Regulation, which *‘applies to the processing<sup>7</sup> of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system’*. It thus applies to all forms of data processing, including automated means and is thus particularly relevant for the provision of digital public services by European public administrations. As the Regulation is equally applicable to both public sector and private, public administrations fall into the scope of GDPR.

Article 20 introduces the right to data portability for all individuals:

1. *‘the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where (a) the processing is based on consent pursuant to point (a) of Article 6(1)<sup>8</sup> or point (a) of Article 9(2)<sup>9</sup> or on a contract pursuant to point (b) of Article 6(1); and the processing is carried out by automated means.*
2. *In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.’*

As such, Article 20(1) lays down the right of data subjects to transmit their personal data to another controller without hindrance – whether these be legal, technical or financial – from the controller to which the personal data has been provided; the transmission of data shall be ensured in structured, commonly used and machine-

---

<sup>7</sup> Processing is understood as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4(2)).

<sup>8</sup> Article 6(1) stipulates that the ‘processing [of data] shall be lawful only if and to the extent that at least one’ of several conditions applies, including (a) *‘the data subject has given consent to the processing of his or her personal data for one or more specific purposes’* and (b) *‘processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract’*.

<sup>9</sup> Article 9(2) lays down conditions under which the processing of special categories of personal data is allowed. These conditions include explicit consent of the data subject or carrying out obligations of data controllers or public interest.



readable format. Potential obstacles, which would limit or delay access, transmission or reuse of personal data by the requesting data subject or by another data controller chosen by the data subject, are thus forbidden. This is applicable not only to the transmission of personal data from a data controller to the requesting data subject: a data subject may request the data controller that the latter transmits directly the data to another data controller.

Data processing by European public administrations may be out of the scope of the right of data portability as they are most of the time processing personal data in the public interest or in the exercise of official authority. It is, however, important to note that, at present, although public administrations rarely process personal data on the basis of consent or contracts, it is best practice that even these actors can positively reply to data portability requests, when they act as data controllers or processors. This on condition that they cannot deny or restrict this right based on another legal ground, be it a law, legal obligation to which they (public administrations) are subject or legitimate interest.

Several scenarios are useful to investigate for public administrations. There are indeed case in which public administrations may deal with citizens in a similar manner as a private entity (company) would do. For example, the collection of personal data via online forms or databases or the dissemination of newsletters, and, in any case, public administrations as data controllers should establish safeguards to ensure they act on behalf of data subjects and that only the personal data that the data subject wants to transfer is transferred. In such situations, the right to data portability may be of relevance for public administrations too.

The right to right is anticipated in recital (68) already, which states that *'where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability'*. When technically feasible, interoperable formats are recommended for data controllers, although there is no obligation for controllers to adopt or maintain technically compatible systems.

Article 12 sets out modalities for the exercise of the rights of the data subject, including transparency and communication by data controllers on the application of rights of data subjects. When facilitating the right of data portability upon request of the data subject, controllers could thus directly transmit data between two systems by electronic means, unless technical barriers prevent such transmission, in which case, *'the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action'* (Article 12.4).

It is also affirmed in Article 13.2 (b) that *'the controller shall, at the time when personal data are obtained, provide the data subject with [...] further information necessary to ensure fair and transparent processing'*, including *'the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability'*. It is thus the responsibility of data controllers to inform the data subject about their rights relating to the processing of their personal data, including the right to data portability.

The Article 29 Data Protection Working Party<sup>10</sup>, further referred to as the Art. 29 WP, was an advisory body composed of a representative from the data protection authority of each EU Member State, the European Data

---

<sup>10</sup> Art. 29 WP has been replaced, in May 2018, by the European Data Protection Board (EDPB) under Regulation (EU) 2016/679 (GDPR).

Protection Supervisor and the European Commission<sup>11</sup>. Since the adoption of the GDPR, the Art. 29 WP has been replaced by the European Data Protection Board (EDPB). The EDPB, established under Article 68, is tasked to *'ensure the consistent application of this Regulation'* (Article 70). The EDPB has endorsed and adopted opinions and guidelines of the Art. 29 WP.

The Art. 29 WP prepared extensive guidelines on the application of data portability under the GDPR<sup>12</sup>, interpreting and providing opinions on how to implement such rights in the context of the GDPR. The main elements of the Art. 29 opinion are summarized below:

- The right to data portability spelled out in Article 20 of the GDPR is closely related to the right of access<sup>13</sup> but differs in many ways, in particular, because data subjects are no longer constrained by the format chosen by the data controller complying with the request to access or transmit personal data. Data portability under the GDPR indeed stipulates that data subjects are able to move, copy or transmit their personal data without any hindrance from one IT environment to another.
- The right to data portability allows data subjects to obtain personal data they have provided to a data controller in a structured, commonly used and machine-readable format as well as to transfer such data to a different controller. The main purpose of this new right is to strengthen the control of data subjects over their personal data. As such, the main elements of data portability are:
  - the right to receive personal data;
  - the right to transmit personal data from one data controller to another data controller; and
  - strengthened control of the data subject over his data.
- The right to data portability only applies if the data processing is *'carried out by automated means'*, including electronic databases and register, and therefore does not cover paper-based data or paper-based supporting tools.
- Because it refers to the direct transmission of personal data from one data controller to another, the right to data portability represents a valuable tool to facilitate and stimulate the free flow of personal data in the EU, including between public administrations.
- Data portability, as defined under Article 20 (1)(a) of the GDPR, applies in the first instance only on the processing of data based on either the data subject's consent or on a contract to which the data subject is partly with the controller. This means that, based on the letter of GDPR, the right to data portability is not applicable when the data processing is necessary to perform a task executed in the

---

<sup>11</sup> Set up under Article 29 of Directive 95/46/EC and so the name.

<sup>12</sup> Article 29 Data Protection Working Party, Guidelines on the right to data portability, Adopted on 13 December 2016, as last revised and adopted on 5 April 2017 (16/EN WP 242 rev.01).

<sup>13</sup> The right of access was prescribed under Article 12 of the Data Protection Directive 95/46/EC, now replaced by the GDPR, as the right of data subjects, guaranteed by Member States, to *'obtain from the controller (a) without constraint at reasonable intervals and without excessive delay or expense:*

- *confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,*
- *communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,*
- *knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);*

*(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data; (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort'.*



public interest or in the exercise of official authority vested in the data controller, or when a data controller is exercising its public duties or complying with a legal obligation, as laid out in Article 20(3) and Recital 68.

- Developing means to prepare for data portability requests and the response to such requests is recognized as a good practice. Suggestions on how to best prepare include the downloading of tools and Application Programming Interfaces (APIs), which could be one of the means for ensuring that personal data are transmitted in a structured, commonly used and machine-readable format and that data formats are interoperable.
- Overall, cooperation between stakeholders is strongly encouraged to develop common sets of interoperable standards and formats to address the request of data portability, in line with the rights established by the GDPR. The European Interoperability Framework (EIF) is identified as a framework to take up such interoperability challenges for organisations delivering public services.

### 3. CORE VOCABULARIES AS A SOLUTION FOR DATA PORTABILITY

*This section seeks to address the key question of how can the Core Person Vocabulary facilitate compliance with the data portability provisions of the GDPR, for public administrations across the EU, reconciling technical aspects of electronic exchange of data with semantic solutions and legal aspects of data portability.*

#### 3.1. ISA<sup>2</sup> specifications: Core Vocabularies

Common specifications for standards and formats would allow controllers, including public administrations, to adequately respond to data portability requests by data subjects. Under the ISA<sup>2</sup> Programme, several Core Vocabulary specifications were developed as early as 2010. These Core Vocabularies are defined as *'simplified, reusable and extensible data models that capture the fundamental characteristics of a data entity in a context-neutral and syntax-neutral fashion'*<sup>14</sup>

The Core Person Vocabulary, as a simplified, reusable, and extensible data model, describing a natural person in a context-neutral way is useful for information exchange between systems. It encompasses the fundamental characteristics of a person, e.g. name, gender, date of birth, location.

#### 3.2. Core Vocabularies and the GDPR

In order to comply with the GDPR, data controllers are faced with two distinct yet complimentary paths for providing portable data to the data subjects or to other data controllers:

- a direct transmission of a dataset of portable data (use case 1); and
- an automated tool allowing the integration of relevant data (use case 2).

Data portability is facilitated by interoperable systems and, as such, Core Vocabularies as semantic interoperability solutions could contribute to such objectives, allowing the reuse of existing data models. Interoperability solutions, such as Core Vocabularies, are thus enablers for the right to data portability of EU citizens.

More specifically, Core Vocabularies could be useful for data controllers to comply with data portability requests for both in both of the above-mentioned use cases.

First, the direct transmission of portable data must be ensured in structured, commonly used and machine-readable format. The Core Vocabularies focus only on fundamental characteristics of an entity. The Core Person vocabulary, in particular, encompasses the fundamental – and most common – characteristics of a person, e.g. name, gender, date of birth, location and captures these characteristics in a context-neutral way. These elements are typically used when processing personal data. It thus provides a potential solution for interoperability among people databases and registers, such as criminal case registers for example, or other ICT based solutions for the processing and exchange of personal-related data between European public administrations. Existing uses of the Core Person vocabulary by public administrations in the EU demonstrate

---

<sup>14</sup> European Commission, ISA Programme, eGovernment Core Vocabularies: The SEMIC.EU approach, 2011.

the usefulness of such vocabulary for the electronic exchange of data related to persons between public administrations, including contact information, by ensuring structured and machine readable data can be exchanged and reused. The Core Person Vocabulary could thus provide the basis of a context-specific data model used to facilitate the processing and exchange data about persons among existing information systems of data controllers, including European public administrations, and in particular, provide a solution for interoperability among people registers or other electronic databases relating to individuals.

Second, Core Vocabularies could also prove useful should data controllers opt to comply with data portability requests through the use of automated tool allowing the integration of relevant data. Core Vocabularies indeed allow for data integration or the combination of heterogeneous data from disparate sources or systems and create a data mash-up or the integration of multiple datasets in a single interface. Again, the use of Core Vocabularies by public administrations – including Core Person - have demonstrated the benefits of using these vocabularies to integrate and link data across public administration systems, within a single Member State as well as in cross-border contexts. In such case, public administrations, acting as data controllers, could readily comply with requests for data portability by data subjects.

The table highlights how technical specifications of Core Vocabularies, and in particular the Core Person Vocabulary, are relevant to legal provisions and in particular rights and obligations related to data portability under the GDPR.

**Table 1 – Overview of ISA<sup>2</sup> technical specifications and legal provisions of the GDPR**

	Data subject	Data controller
<b>Legal provisions: data portability from a legal perspective</b>		
<b>Receipt of personal data</b>	The data subject is entitled to receive personal data, which has been provided to a controller by the data subject itself.	<p>The data controller must provide personal data to data subject upon request.</p> <p>The controller has no obligation, according to the GDPR, to adopt or maintain processing systems which are technically compatible in order to address a data subject's right to transmit or receive personal data concerning it; it is however advisable. Depending on how implementation of GDPR will evolve and how its principles will be embodied in the national legal regime of the Member States, it is likely that data controllers will <i>de facto</i> be required later to adopt interoperable systems. Yet, even under the actual state of play, no adoption of interoperable systems will practically render the implementation of the data portability right void of its practical meaning and sense in many cases.</p>

	Data subject	Data controller
<b>Transmission of personal data</b>	The data subject is entitled to request personal data from one controller and its transmission to another. The data subject has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.	The data controller must transmit data to another data controller, in a specific format (structured, commonly used and machine-readable) upon request of the data subject and when technically feasible.
<b>Technical specifications: data portability from an (semantic) interoperability perspective</b>		
<b>Format of personal data</b>	The data subject has the right to receive the data in a structured, commonly used and machine-readable format. The format should allow data subjects to read and transmit personal data to another data controller in a manner that allows its (re)use.	There is no obligation, according to the GDPR, for compatible systems between data controllers to address data subject's data portability requests. However, there is a need for interoperable formats and systems to enable controllers to address such requests. Therefore, when there are no commonly used formats for a given industry or given context, data controllers should provide personal data using commonly used open formats (e.g. XML, JSON, CSV,...) along with useful metadata. The latter can be achieved through the use of Core Vocabularies, as a simplified, reusable, and extensible data model describing specific sets of data.  The Core Person Vocabulary, in particular, covers and describes identified fundamental characteristics of natural persons. It could thus be a cost-efficient, time-efficient and established solution to such data portability requests.

	Data subject	Data controller
<b>Interoperable Processing systems</b>	Interoperable processing systems enable data subjects to exercise their right to data portability under the GDPR.	Compatible systems are by no means required by the GDPR. Interoperable processing systems, however, are decidedly encouraged. Ultimately, a common set of interoperable standards and formats are highly desirable to comply with requirements of the right to data portability, allowing for the integration and the exchange of personal data between the processing systems of different controllers.

## 4. CONCLUSIONS AND RECOMMENDATIONS

*This section summarises the main findings and presents some recommendations emerging from the previous analysis for consideration.*

### 4.1. Conclusions

Several conclusions can be drawn from the above assessment:

- The GDPR came into effect in May 2018 and provides a new framework for harmonised governance of data privacy rules across the EU and for the protection and empowerment of EU citizens regarding the use of their personal data.
- Article 20 introduces the right to data portability for all individuals and the right of data subjects to transmit their personal data to another controller without hindrance – whether these be legal, technical or financial – from the controller to which the personal data have been provided. This is also applicable to direct transmission from controller to controller upon explicit request of data subject.
- Data controllers are expected to transmit personal data in an interoperable format. As such, *‘structured, commonly used and machine-readable’* are means for enabling data portability, while interoperability is the desired outcome.
- Developing means to prepare for data portability requests and the response to such requests is recognised as a good practice, even for public administrations and institutions acting in the public sector or vested with public service/public authority tasks.
- Core Vocabularies as *‘simplified, re-usable and extensible data models that capture the fundamental characteristics of a data entity in a context-neutral and syntax-neutral fashion’*, are examples of such solutions to enable data portability from a technical point of view and provide means to transmit personal data in an interoperable format.
- The Core Person Vocabulary could in such situations provide a solution for interoperability among people registers or other electronic databases relating to individuals and facilitate the processing and exchange of data about persons.

### 4.2. Recommendations for possible action

In the light of the above conclusions a number of steps can be taken to support public administrations to ensure the right to data portability of EU citizens, notably through the use of common specifications:

- Developing means to prepare for data portability requests and the response to such requests is highly advisable; means include common specifications for the format to exchange personal data. A teleological interpretation of GDPR would indeed suggest that there is a strong recommendation – if not request – of the EU legislator towards Member States to support national self-regulatory initiatives or take part in co-regulatory initiatives with the private sector (system owners and applications developers) with the objective to work on technical means, applications and method that would promote interoperability.



- Dialogue, mutual learning and exchanging of best practices between European public authorities could allow better preparedness for cooperation in case of portability requests.
- The use of existing specific semantic tools, including those developed under the ISA<sup>2</sup> programme, could allow public administrations to ensure that personal data are transmitted in a structured, commonly used, and machine-readable format and that data formats are interoperable.

## Annex I. REFERENCES

- Article 29 Data Protection Working Party, Guidelines on the right to data portability, Adopted on 13 December 2016, as last revised and adopted on 5 April 2017 (16/EN WP 242 rev.01). Available via: [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=44099](http://ec.europa.eu/newsroom/document.cfm?doc_id=44099).
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM(2017) 134 final, 'European Interoperability Framework -Implementation Strategy. Available via: [https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_1&format=PDF).
- Decision (EU) 2015/2240 of the European Parliament and of the Council of 25 November 2015 establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA<sup>2</sup> programme) as a means for modernizing the public sector. Available via: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015D2240>.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available via: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046>.
- European Commission, ISA Programme, eGovernment Core Vocabularies: The SEMIC.EU approach, 2011. Available via: <https://joinup.ec.europa.eu/sites/default/files/document/2011-12/egovernment-core-vocabularies.pdf>.
- European Commission, ISA<sup>2</sup> solutions, [https://ec.europa.eu/isa2/solutions/core-vocabularies\\_en](https://ec.europa.eu/isa2/solutions/core-vocabularies_en)
- European Commission, e-Government Core Vocabularies Handbook: Using horizontal data standards for promoting interoperability, 2015. Available via: [https://ec.europa.eu/isa2/library/e-government-core-vocabularies-handbook\\_en](https://ec.europa.eu/isa2/library/e-government-core-vocabularies-handbook_en).
- JoinUp: <https://joinup.ec.europa.eu/release/core-person-vocabulary/100>).
- 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). Available via: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>.

## **An action supported by ISA<sup>2</sup>**

ISA<sup>2</sup> is a EUR 131 million programme of the European Commission which develops digital solutions that enable interoperable cross-border and cross-sector public services, for the benefit of public administrations, businesses and citizens across the EU. ISA<sup>2</sup> supports a wide range of activities and solutions, among which is the Semantic Interoperability Community (SEMIC) action.

ISA<sup>2</sup> solutions can be used free of charge and are open source when related to IT.

## **More on the programme**

[ec.europa.eu/isa2](http://ec.europa.eu/isa2)

## **Contact ISA<sup>2</sup>**

[isa2@ec.europa.eu](mailto:isa2@ec.europa.eu)

## **Follow us**



**@EU\_ISA2**  
**@Joinup\_eu**



**isa<sup>2</sup> programme**