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)

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)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[(1)],

Acting in accordance with the ordinary legislative procedure[(2)],

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her. This right is also guaranteed under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(2) Regulation (EC) No 45/2001 of the European Parliament and of the Council[(3)] provides natural persons with legally enforceable rights, specifies the data processing obligations of controllers within the Community institutions and bodies, and creates an independent supervisory authority, the European Data Protection Supervisor, responsible for monitoring the processing of personal data by the Union institutions and bodies. However, it does not apply to the processing of personal data in the course of an activity of Union institutions and bodies which fall outside the scope of Union law.

(3) Regulation (EU) 2016/679 of the European Parliament and of the Council[(4)] and Directive (EU) 2016/680 of the European Parliament and of the Council[(5)] were adopted on 27 April 2016. While the Regulation lays down general rules to protect natural

Changes to legislation: *Regulation (EU) 2018/1725 of the European Parliament and of the Council is up to date with all changes known to be in force on or before 24 December 2020. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

persons with regard to the processing of personal data and to ensure the free movement of personal data within the Union, the Directive lays down the specific rules to protect natural persons with regard to the processing of personal data and to ensure the free movement of personal data within the Union in the fields of judicial cooperation in criminal matters and police cooperation.

(4) Regulation (EU) 2016/679 provides for the adaptation of Regulation (EC) No 45/2001 in order to ensure a strong and coherent data protection framework in the Union and to allow its application in parallel with Regulation (EU) 2016/679.

(5) It is in the interest of a coherent approach to personal data protection throughout the Union, and of the free movement of personal data within the Union, to align as far as possible the data protection rules for Union institutions, bodies, offices and agencies with the data protection rules adopted for the public sector in the Member States. Whenever the provisions of this Regulation follow the same principles as the provisions of Regulation (EU) 2016/679, those two sets of provisions should, under the case law of the Court of Justice of the European Union (the 'Court of Justice'), be interpreted homogeneously, in particular because the scheme of this Regulation should be understood as equivalent to the scheme of Regulation (EU) 2016/679.

(6) Persons whose personal data are processed by Union institutions and bodies in any context whatsoever, for example, because they are employed by those institutions and bodies, should be protected. This Regulation should not apply to the processing of personal data of deceased persons. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

(7) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used.

(8) This Regulation should apply to the processing of personal data by all Union institutions, bodies, offices and agencies. It should apply to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

(9) In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and on the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU could prove necessary because of the specific nature of those fields. A distinct Chapter of this Regulation containing general rules should therefore apply to the processing of operational personal data, such as personal data processed for the purposes of a criminal investigation by Union bodies, offices or agencies when carrying out activities in the fields of judicial cooperation in criminal matters and police cooperation.

***Changes to legislation:** Regulation (EU) 2018/1725 of the European Parliament and of the Council is up to date with all changes known to be in force on or before 24 December 2020. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

(10) Directive (EU) 2016/680 sets out harmonised rules for the protection and the free movement of personal data processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. In order to ensure the same level of protection for natural persons through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU and competent authorities, the rules for the protection and the free movement of operational personal data processed by such Union bodies, offices or agencies should be consistent with Directive (EU) 2016/680.

(11) The general rules of the Chapter of this Regulation on the processing of operational personal data should apply without prejudice to the specific rules applicable to the processing of operational personal data by Union bodies, offices and agencies when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU. Such specific rules should be regarded as *lex specialis* to the provisions in the Chapter of this Regulation on the processing of operational personal data (*lex specialis derogat legi generali*). In order to reduce legal fragmentation, specific data protection rules applicable to the processing of operational personal data by Union bodies, offices or agencies when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU should be consistent with the principles underpinning the Chapter of this Regulation on the processing of operational personal data, as well as with the provisions of this Regulation relating to independent supervision, remedies, liability and penalties.

(12) The Chapter of this Regulation on the processing of operational personal data should apply to 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, whether they exercise such activities as their main or ancillary tasks, for the purposes of the prevention, detection, investigation or prosecution of criminal offences. However, it should not apply to Europol or to the European Public Prosecutor's Office until the legal acts establishing Europol and the European Public Prosecutor's Office are amended with a view to rendering the Chapter of this Regulation on the processing of operational personal data, as adapted, applicable to them.

(13) The Commission should conduct a review of this Regulation, in particular the Chapter of this Regulation on the processing of operational personal data. The Commission should also conduct a review of other legal acts adopted on the basis of the Treaties which regulate the processing of operational personal data by Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU. After such a review, in order to ensure uniform and consistent protection of natural persons with regard to the processing of personal data, the Commission should be able to make any appropriate legislative proposals, including any necessary adaptations of the Chapter of this Regulation on the processing of operational personal data, with a view to applying it to Europol and to the European

Changes to legislation: *Regulation (EU) 2018/1725 of the European Parliament and of the Council is up to date with all changes known to be in force on or before 24 December 2020. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

Public Prosecutor's Office. The adaptations should take into account provisions relating to independent supervision, remedies, liability and penalties.

(14) The processing of administrative personal data, such as staff data, by Union bodies, offices or agencies carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU should be covered by this Regulation.

(15) This Regulation should apply to the processing of personal data by Union institutions, bodies, offices or agencies carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU). This Regulation should not apply to the processing of personal data by missions referred to in Articles 42(1), 43 and 44 TEU, which implement the common security and defence policy. Where appropriate, relevant proposals should be put forward to further regulate the processing of personal data in the field of the common security and defence policy.

(16) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person, to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

(17) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

(18) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

(19) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or

***Changes to legislation:** Regulation (EU) 2018/1725 of the European Parliament and of the Council is up to date with all changes known to be in force on or before 24 December 2020. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided. At the same time, the data subject should have the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal. In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have an opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

(20) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing and for preventing its unauthorised disclosure when it is transmitted.