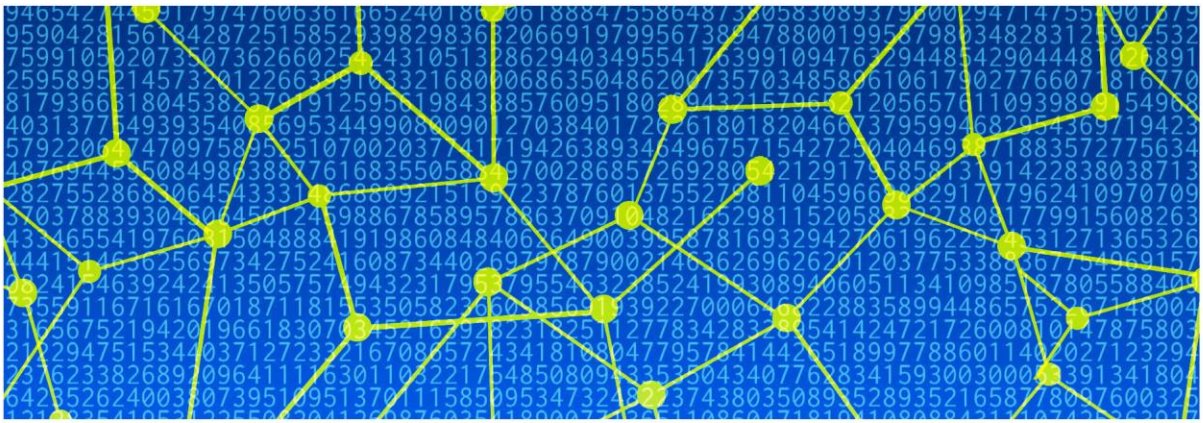

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 8/2017

EDPS Opinion on the proposal for a Regulation establishing a single digital gateway and the 'once-only' principle

EDPS

1 August 2017

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41(2) of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 28(2) of Regulation 45/2001, the Commission is required, 'when adopting a legislative Proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data...', to consult the EDPS.

He was appointed in December 2014 together with the Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion responds to a formal consultation by the European Commission pursuant to Article 28(2) of Regulation 45/2001, as well as to a concurrent consultation by the European Parliament and provides comments and recommendations on how to better safeguard the right to privacy and the protection of personal data in the proposed Regulation establishing a Single Digital Gateway and amending the IMI Regulation (1024/2012).

Executive Summary

The Proposal is among the first EU instruments that explicitly refer to and implement the principle of *'once-only'*, which is aimed at ensuring that citizens and businesses are requested to supply the same information only once to a public administration, which can then re-use the information they already have. The Proposal foresees that the exchange of evidence for specified cross-border procedures (such as, for example, requesting recognition of a diploma) would be initiated by the explicit request of a user and it would take place in a technical system established by the Commission and Member States, with a built-in preview mechanism ensuring transparency towards the user.

The EDPS welcomes the Commission's proposal to modernise administrative services and appreciates their concerns for the impact this Proposal may have on the protection of personal data. The Opinion is issued upon the specific request of both the Commission and of the Parliament. It is also inspired by the priorities of the Estonian Presidency of the Council, which specifically includes *'digital Europe and the free movement of data'*.

In addition to providing specific recommendations to further improve the quality of legislation, the EDPS also wishes to seize this opportunity to provide an introductory overview of key issues related to the *'once-only'* principle in general, although many such concerns are not necessarily borne out by the Proposal in its present form. These relate, in particular, to the legal basis of the processing, purpose limitation, and data subject rights. The EDPS stresses that in order to ensure successful implementation of EU-wide *'once-only'*, and enable lawful cross-border exchange of data, *'once-only'* must be implemented in line with relevant data protection principles.

With regard to the Proposal itself, the EDPS supports the efforts made to ensure that individuals remain in control of their personal data, including by requiring *'an explicit request of the user'* before any transfer of evidence between competent authorities and by offering the possibility for the user to *'preview'* the evidence to be exchanged. He also welcomes the amendments to the IMI Regulation that confirm and update the provisions on the coordinated supervision mechanism foreseen for IMI and would also enable the European Data Protection Board *('EDPB')* to benefit from the technical possibilities offered by IMI for information exchange in the context of the General Data Protectoin Regulation (GDPR).

The Opinion provides recommendations on a range of issues, focusing on the legal basis for the cross-border exchange of evidence, purpose limitation, and the scope of the *'once-only principle'* as well as practical concerns surrounding user control. Key recommendations include clarifying that the Proposal does not provide a legal basis for using the technical system for exchanging information for purposes other than those provided for in the four directives listed or otherwise foreseen under applicable EU or national law, and that the Proposal does not aim to provide a restriction on the principle of purpose limitation under the GDPR; as well as clarifying a range of issues relating to the practical implementation of user control. With regard to the amendments to the IMI Regulation, the EDPS recommends adding the GDPR to the Annex of the IMI Regulation to allow the potential use of IMI for the purposes of data protection.

TABLE OF CONTENTS

I. Contents

1. INTRODUCTION AND BACKGROUND 5

2. THE 'ONCE-ONLY' PRINCIPLE AND DATA PROTECTION 7

3. RECOMMENDATIONS 11

3.1. LEGAL BASIS FOR THE CROSS-BORDER EXCHANGE OF EVIDENCE (ARTICLE 12) 11

3.2. PURPOSE LIMITATION (ARTICLE 12(6)) 13

3.3. *'EXPLICIT REQUEST OF THE USER'* (ARTICLE 12(4)) 14

3.4. *'PREVIEW'* (ARTICLE 12(2)(E)) 15

3.5. DEFINITION OF EVIDENCE; RANGE OF ONLINE PROCEDURES COVERED (ARTICLES 3(4) AND 2(2)(B)) 15

3.6 FURTHER RECOMMENDATIONS: AMENDMENTS TO THE IMI REGULATION (ARTICLE 36) 16

3.7 DATA PROTECTION AS AN INFORMATION AREA AND DATA PROTECTION AUTHORITIES AS PROBLEM SOLVERS (ARTICLE 2 AND ANNEXES I AND III) 17

4. CONCLUSIONS 18

Notes 21

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to 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[1], and to 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)[2],

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[3], and in particular Articles 28(2), 41(2) and 46(d) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION AND BACKGROUND

On 2 May 2017, the European Commission (*'Commission'*) adopted a Proposal for a Regulation of the European Parliament and of the Council on establishing a single digital gateway to provide information, procedures, assistance and problem solving services and amending Regulation (EU) No 1024/2012[4] (*'Proposal'*).

The aim of the Proposal is to facilitate citizens' and businesses' cross-border activities by offering them user-friendly access, through a single digital gateway, to information, procedures and assistance and problem-solving services they need for exercising their internal market rights. In this respect, this Proposal represents an important initiative in the Commission's journey to develop a deeper and fairer internal market as well as a Digital Single Market[5].

Articles 4 to 6 of the Proposal outline the 'gateway services' offered by the single digital gateway. These closely mirror the title of the Proposal itself and include:

- access to information,
- access to procedures and
- access to assistance and problem solving services.

It is also notable that the Proposal, in its Article 36, seeks to amend several provisions of Regulation (EU) No 1024/2012 (the *'IMI Regulation'*)[6], which establishes the legal basis for the operation of the Internal Market Information System (*'IMI'*)[7].

The Proposal is among the first EU instruments that explicitly refer to and implement the principle of *'once-only'*[8]. The Proposal refers to the notion of once-only and its benefits by explaining that *'citizens and businesses should not have to supply the same information to public authorities more than once for the cross-border exchange of evidence'*[9]. The Proposal foresees that the exchange of evidence for specified procedures would be initiated by the

request of a user and it would take place in the technical system established by the Commission and Member States[10] (for further details, see Section 3 below).

This Opinion is in response to a request of the Commission and a subsequent separate request of the European Parliament (*'Parliament'*) to the European Data Protection Supervisor ('*EDPS'*), as an independent supervisory authority, to provide an opinion on the Proposal. The EDPS welcomes that he has been consulted by both institutions. The Opinion follows an informal consultation by the Commission of the EDPS prior to the adoption of the Proposal.

The EDPS takes note and welcomes the Commission's proposal to modernise administrative services by facilitating the availability, quality and accessibility of information across the European Union. He also highlights, in particular, that the *'once-only'* principle could contribute towards these goals, subject to compliance with applicable data protection law and respect for the fundamental rights of individuals.

The EDPS appreciates the Commission's and Parliament's concerns for the impact this Proposal may have on the protection of personal data. He welcomes that many of his informal comments have been taken into account. In particular, he supports:

- the efforts made to ensure that individuals remain in control of their personal data, including by requiring *'an explicit request of the user'* before any transfer of evidence between competent authorities (Article 12(4)), and by offering the possibility for the user to *'preview'* the evidence to be exchanged (Article 12(2)(e));
- the efforts made to define the material scope of application for the principle of *'once-only'* (Article 12(1)); and
- the explicit requirement of using anonymous and/or aggregate data for collection of relevant user feedback and statistics (Articles 21-23);
- moreover, he welcomes the proposed amendment of the IMI Regulation which confirms and updates the provisions on coordinated supervision mechanism foreseen for IMI in order to ensure a consistent and coherent approach (Article 36(6)(b);
- finally, more general provisions showing commitment to ensuring the respect for the fundamental rights of individuals, including the right to protection of personal data, such as those in recitals 43 and 44 and Article 29 are also welcome.

The purpose of this Opinion is to provide specific recommendations to address remaining data protection concerns and thereby further improve the quality of legislation (see Section 3 below). Of the three gateway services listed above, this Opinion will focus on *'access to procedures'* (Article 5) and in particular, the provisions relating to the *'cross-border exchange of evidence between competent authorities'* under Article 12, as these are most relevant for the protection of personal data. The remainder of the Proposal (including its provisions on access to information and access to assistance and problem-solving services) raises fewer relevant concerns. Further, the EDPS also briefly comments on selected amendments to the IMI Regulation.

In addition, the EDPS wishes to seize this opportunity to provide an introductory overview of key issues related to the *'once-only'* principle in general, although many such concerns are not necessarily borne out by the Proposal in its present form (see Section 2 below).

2. THE 'ONCE-ONLY' PRINCIPLE AND DATA PROTECTION

There is no uniformly agreed definition of the principle of *'once-only'*: indeed, it can be implemented in different ways and to varying degrees[11]. Generally, *'once-only'* implies exchange of information or documents (automatically or on request) between various government departments for purposes of fulfilment of their public tasks. The objective is to lessen administrative burdens, facilitate reuse of information and help avoid -as the name suggests- that individuals and businesses have to submit the same documents or information to the government more than once.

'Once-only' under the EU eGovernment Action Plan 2016-2020: potential benefits

The EU eGovernment Action Plan 2016-2020 recognises that opening data between public administrations would *'increase their efficiency and facilitate the free movement of businesses and citizens'*[12]. A study prepared for the Commission, *EU-wide digital Once-Only Principle for citizens and businesses* ('Smart Study'), reinforces this claim and recognises that a European wide application of the principle of *'once-only'* could offer significant benefits to public administration, individuals and businesses[13]. Moreover, it explains that applying the principle across the European Union could live up to the expectation of non-nationals to receive services without being subject to unnecessary administrative burdens[14].

The eGovernment Action Plan 2016-2020 referred to above describes the *'once-only'* principle as follows: *'public administrations should ensure that citizens and businesses supply the same information only once to a public administration'*[15]. In consequence, governments will no longer make *'multiple requests for the same information when they can use the information they already have'*[16] and no additional burden will be placed on citizens and businesses[17]. In essence, this means that competent authorities would be allowed (or indeed required) to exchange and use (further process) data (including personal data) in a different context and for a different purpose than was intended when the data were initially collected. Indeed, the Smart Study recognises that *'once-only' 'depends on collective understanding and acceptance of data reuse'*[18].

Data protection aspects

The *'once-only'* principle -depending on the way in which it is defined and implemented- may potentially raise some questions in relation to the protection of personal data including, in particular, in relation to:

- the legal basis for the processing;
- purpose limitation and data minimisation
- and data subject rights.

The EDPS stresses that in order to ensure successful implementation of EU-wide *'once-only'*, and enable lawful cross-border exchange of data, once-only must be implemented fully in line with relevant data protection principles[19]. Some of the key data protection issues are highlighted below.

Legal basis of the processing

Article 6 of the General Data Protection Regulation (henceforth *'GDPR'*)[20] requires that personal data shall only be processed if at least one of six legal grounds listed in that Article applies. This requirement is related to the broader principle of *'lawfulness'* set forth in Article 5(1)(a), which

requires that personal data must be processed 'lawfully'. The three most relevant legal grounds for implementing the *'once-only'* principle are consent[21], legal obligation[22] and public task/official authority[23].

Depending on the circumstances, one or another of these legal basis could be the most appropriate choice. The following subsections provide a quick overview of each ground and a few practical examples.

As a general rule of thumb, for the case of any recurring and structural data sharing, the EDPS recommends -in order to ensure legal certainty- that whenever possible, further processing of personal data based on the once-only principle be specified in a legislative instrument, which provide appropriate safeguards to ensure compliance with data protection law, including the principle of purpose limitation and ensuring data subjects' rights[24].

The legislative instrument introducing application of the principle of *'once-only'* should be clear on whether any government data sharing is subject to freely given, specific, informed and unambiguous consent of the individuals concerned; or whether the law creates an obligation or a permission for data sharing.

To ensure legal certainty, it is normally also helpful if the law clearly specifies the legal basis for processing of personal data (typically in the main body of the legal instrument or in a recital where sufficient and appropriate).

Consent

If used appropriately, consent can afford the data subjects a good degree of control over their personal data. However, this requires that consent fulfil the requirements of the GDPR: it should be freely given, specific, informed and unambiguous. These requirements have been elaborated upon by the WP29 in its Opinion 15/2011 on Consent[25] and further specified in the GDPR.

One of the conditions for valid consent is that it is freely given[26]. The GDPR provides that consent cannot be considered to be freely given -and therefore lawful- if there is a clear imbalance between the data subject and the controller.

Although every situation is to be assessed on a case-by-case basis, such an imbalance is likely to exist where the controller is a public authority[27]. If *'once-only'* were to be based on the consent of the data subject, sufficient safeguards must be in place ensuring freely given consent. Consent cannot be 'coerced'.

Legal obligation

A controller may rely on the legal ground of legal obligation where *'processing is necessary for compliance with a legal obligation to which the controller is subject'*[28]. This legal ground may be used both by private and public entities where the obligation to process personal data is imposed by law[29].

It cannot be used as a legal ground in cases where the law merely permits a processing, but does not require it. Further, as explained by the WP29 in its Opinion 6/2014 on legitimate interest[30], the law imposing the legal obligation must fulfil *'all relevant conditions to make the obligation valid and binding, and must also comply with data protection law, including the requirement of necessity, proportionality and purpose limitation'*[31]. Moreover, in order to be

able to rely on this legal basis, a controller cannot have *'an undue degree of discretion on how to comply with the legal obligation'*[32].

Recital 45 of the GDPR sets out further specifications for the law imposing the obligation. Among others, the law must specify the purposes of processing, provide specifications for determining the controller, specify the type of personal data processed, entities to which data may be disclosed, purpose limitations, storage period and *'other measures to ensure lawful and fair processing'*.

In conclusion, appropriate use of the legal ground of legal obligation contributes to legal certainty to the processing of personal data and may therefore be an appropriate legal ground in many situations of government data sharing, especially when the risks to the protection of personal data are high. At the same time, the limitations of this legal ground must also be born in mind: it is a less flexible legal ground and may therefore restrict the controller's ability to choose and optimise their processing activities to specific circumstances. In addition, it also cannot be used in situations when the controller is authorised but not required to share personal data.

Public task/exercise of official authority

Finally, Article 6(1)(e) provides that a controller may process personal data where *'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'*. A controller can only rely on this legal basis if there is a Union or Member State law setting out the public interest task[33].

This legal ground is very similar to that of legal obligation elaborated upon above. Indeed, the specific requirements of recital 45 of the GDPR summarised above also equally apply to this legal ground. Therefore, in practice, there is a great deal of specificity that this legal ground also requires, while at the same time, allowing some more flexibility to the organisation processing the data.

Further, unlike the legal ground of legal obligation, the law may allow the controller some discretion whether or not to share data and may therefore also apply in cases where there is a legal authorization but not a mandatory requirement for data sharing[34]. Moreover, it is an important additional safeguard that -just like in case of processing on legitimate interest grounds- data subjects have the right to object to processing based on this legal ground[35].

Purpose limitation

In order to comply with the purpose limitation principle, Article 5(1)(b) of the GDPR requires that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner which is incompatible with those purposes.

To implement this principle (subject to some notable exceptions as will be discussed below), Article 6(4) of the GDPR then requires that the different purposes for which personal data are to be processed should be assessed against the purpose for which the data were initially collected in order to ensure compatibility. Article 6(4) lists the following factors, which must, in particular, be taken into account during the compatibility assessment:

- link between the initial and further purposes;
- context of collection, including the relationship between the individual and the controller;

- nature of the data (including whether special categories of data are processed);
- the possible consequences for the individuals, and
- safeguards (including encryption or pseudonymisation)[36].

A novelty in the GDPR is that Article 6(4) also codifies an exception to the principle of purpose limitation for the case if the further processing is based on consent or Union or Member State law[37].

However, this is not an open-ended permission to enact any sweeping and generic legislative text to allow for unlimited reuse of personal data across government departments. In line with the Charter of Fundamental Rights, the law must meet certain requirements if the principle of purpose limitation is to be derogated from.

In particular, it *must 'constitute a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1)'*. These include national security, defence, fight against crime and other specifically listed objectives of general public interest.

Some of these types of public interests listed may be relevant for some specific and targeted applications of the once-only principle (for example, certain necessary and proportionate measures in the fight against crime under Article 23(1)(d) or in connection with the collection of tax revenues under Article (e)).

Easing administrative burden on individuals or organisations, increasing efficiency of administrative procedures, and saving time and resources, which are often the primary aims of *'once-only'* implementations are undoubtedly worthwhile public interest objectives. Nevertheless, they are not specifically listed under Article 23(1) and do not, in and of themselves, provide a lawful ground for restricting the principle of purpose limitation for these purposes. That being said, as noted before, it cannot be excluded that in some specific cases one or another of the legal grounds for restrictions under Article 23(1)(d) may be appropriate.

In conclusion, and in line with the foregoing, and unless an appropriate ground for restriction under Article 23(1) is available, or the data subjects concerned have given their consent, the principle of purpose limitation must be complied with even when there is Union and Member State law which provides for the implementation of the once-only principle.

User control, transparency and personal information management systems (PIMS)

In his Opinion on *'Meeting the challenges of big data'*[38] the EDPS argued that transparency and user control should help ensure that individuals are empowered to challenge misuse and prevent the secondary use of data for purposes that do not meet their legitimate expectations.

These considerations equally apply to government data sharing in the context where the *'once-only'* principle is applied. Indeed, in his Opinion 9/2016 of 20 October 2016 on Personal Information Management Systems (PIMS)[39], the EDPS explained that features in information management systems to allow user control can be very useful to enhance transparency and traceability. The Opinion specifically highlighted that public sector bodies can take advantage of these features in order to allow citizens to better manage access and use of their data.

Such features could indeed facilitate informing individuals about government data sharing. For example, by looking at their dashboard in their PIMS (and/or by receiving an alert on their smart phones) individuals could keep track of whether their personal data have been transferred between two different public administrations in cases where transfers are defined by law. PIMS

can also help individuals to effectively manage their consent for possible further use in cases where their consent is required for such use.

Finally, the Opinion suggested that an initiative by public eGovernment services to accept PIMS as a data source instead of direct data collection could add critical mass to the acceptance of PIMS.

Data minimisation and other data protection principles

In addition to the issues highlighted above, lawful implementation of *'once-only'* also has to ensure compliance with the remaining principles of data protection, including the principles of fairness, transparency[40], data minimisation, accuracy, storage limitation, integrity and confidentiality[41] as well as data protection by design and by default[42]. In line with the principle of accountability, competent authorities must be able to demonstrate compliance with these aforementioned principles[43].

For example, the Smart Study identified that public authorities collect a lot of unnecessary data because such data used to be relevant for a particular purpose in the past[44]. Such a practice does not comply with either the purpose limitation or the data minimisation principle and should be reviewed prior to any implementation of *'once-only'*.

3. RECOMMENDATIONS

As noted in Section 1, the EDPS welcomes the efforts made to address data protection concerns while drafting these provisions. At the same time, in order to further improve the quality of legislation, increase legal certainty, reinforce transparency and user control, the EDPS provides further recommendations with regard to the exchange of evidence, in particular, on the following issues:

- legal basis for the exchange of evidence (Article 12(1));
- purpose limitation;
- the notion of explicit request (Article 12(4));
- the notion and consequences of the preview (Article 12(2)(e));
- definition of evidence and range of online procedures covered (Articles 3(4) and 2(2)(b))

The recommendations in this Opinion focus on the provisions relating to the *'cross-border exchange of evidence between competent authorities'* under Article 12, as these provisions are most relevant for the protection of personal data. These recommendation are discussed under Sections 3.1 to 3.5 below and will be followed by additional recommendation on other relevant parts of the Proposal in Sections 3.6 and 3.7.

3.1. Legal basis for the cross-border exchange of evidence (Article 12)

Article 12(1) provides that for certain specified online procedures a technical system shall be established by the Commission (in cooperation with the Member States) for the electronic exchange of evidence between competent authorities in different Member States. The same provision specifies which online procedures come under the scope of the requirement to use this technical system for the exchange of cross-border evidence.

In particular, Article 12(1) refers to procedures based on the following four directives: Directive on recognition of professional qualification[45], the Services Directive[46], the Directive on public procurement[47] and the Directive on procurement by entities operating in the water, energy, transport and postal services sectors[48].

In addition, Article 12(1) also refers to the online procedures listed in Annex II of the Proposal. These include:

- requesting birth certificates;
- applications for study grants;
- registering for social security benefits;
- recognition of diplomas;
- change of address, issue or renewal of an ID card or a passport, registration of motor vehicles;
- claims for a pension or pre-retirement benefits;
- general registration of business activity; registration of an employer (a natural person) with public or semi-public pension and insurance schemes; registration of employees with public or semi-public pension and insurance schemes;
- notification to the social security schemes of the end of contract with an employee, payment of social contributions for employees.

One of the main concerns of the EDPS is that it is not sufficiently clear from the Proposal what is the legal basis for the processing of personal data for the purpose of the cross-border exchange of evidence. In particular, whether the exchange of evidence is based on a legal obligation[49], or a public task/official authority[50].

By stipulating that competent authorities *'shall... request evidence directly from competent authorities issuing evidence in other Member States through the technical system'* and that *'issuing authorities shall ... make such evidence available through the same system'*, Article 12(4) appears to suggest that the competent authorities are under a legal obligation to make the evidence available, once requested by their counter-parts in the requesting Member State. This, in turn, may suggest that the legal basis is either legal obligation or performance of a task in the public interest. Recital 28, which provides that *'this Regulation should ... provide the basis for the exchange of evidence directly between the competent authorities concerned, ... at the request of citizens and businesses'* also appears to support this latter conclusion[51].

To ensure legal certainty, the EDPS recommends explicitly stating the legal basis of the exchange of evidence in a substantive provision.

Before making a recommendation as between these options, it is important to distinguish the legal basis of the exchange of evidence itself on the one hand and the legal basis for exchanging the evidence via the technical system specified in Article 12.

As mentioned at the start of this Section 3, for the exchange of evidence itself, Article 12(1) refers to procedures based on the four directives listed therein. In addition, Article 12(1) also refers to the online procedures listed in Annex II of the Proposal (without clarifying further the legal basis for those exchanges).

Another, separate matter is what is the legal basis for using the technical system specified in Article 12 for the exchange of evidence.

To help ensure legal certainty, the EDPS recommends that a recital be added to specify that:

- the Proposal itself does not provide a legal basis for exchanging evidence, and that any exchange of evidence under Article 12(1) must have an appropriate legal basis elsewhere, such as in the four directives listed in Article 12(1) or under applicable EU or national law;
- the legal basis for the use of the technical system specified in Article 12 for the exchange of evidence is performance of a task in the public interest under Article 6(1)(e) of the GDPR; and that
- users have the right to object to the processing of their personal data in the technical system pursuant to Article 21(1) of the GDPR.

3.2. Purpose limitation (Article 12(6))

Article 12(6) of the Proposal limits the cross-border exchange of evidence between competent authorities for online procedures to evidence that is *'strictly limited to what has been requested'.*

The EDPS welcomes the Commission's intention to respect the principle of purpose limitation. As mentioned above in Section 2, the principle of purpose limitation is a key principle of data protection requiring that personal data must be *'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes'*[52].

As mentioned at the start of this Section 3, pursuant to Article 12(1) of the Proposal, the *'once-only'* principle would apply to the exchange of evidence for online procedures listed in its Annex II. In addition, it would also apply to any cross-border exchange of evidence under the four directives listed in Article 12(1) of the Proposal.

As we explained in Section 2, the principle of *'once-only'* potentially challenges the principle of purpose limitation in the sense that personal data that have been collected by public authorities for a specific purpose should not be asked for again but instead be processed for future administrative purposes. However, it is our understanding that the objective of the Proposal is not to allow information exchange beyond what is already foreseen in applicable sectoral EU legislation (i.e. the four directives listed above) or under other applicable EU or national law. It is also our understanding that the Proposal does not aim to provide any restriction on the principle of purpose limitation under Articles 6(4) and 23(1) of the GDPR.

In order to ensure legal certainty, however, the EDPS recommends adding a recital to the Proposal confirming this understanding. In particular, the recital should:

- clarify that the Proposal does not provide a legal basis for using the technical system for exchanging information for purposes other than those provided for in the four directives listed or otherwise foreseen under applicable EU or national law;
- and that the Proposal does not in any way aim to provide a restriction on the principle of purpose limitation pursuant to Articles 6(4) and 23(1) of the GDPR.

3.3. *'Explicit request of the user'* (Article 12(4))

As explained above in Section 1, the EDPS welcomes the efforts made in the Proposal to ensure transparency and that individuals remain in control of their personal data, by requiring *'an explicit request of the user'* before any transfer of evidence between competent authorities (Article 12(4)).

To further improve the text, the EDPS recommends that the Proposal clarify (in substantive provisions and/or recitals, as appropriate):

- what makes the request *'explicit'* and how specific the request must be;
- whether the request can be submitted via the technical system referred to in Article 12(1):
- what are the consequences if the user chooses not to make an *'explicit request'*, and
- whether such request can be withdrawn.

These clarification may help ensuring that the technical system be built in such a way so as to give an appropriate level of control to individuals using the system, while at the same time also ensuring an efficient flow of information.

The EDPS, in particular, recommends that:

- a recital clarify that a request can only be considered *explicit* if it contains a freely given, specific, informed and unambiguous indication of the individual's wishes to have the relevant information exchanged, either by statement or affirmative action;
- the same recital also clarify that an explicit request for the exchange of evidence cannot simply be implied from a request to carry out a particular administrative procedure (e.g. to register a car); neither it is sufficient to make a general request, such as, for example, to request to obtain all necessary documents from all relevant authorities for purposes of the administrative procedure at hand;
- Article 12(2), which lists the requirements that the technical system must fulfil, include as an additional subparagraph that the system *'shall enable the processing of the explicit request of the user referred to in para 4 as well as the withdrawal of such request';*
- a substantive provision clarify that while the use of the technical system is recommended not just for the authorities exchanging evidence but also for users to interact with these authorities (in particular, to submit a request and to preview evidence), a user can also submit a request outside the technical system (i.e. the use of the technical system for making the request is not mandatory for the users: they may still make their request directly via other means outside the technical system);
- a substantive provision or a recital clarify that no exchange of evidence can take place via the technical system if the user has not made or has withdrawn her explicit request;
- a substantive provision clarify whether or not the user can also submit the evidence outside the technical system (i.e. whether the use of the technical system for submission of evidence is mandatory for the users);
- Article 12(4) clarify that the user may withdraw her request for the exchange of evidence at any time; a recital may then clarify that a user may choose to withdraw her request with or without stating a reason, but, typically, a withdrawal may happen, for example, if, after the *'preview'* of the evidence under Article 12(2)(e), she finds out that

the information is inaccurate, out-of-date or goes beyond what is necessary for the purposes of the procedure at hand (e.g. a document lists all previous registered addresses for the past five years instead of just the current address, which is the only one relevant for the purposes of the procedure at hand).

3.4. *'Preview'* (Article 12(2)(e))

As also explained above in Section 1, in addition to the requirement of an explicit consent, offering the possibility for the user to *'preview'* the evidence to be exchanged (Article 12(2)(e)) can also greatly contribute to transparency and user control. Importantly, it may also help ensure that any evidence exchanged is adequate, relevant, limited to what is necessary in relation to the purposes for which they are processed (*'data minimisation'*) as well as accurate and, where necessary, kept up to date (*'accuracy'*).

To further improve the text, the EDPS recommends that:

- the Proposal clarify what are the choices for the user who avails herself of the possibility to *'preview'* the data to be exchanged;
- in particular, Article 12(2)(e) should clarify that the user is offered a possibility of preview in a timely manner before the evidence is made accessible to the recipient; and can withdraw the request for the exchange of the evidence (see also our related recommendations on *'explicit requests'*);
- this can be done, for example, by inserting the words at the end of the sentence in Article 12(2)(e): *'before it is made accessible to the requesting authority, and may withdraw the request at any time'*).

In addition, to remind relevant organisations of their obligations under the GDPR with regard to transparency, the EDPS highlights that the organisations exchanging evidence via the technical system must also ensure that users are provided with clear information on how personal data relating to them will be processed. This is an obligation conferred on controllers under Articles 13 and 14 of the GDPR and Articles 11 and 12 of Regulation (EC) 45/2001. Therefore, the EDPS recommends including a reference to these requirements in a recital.

Finally, the EDPS emphasises that while the preview mechanism may help ensure compliance with data quality, it follows from the generally applicable data protection rules that the authorities should still put in place effective procedures that ensure that personal data is updated where necessary and that inaccurate or outdated data are no longer processed[53].

3.5. Definition of evidence; range of online procedures covered (Articles 3(4) and 2(2)(b))

Article 3(4) of the Proposal defines the term *'evidence'* as *'any document or data, including text or sound, visual or audio-visual recording, irrespective of the medium used, issued by a competent authority to prove facts or compliance with requirements for procedures referred to in Article 2(2)(b)'*.

The definition is broad and can potentially include a broad range of personal data. It also appears that the definition covers not only available documents, but also any extracts from those documents, or other information or data available to the requested competent authority in any format.

The range of personal data that can be potentially exchanged, however, is limited by reference to Article 2(2)(b) of the Proposal, which, in turn, refers to Article 2(2)(a) and Annex I. Annex I provides a broad list of areas, from travel, work and retirement within the Union, through healthcare, to running business, or public contracts. Importantly, the list in Annex I is not identical, and appears to be much broader and much more generic than the permitted scope of exchange of cross-border evidence under Article 12(1), which refers to the (much slimmer and specific) Annex II, as well as to four specifically listed directives.

The EDPS recommends that the two provisions be aligned in order to ensure consistency and legal certainty. In general, from the perspective of protection of personal data, the more clearly defined the scope of any information exchange, the more legal certainty there is and the less risk of exchanges of evidence occurring in violation of data protection law.

In principle, therefore, the EDPS would recommend:

- clarifying the relationship between Article 2(2)(b) and Article 3(4) on the one hand, and Article 12(1) on the other hand;
- the EDPS also emphasises that he welcomes the efforts made in the Proposal to limit the information exchange to the online procedures listed in Annex II and the four specifically listed directives;
- therefore, he recommends that the scope of the Proposal remain clearly defined and continue to include Annex II and the references to the four specifically listed directives.

3.6 Further recommendations: amendments to the IMI Regulation (Article 36)

Possible use of IMI for cooperation within the European Data Protection Board ('EDPB')

Article 36(1) of the Proposal ensures that IMI actors (as defined under the IMI Regulation) now include not only competent authorities of the Member States and the Commission but also Union bodies, offices and agencies. This change would potentially enable the EDPS and the European Data Protection Board (*'EDPB'*) to make use of the IMI system for information exchanges in the context of the GDPR.

Cross-border cooperation of national supervisory authorities for data protection with each other, the EDPS, the EDPB and the Commission is necessary to implement the GDPR in such a way that it can achieve both of its objectives: the protection of the fundamental rights and freedoms of individuals with regard to the processing or personal data on the hand and the free movement of such data within the Union on the other hand. The free movement of data within the Union is a precondition for the functioning of the Internal Market.

The GDPR strengthens the mechanisms to enable a harmonious application of data protection considerably and introduces new ways of cooperation between national authorities for this purpose. It provides that the authorities shall use electronic means for exchanging information. As the Internal Market Information System (*'IMI'*) is designed to enable efficient information exchange between IMI actors, it should be available to support cooperation in the field of data protection, where the authorities consider this appropriate.

Therefore, the EDPS:

- welcomes the inclusion of EU bodies in the definition of IMI actors in the Proposal;

- he recommends further to add the GDPR to the Annex of the IMI Regulation to allow the full use of the system for the purpose of data protection.

The EDPS also wants to clarify that the recommendation to include the GDPR in the Annex of the IMI Regulation is valid regardless of whether the legislator decides to include data protection in the scope of the Single Digital Gateway (*'SDG'*) or not. Even if the SDG were not available in this domain, the cooperation between national supervisory authorities for data protection, the EDPS, the EDPB and the Commission can benefit from access to IMI.

Coordinated supervision by the EDPS and national data protection supervisory authorities

As already highlighted in Section 1, the EDPS welcomes the proposed amendment of the IMI Regulation which confirms and updates the provisions on the coordinated supervision mechanism foreseen for IMI in order to ensure a consistent and coherent approach (Article 36(6)(b).

This amendment provides that the national (data protection) supervisory authorities, *'each acting within the scope of their respective competences, shall cooperate with each other to ensure coordinated supervision of IMI and its users by IMI actors in accordance with Article 62 of [Regulation (EU) No XX/201Y]'.*

This reference, in turn, is made to the proposed Regulation that will replace Regulation 45/2001 and which provides for a single coherent model for coordinated supervision[54].

The EDPS, as already stated in his Opinion 5/2017 on Upgrading data protection rules for EU institutions and bodies[55] welcomes the approach of a single coherent model of coordinated supervision for EU large scale information systems, as this will contribute to the comprehensiveness, effectiveness and coherence of data protection supervision and ensure a sound environment for further development in the years to come.

The EDPS further understands that the objective is to use this model both for the supervision of future systems and for existing ones. He notes that recital 65 of the 45/2001 Proposal[56] specifically mentions that *'[T]he Commission should therefore, where appropriate, submit legislative proposals with a view to amending Union legal acts providing for a model of coordinated supervision, in order to align them with the coordinated supervision model of this Regulation'*. The EDPS welcomes such a streamlining with regard to the IMI Regulation under Article 36(6)(b) of the current Proposal.

3.7 Data protection as an information area and data protection authorities as problem solvers (Article 2 and Annexes I and III)

Article 2(2)(a) of the Proposal stipulates that the single digital gateway shall provide information on rights, obligations and rules in areas listed in Annex I (e.g.travel within the Union, residence in another Member State, starting, running and closing a business). These areas are relevant for individuals and businesses wishing to exercise their rights derived from EU law in the field of the internal market.

Considering the importance of cross-border personal data flows for the functioning of the internal market, the EDPS recommends adding protection of personal data as an information area to Annex I.

Article 2(2)(c) of the Proposal provides that the single digital gateway shall inform and link to certain assistance and problem solving services. These services are listed in Annex III (e.g. Points of Single Contact, EURES, Online Dispute Resolution). As one of the tasks of data protection supervisory authorities is to inform data subjects about their rights under the GDPR and to handle complaints lodged by data subjects, the EDPS recommends adding data protection supervisory authorities to the list of assistance and problem solving services listed in Annex III.

4. CONCLUSIONS

The EDPS welcomes the Commission's proposal to modernise administrative services by facilitating the availability, quality and accessibility of information across the European Union and appreciates the Commission's and Parliament's consultation and concerns for the impact this Proposal may have on the protection of personal data.

In addition to providing specific recommendations to further improve the quality of legislation, he also wishes to seize this opportunity to provide an introductory overview of key issues related to the *'once-only'* principle in general, although many such concerns are not necessarily borne out by the Proposal in its present form. These relate, in particular to:

- the legal basis for the processing,
- purpose limitation
- and data subject rights.

The EDPS stresses that in order to ensure successful implementation of EU-wide *'once-only'*, and enable lawful cross-border exchange of data, once-only must be implemented in line with relevant data protection principles.

With regard to the Proposal itself, the EDPS supports:

- the efforts made to ensure that individuals remain in control of their personal data, including by requiring *'an explicit request of the user'* before any transfer of evidence between competent authorities (Article 12(4)), and by offering the possibility for the user to *'preview'* the evidence to be exchanged (Article 12(2)(e)); and
- the efforts made to define the material scope of application for the principle of *'once-only'* (Article 12(1));
- moreover, he welcomes the proposed amendment of the IMI Regulation which confirms and updates the provisions on coordinated supervision mechanism foreseen for IMI in order to ensure a consistent and coherent approach (Article 36(6)(b);
- he also welcomes the inclusion of EU bodies in the definition of IMI actors in the Proposal, which may help enable the European Data Protection Board (*'EDPB'*) to benefit from the technical possibilities offered by IMI for information exchange.

With regard to the legal basis of the processing, the EDPS recommends that one or more recitals be added to clarify that:

- the Proposal itself does not provide a legal basis for exchanging evidence, and that any exchange of evidence under Article 12(1) must have an appropriate legal basis elsewhere, such as in the four directives listed in Article 12(1) or under applicable EU or national law;

- the legal basis for the use of the technical system specified in Article 12 for the exchange of evidence is performance of a task in the public interest under Article 6(1)(e) of the GDPR; and that
- users have the right to object to the processing of their personal data in the technical system pursuant to Article 21(1) of the GDPR.

With regard to purpose limitation, the EDPS recommends that one or more recitals be added to clarify that:

- the Proposal does not provide a legal basis for using the technical system for exchanging information for purposes other than those provided for in the four directives listed or otherwise foreseen under applicable EU or national law;
- and that the Proposal does not in any way aim to provide a restriction on the principle of purpose limitation pursuant to Articles 6(4) and 23(1) of the GDPR.

On the notion of *'explicit request'*, the EDPS recommends that the Proposal clarify (preferably in a substantive provision):

- what makes the request *'explicit'* and how specific the request must be;
- whether the request can be submitted via the technical system referred to in Article 12(1);
- what are the consequences if the user chooses not to make an *'explicit request'*, and whether such request can be withdrawn. (For specific recommendations, see Section 3.3 above).

In relation to the issue of *'preview'*, the EDPS recommends that:

- the Proposal clarify what are the choices for the user who avails herself of the possibility to *'preview'* the data to be exchanged;
- in particular, Article 12(2)(e) should clarify that the user is offered a possibility of preview in a timely manner before the evidence is made accessible to the recipient; and can withdraw the request for the exchange of the evidence (see also our related recommendations on *'explicit requests'*);
- this can be done, for example, by inserting the words at the end of the sentence in Article 12(2)(e): *'before it is made accessible to the requesting authority, and may withdraw the request at any time'*).

With regard to the definition of evidence and the range of online procedures covered, the EDPS recommends:

- replacing the reference to Article 2(2)(b) in Article 3(4) by reference to Article 12(1) or providing another legislative solution that would result in a similar effect;
- the EDPS also emphasises that he welcomes the efforts made in the Proposal to limit the information exchange to the online procedures listed in Annex II and the four specifically listed directives;
- therefore, he recommends that the scope of the Proposal remain clearly defined and continue to include Annex II and the references to the four specifically listed directives.

Finally, the EDPS recommends:

- adding the GDPR to the Annex of the IMI Regulation to allow the potential use of IMI for the purposes of data protection; and
- adding data protection supervisory authorities to the list of assistance and problem solving services listed in Annex III.

Brussels, 1 August 2017

Giovanni BUTTARELLI

European Data Protection Supervisor

Notes

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 119, 4.5.2016, p. 1.
[3] OJ L 8, 12.1.2001, p. 1.
[4] Proposal for a Regulation of the European Parliament and of the Council on establishing a single digital gateway to provide information, procedures, assistance and problem solving services and amending Regulation (EU) No 1024/2012, COM(2017) 256 final, 2017/0086 (COD) (henceforth, the Proposal).
[5] Explanatory memorandum to the Proposal, p. 2.
[6] Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC (the 'IMI Regulation') (OJ L 316, 14.11.2012, p.1).
[7] See also EDPS Opinion of 22 November 2011 on the Commission Proposal for a Regulation of the European Parliament and of the Council on administrative cooperation through the Internal Market Information System ('*IMI*') available at https://edps.europa.eu/sites/edp/files/publication/11-11-22_imi_opinion_en.pdf .
[8] See also Article 14 of the Proposal for a Directive of the European Parliament and Council on the legal and operational framework of the European services e-card introduced by Regulation... [ESC Regulation], COM(2016) 823 final, 2016/0402(COD).
[9] Recital 28 of the Proposal.
[10] Article 12(1) and (4) of the Proposal.
[11] For example, in their first position paper, the partners of the Once-Only Principle Project (TOOP) recognise that Member States interpret the principle differently: some consider it to relate to data storage whereby national legislation requires authorities to store data in one database only, whereas others consider it to relate to collection of data, allowing data to be stored in several repositories. Krimmer et al, 'Position paper on definition of OOP and situation in Europe', p. 9, available at http://toop.eu/sites/default/files/D2.6_Position%20paper%20on%20definition%20of%20OOP%20and%20situation%20in%20Europe.pdf. See also Smart Study, cited above, p. 7. Note also the discussion about 'authoritative sources' and 'reference directories' (van Alsenoy et al, p. 256-257 and Annex IX of SMART Study p. 192 onwards).
[12] European Commission, 'EU eGovernment Action Plan 2016-2020' COM(2016) 179 final, p. 2.
[13] EU-wide digital Once-Only Principle for citizens and businesses' study prepared for the European Commission DG Networks, Content & Technology, SMART 2015/0062 ('Smart Study'), available at https://ec.europa.eu/digital-single-market/en/news/eu-wide-digital-once-only-principle-citizens-and-businesses-policy-options-and-their-impacts. See also Estonian Vision Paper on the Free Movement of Data - the Fifth Freedom of the European Union, p. 18-19, available at https://www.eu2017.ee/news/insights/FreeMovementOfData.
[14] Smart Study, cited above.
[15] EU eGovernment Action Plan 2016-2020', cited above, p. 3.
[16] Smart Study, cited above, p. 4.
[17] EU eGovernment Action Plan 2016-2020, cited above, p. 3.
[18] Smart Study, cited above, p. 45.
[19] See also Estonian Vision Paper on the Free Movement of Data - the Fifth Freedom of the European Union, p. 18, available at https://www.eu2017.ee/news/insights/FreeMovementOfData.
[20] Cited above.
[21] Article 6(1)(a) GDPR.
[22] Article 6(1)(c) GDPR.
[23] Article 6(1)(e) GDPR.
[24] See also Smart Study, cited above, p. 17, 19 and 46-48.
[25] WP29 Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, (WP 187), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.
[26] Article 4(11), 7, recitals 32, 42 and 43 of the GDPR.
[27] Recital 43 of the GDPR. See also WP 29 Opinion 15/2011.
[28] Article 6(1)(c).
[29] Opinion 6/2014 of the WP29 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, (WP 217), p. 19, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.
[30] Cited above.

[31] Cited above, p. 19.
[32] Cited above.
[33] Recital 45 of the GDPR.
[34] Cited above, p. 21.
[35] Article 21(1) GDPR.
[36] See also Opinion 3/2013 of the WP29 on purpose limitation, adopted on 2 April 2013, (WP 203), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
[37] See Article 6(4) of the GDPR. For completeness, see also Article 5(1)(b), which provides that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, carried out in accordance with Art 89(1) GDPR, are not considered to be incompatible with the initial purpose. This specific exception, while may be relevant in some cases of government data sharing, is not directly relevant for purposes of the principle of once-only, and therefore will not be further discussed in this Opinion.
[38] EDPS Opinion 7/2015: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf . See more specifically Section 3.
[39] EDPS Opinion 9/2016 of 20 October 2016 on Personal Information Management Systems, OJ 463/10, 13.12.2016, available at https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf
See, in particular, paras 36, 50 and 57.
[40] Transparency is a precondition for ensuring effective exercise of data protection rights and it is also important for creating trust. See, for example, Estonian Vision Paper on the Free Movement of Data - the Fifth Freedom of the European Union, p. 19, available at https://www.eu2017.ee/news/insights/FreeMovementOfData. See also C-201/14 *Smaranda Bara and Others v Casa Naţională de Asigurări de Sănătate and Others*, EU:C:2015:638.
[41] Article 5 GDPR.
[42] Article 25 GDPR.
[43] Article 5(2) GDPR.
[44] Smart Study, cited above, p. 211.
[45] Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications, (OJ L 255, 30.92005, p. 22-142).
[46] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (OJ L 376, 27.12.2006, p. 36-68).
[47] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65–242).
[48] Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC (OJ L 94, 28.3.2014, p. 243–374).
[49] Article 6(1)(c) GDPR.
[50] Article 6(1)(e) GDPR.
[51] See also p. 24-26 of the Smart Study.
[52] Article 5(1)(b) of the GDPR.
[53] See also Smart Study, cited above, p. 52.
[54] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.
[55] EDPS Opinion 5/2017 on Upgrading data protection rules for EU institutions and bodies (subtitle: EDPS Opinion on the proposal for a Regulation on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC), available at https://edps.europa.eu/sites/edp/files/publication/17-03-15_regulation_45-2001_en.pdf, paras 77 and 78.
[56] Cited above.