Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons 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 (Text with EEA relevance)

CHAPTER IX

PROCESSING OF OPERATIONAL PERSONAL DATA BY UNION BODIES, OFFICES AND AGENCIES WHEN CARRYING OUT ACTIVITIES WHICH FALL WITHIN THE SCOPE OF CHAPTER 4 OR CHAPTER 5 OF TITLE V OF PART THREE TFEU

Article 70

Scope of the Chapter

This Chapter applies only to the processing of operational personal data by Union bodies, offices and agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU, without prejudice to specific data protection rules applicable to such a Union body, office or agency.

Article 71

Principles relating to processing of operational personal data

1 Operational personal data shall be:

- a processed lawfully and fairly (‘lawfulness and fairness’);
- b collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes (‘purpose limitation’);
- c adequate, relevant, and not excessive in relation to the purposes for which they are processed (‘data minimisation’);
- d accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that operational personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);
- e kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the operational personal data are processed (‘storage limitation’);
- f processed in a manner that ensures appropriate security of the operational personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

2 Processing by the same or another controller for any of the purposes set out in the legal act establishing the Union body, office or agency other than that for which the operational personal data are collected shall be permitted in so far as:

- a the controller is authorised to process such operational personal data for such a purpose in accordance with Union law; and

b processing is necessary and proportionate to that other purpose in accordance with Union law.

3 Processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use, for the purposes set out in the legal act establishing the Union body, office or agency, subject to appropriate safeguards for the rights and freedoms of data subjects.

4 The controller shall be responsible for, and be able to demonstrate compliance with, paragraphs 1, 2 and 3.

Article 72

Lawfulness of processing of operational personal data

1 Processing of operational personal data shall be lawful only if and to the extent that processing is necessary for the performance of a task carried out by Union bodies, offices and agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU and that it is based on Union law.

2 Specific Union legal acts regulating processing within the scope of this Chapter shall specify at least the objectives of processing, the operational personal data to be processed, the purposes of the processing and the time limits for storage of the operational personal data or for periodic review of the need for further storage of the operational personal data.

Article 73

Distinction between different categories of data subjects

The controller shall, where applicable and as far as possible, make a clear distinction between the operational personal data of different categories of data subjects, such as the categories listed in the legal acts establishing Union bodies, offices and agencies.

Article 74

Distinction between operational personal data and verification of the quality of operational personal data

1 The controller shall distinguish, as far as possible, operational personal data based on facts from operational personal data based on personal assessments.

2 The controller shall take all reasonable steps to ensure that operational personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, the controller shall, as far as practicable and where relevant, verify the quality of operational personal data before they are transmitted or made available, for example by consulting the competent authority from which the data originates. As far as possible, in all transmissions of operational personal data, the controller shall add the necessary information enabling the recipient to assess the degree to which the operational personal data are accurate, complete and reliable, and the extent to which they are up to date.

3 If it emerges that incorrect operational personal data have been transmitted or that operational personal data have been unlawfully transmitted, the recipient shall be notified

without delay. In such a case, the operational personal data concerned shall be rectified or erased or their processing shall be restricted in accordance with Article 82.

Article 75

Specific processing conditions

1 When Union law applicable to the transmitting controller provides for specific conditions for processing, the controller shall inform the recipient of the operational personal data of those conditions and the requirement to comply with them.

2 The controller shall comply with specific processing conditions for processing provided by a transmitting competent authority in accordance with Article 9(3) and (4) of Directive (EU) 2016/680.

Article 76

Processing of special categories of operational personal data

1 Processing of operational personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, operational personal data concerning health or concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary for operational purposes, within the mandate of the Union body, office or agency concerned and subject to appropriate safeguards for the rights and freedoms of the data subject. Discrimination against natural persons on the basis of such personal data shall be prohibited.

2 The data protection officer shall be informed without undue delay of recourse to this Article.

Article 77

Automated individual decision-making, including profiling

1 A decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her shall be prohibited unless authorised by Union law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.

2 Decisions referred to in paragraph 1 of this Article shall not be based on the special categories of personal data referred to in Article 76 unless suitable measures to safeguard the data subject's rights, freedoms and legitimate interests are in place.

3 Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 76 shall be prohibited, in accordance with Union law.

Article 78

Communication and modalities for exercising the rights of the data subject

1 The controller shall take reasonable steps to provide any information referred to in Article 79 and make any communication with regard to Articles 80 to 84 and 92 relating to processing to the data subject in a concise, intelligible and easily accessible form, using clear and plain language. The information shall be provided by any appropriate means, including by electronic means. As a general rule, the controller shall provide the information in the same form as the request.

2 The controller shall facilitate the exercise of the rights of the data subject under Articles 79 to 84.

3 The controller shall inform the data subject in writing about the follow-up to his or her request without undue delay and in any case at the latest within three months after receipt of the request by the data subject.

4 The controller shall provide the information under Article 79 and any communication made or action taken pursuant to Articles 80 to 84 and 92 free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

5 Where the controller has reasonable doubts concerning the identity of the natural person making a request referred to in Article 80 or 82, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

Article 79

Information to be made available or given to the data subject

1 The controller shall make available to the data subject at least the following information:

a the identity and the contact details of the Union body, office or agency;

b the contact details of the data protection officer;

c the purposes of the processing for which the operational personal data are intended;

d the right to lodge a complaint with the European Data Protection Supervisor and his or her contact details;

e the existence of the right to request from the controller access to and rectification or erasure of operational personal data and restriction of processing of the operational personal data concerning the data subject.

2 In addition to the information referred to in paragraph 1, the controller shall give to the data subject, in the specific cases foreseen by Union law, the following further information to enable the exercise of his or her rights:

a the legal basis for the processing;

b the period for which the operational personal data will be stored, or, where that is not possible, the criteria used to determine that period;

c where applicable, the categories of recipients of the operational personal data, including in third countries or international organisations;

d where necessary, further information, in particular where the operational personal data are collected without the knowledge of the data subject.

3 The controller may delay, restrict or omit the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:

a avoid obstructing official or legal inquiries, investigations or procedures;

b avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

c protect the public security of Member States;

d protect the national security of Member States;

e protect the rights and freedoms of others, such as victims and witnesses.

Article 80

Right of access by the data subject

The data subject shall have the right to obtain from the controller confirmation as to whether or not operational personal data concerning him or her are processed, and where that is the case, have the right to access operational personal data and the following information:

(a) the purposes of and legal basis for the processing;

(b) the categories of operational personal data concerned;

(c) the recipients or categories of recipients to whom the operational personal data have been disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the operational personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of operational personal data or restriction of processing of operational personal data concerning the data subject;

(f) the right to lodge a complaint with the European Data Protection Supervisor and his or her contact details;

(g) communication of the operational personal data undergoing processing and of any available information as to their origin.

Article 81

Limitations to the right of access

1 The controller may restrict, wholly or partly, the data subject's right of access to the extent that, and for as long as, such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:

a avoid obstructing official or legal inquiries, investigations or procedures;

b avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

c protect the public security of Member States;

d protect the national security of Member States;

e protect the rights and freedoms of others, such as victims and witnesses.

2 In the cases referred to in paragraph 1, the controller shall inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may be omitted where the provision thereof would undermine a purpose under paragraph 1. The controller shall inform the data subject of the possibility of lodging a complaint with the European Data Protection Supervisor or of seeking a judicial remedy before the Court of Justice. The controller shall document the factual or legal reasons on which the decision is based. That information shall be made available to the European Data Protection Supervisor on request.

Article 82

Right to rectification or erasure of operational personal data and restriction of processing

1 Any data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate operational personal data relating to him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete operational personal data completed, including by means of providing a supplementary statement.

2 The controller shall erase operational personal data without undue delay and the data subject shall have the right to obtain from the controller the erasure of operational personal data concerning him or her without undue delay where processing infringes Articles 71, 72(1) or 76, or where operational personal data must be erased in order to comply with a legal obligation to which the controller is subject.

3 Instead of erasure, the controller shall restrict processing where:

a the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or

b the personal data must be maintained for the purposes of evidence.

Where processing is restricted pursuant to point (a) of the first subparagraph, the controller shall inform the data subject before lifting the restriction of processing.

Restricted data shall be processed only for the purpose that prevented their erasure.

4 The controller shall inform the data subject in writing of any refusal of rectification or erasure of operational personal data or restrict processing and of the reasons for the refusal. The controller may restrict, wholly or partly, the provision of such information to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned in order to:

a avoid obstructing official or legal inquiries, investigations or procedures;

b avoid prejudicing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

c protect the public security of Member States;

d protect the national security of Member States;

e protect the rights and freedoms of others, such as victims and witnesses.

The controller shall inform the data subject of the possibility of lodging a complaint with the European Data Protection Supervisor or seeking a judicial remedy from the Court of Justice.

5 The controller shall communicate the rectification of inaccurate operational personal data to the competent authority from which the inaccurate operational personal data originate.

6 The controller shall, where operational personal data has been rectified or erased or processing has been restricted pursuant to paragraphs 1, 2 or 3, notify the recipients and inform them that they have to rectify or erase the operational personal data or restrict processing of the operational personal data under their responsibility.

Article 83

Right of access in criminal investigations and proceedings

Where operational personal data originates from a competent authority, Union bodies, offices and agencies shall, prior to deciding on a data subject's right of access, verify with the competent authority concerned whether such personal data are contained in a judicial decision or record or a case file processed in the course of criminal investigations and proceedings in the Member State of that competent authority. Where this is the case, a decision on the right of access shall be taken in consultation and in close cooperation with the competent authority concerned.

Article 84

Exercise of rights by the data subject and verification by the European Data Protection Supervisor

1 In the cases referred to in Articles 79(3), 81 and 82(4), the rights of the data subject may also be exercised through the European Data Protection Supervisor.

2 The controller shall inform the data subject of the possibility of exercising his or her rights through the European Data Protection Supervisor pursuant to paragraph 1.

3 Where the right referred to in paragraph 1 is exercised, the European Data Protection Supervisor shall at least inform the data subject that all necessary verifications or a review by him or her have taken place. The European Data Protection Supervisor shall also inform the data subject of his or her right to seek a judicial remedy before the Court of Justice.

Article 85

Data protection by design and by default

1 Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing, in order to meet

the requirements of this Regulation and the legal act establishing it, and protect the rights of the data subjects.

2 The controller shall implement appropriate technical and organisational measures ensuring that, by default, only operational personal data which are adequate, relevant and not excessive in relation to the purpose of the processing are processed. That obligation applies to the amount of operational personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default operational personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Article 86

Joint controllers

1 Where two or more controllers or one or more controllers together with one or more controllers other than Union institutions and bodies jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with their data protection obligations, in particular as regards the exercise of the rights of the data subject and their respective duties to provide the information referred to in Article 79, by means of an arrangement between them, unless and in so far as the respective responsibilities of the joint controllers are determined by Union or Member State law to which the joint controllers are subject. The arrangement may designate a contact point for data subjects.

2 The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subject. The essence of the arrangement shall be made available to the data subject.

3 Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Article 87

Processor

1 Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and the legal act establishing the controller and ensure the protection of the rights of the data subject.

2 The processor shall not engage another processor without prior specific or general written authorisation by the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3 Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of operational personal data and categories of data subjects and

the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

a acts only on instructions from the controller;

b ensures that persons authorised to process the operational personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c assists the controller by any appropriate means to ensure compliance with the provisions on the data subject's rights;

d at the choice of the controller, deletes or returns all the operational personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union law or Member State law requires storage of the operational personal data;

e makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article;

f complies with the conditions referred to in paragraph 2 and in this paragraph for engaging another processor.

4 The contract or the other legal act referred to in paragraph 3 shall be in writing, including in electronic form.

5 If a processor infringes this Regulation or the legal act establishing the controller by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 88

Logging

1 The controller shall keep logs for any of the following processing operations in automated processing systems: the collection, alteration, access, consultation, disclosure, including transfers, combination and erasure of operational personal data. The logs of consultation and disclosure shall make it possible to establish the justification for, and the date and time of, such operations, the identification of the person who consulted or disclosed operational personal data, and, as far as possible, the identity of the recipients of such operational personal data.

2 The logs shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the operational personal data, and for criminal proceedings. Such logs shall be deleted after three years, unless they are required for ongoing control.

3 The controller shall make the logs available to its data protection officer and to the European Data Protection Supervisor on request.

Article 89

Data protection impact assessment

1 Where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out, prior to the

processing, an assessment of the impact of the envisaged processing operations on the protection of operational personal data.

2 The assessment referred to in paragraph 1 shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of operational personal data and to demonstrate compliance with data protection rules, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

Article 90

Prior consultation of the European Data Protection Supervisor

1 The controller shall consult the European Data Protection Supervisor prior to processing which will form part of a new filing system to be created, where:

a a data protection impact assessment under Article 89 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or

b the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.

2 The European Data Protection Supervisor may establish a list of the processing operations which are subject to prior consultation pursuant to paragraph 1.

3 The controller shall provide the European Data Protection Supervisor with the data protection impact assessment referred to Article 89 and, on request, with any other information to allow the European Data Protection Supervisor to make an assessment of the compliance of the processing and in particular of the risks for the protection of operational personal data of the data subject and of the related safeguards.

4 Where the European Data Protection Supervisor is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation or the legal act establishing the Union body, office or agency, in particular where the controller has insufficiently identified or mitigated the risk, the European Data Protection Supervisor shall provide written advice to the controller within a period of up to six weeks of receipt of the request for consultation. That period may be extended by a month, taking into account the complexity of the intended processing. The European Data Protection Supervisor shall inform the controller of any such extension within one month of receipt of the request for consultation, together with the reasons for the delay.

Article 91

Security of processing of operational personal data

1 The controller and the processor shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks, in particular as regards the processing of special categories of operational personal data.

2 In respect of automated processing, the controller and the processor shall, following an evaluation of the risks, implement measures designed to:

a deny unauthorised persons access to data processing equipment used for processing (‘equipment access control’);

b prevent the unauthorised reading, copying, modification or removal of data media (‘data media control’);

c prevent the unauthorised input of operational personal data and the unauthorised inspection, modification or deletion of stored operational personal data (‘storage control’);

d prevent the use of automated processing systems by unauthorised persons using data communication equipment (‘user control’);

e ensure that persons authorised to use an automated processing system have access only to the operational personal data covered by their access authorisation (‘data access control’);

f ensure that it is possible to verify and establish the bodies to which operational personal data have been or may be transmitted or made available using data communication (‘communication control’);

g ensure that it is subsequently possible to verify and establish which operational personal data have been input into automated data processing systems, and when and by whom the operational personal data were input (‘input control’);

h prevent unauthorised reading, copying, modification or deletion of operational personal data during transfers of operational personal data or during transportation of data media (‘transport control’);

i ensure that installed systems may, in the case of interruption, be restored (‘recovery’);

j ensure that the functions of the system perform, that the appearance of faults in the functions is reported (‘reliability’) and that stored operational personal data cannot be corrupted by means of a malfunctioning of the system (‘integrity’).

Article 92

Notification of a personal data breach to the European Data Protection Supervisor

1 In the case of a personal data breach, the controller shall notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the European Data Protection Supervisor, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the European Data Protection Supervisor is not made within 72 hours, it shall be accompanied by reasons for the delay.

2 The notification referred to in paragraph 1 shall at least:

a describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of operational personal data records concerned;

b communicate the name and contact details of the Data Protection Officer;

c describe the likely consequences of the personal data breach;

d describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

3 Where, and in so far as, it is not possible to provide the information referred to in paragraph 2 at the same time, the information may be provided in phases without undue further delay.

4 The controller shall document any personal data breaches referred to in paragraph 1, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the European Data Protection Supervisor to verify compliance with this Article.

5 Where the personal data breach involves operational personal data that have been transmitted by or to the competent authorities, the controller shall communicate the information referred to in paragraph 2 to the competent authorities concerned without undue delay.

Article 93

Communication of a personal data breach to the data subject

1 Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2 The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and shall contain at least the information and the recommendations provided for in points (b), (c) and (d) of Article 92(2).

3 The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

a the controller has implemented appropriate technological and organisational protection measures, and those measures were applied to the operational personal data affected by the personal data breach, in particular those that render the operational personal data unintelligible to any person who is not authorised to access it, such as encryption;

b the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

c it would involve a disproportionate effort. In such a case, there shall instead be a public communication or a similar measure whereby the data subjects are informed in an equally effective manner.

4 If the controller has not already communicated the personal data breach to the data subject, the European Data Protection Supervisor, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so, or may decide that any of the conditions referred to in paragraph 3 are met.

5 The communication to the data subject referred to in paragraph 1 of this Article may be delayed, restricted or omitted subject to the conditions and on the grounds referred to in Article 79(3).

Article 94

Transfer of operational personal data to third countries and international organisations

1 Subject to restrictions and conditions laid down in the legal acts establishing the Union body, office or agency, the controller may transfer operational personal data to an authority of a third country or to an international organisation insofar as such transfer is necessary for the performance of controller's tasks and only where the conditions laid down in this Article are met, namely:

a the Commission has adopted an adequacy decision in accordance with Article 36(3) of Directive (EU) 2016/680, finding that the third country or a territory or a processing sector within that third country or the international organisation in question ensures an adequate level of protection;

b in the absence of a Commission adequacy decision under point (a), an international agreement has been concluded between the Union and that third country or international organisation pursuant to Article 218 TFEU adducing adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals;

c in the absence of a Commission adequacy decision under point (a) or an international agreement under point (b), a cooperation agreement has been concluded allowing for the exchange of operational personal data before the date of application of the legal act establishing the Union body, office or agency concerned, between that Union body, office or agency and the third country in question.

2 The legal acts establishing the Union bodies, offices and agencies may maintain or introduce more specific provisions on the conditions for international transfers of operational personal data, in particular on the transfers by way of appropriate safeguards and derogations for specific situations..

3 The controller shall publish on its website and keep up to date a list of adequacy decisions referred to in point (a) of paragraph 1, agreements, administrative arrangements and other instruments relating to the transfer of operational personal data in accordance with paragraph 1.

4 The controller shall keep detailed records of all transfers made pursuant to this Article.

Article 95

Secrecy of judicial inquiries and criminal proceedings

The legal acts establishing the Union bodies, offices or agencies carrying out the activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU may oblige the European Data Protection Supervisor, in the exercise of his or her supervision powers, to take utmost account of the secrecy of judicial inquiries and criminal proceedings, in accordance with Union or Member State law.

Status:
Point in time view as at 23/10/2018.

Changes to legislation:
There are currently no known outstanding effects for the Regulation (EU) 2018/1725 of the European Parliament and of the Council, CHAPTER IX.