6 September 2017

TF50 (2017) 14 – Commission to EU 27

Subject: Position paper transmitted to EU27 on the **Use of Data and Protection of Information Obtained or Processed before the Withdrawal Date**

Origin: European Commission, Task Force for the Preparation and Conduct of the Negotiations with the United Kingdom under Article 50 TEU

Objective: For discussion at the Council Working party (Art. 50) of 7 September 2017

Remarks: The attached position paper on the **Use of Data and Protection of Information Obtained or Processed before the Withdrawal Date** contains the main principles of the EU position in this regard, to be presented to the UK in the context of negotiations under Art. 50

Essential Principles on the Use of Data and Protection of Information Obtained or Processed before the Withdrawal Date

It is recalled that the United Kingdom's access to networks, information systems and databases established by Union law is, as a general rule, terminated on the date of withdrawal.

The United Kingdom or entities in the United Kingdom may keep and continue to use data or information received/processed[1] in the United Kingdom before the withdrawal date and referred to below only if the conditions set out in this paper are fulfilled. Otherwise such data or information (including any copies thereof) should be erased or destroyed.

The principles set out in this paper should also apply, *mutatis mutandis*, to personal data, data or information which was received /processed by the United Kingdom or entities in the United Kingdom after the withdrawal date pursuant to the Withdrawal Agreement.

I. Protection of personal data processed before the withdrawal date

The following general principles should apply in accordance with Union law, as interpreted by the Court of Justice of the European Union on the date of entry into force of the Withdrawal Agreement:

(1) The provisions of Union law on personal data protection applicable on the withdrawal date should continue to apply to personal data in the United Kingdom processed before the withdrawal date and pertaining to

(i) data subjects in the EU27,

(ii) data subjects outside the Union,

to the extent that this data is covered by Union law on personal data protection before the withdrawal date.

The data subjects concerned should, for example, continue to have the right to be informed, the right of access, the right to rectification, to erasure, to restriction of processing, to data portability as well as the right to object to processing and not to be subject to a decision based solely on automated processing, on the basis of relevant provisions of Union law applicable on the withdrawal date. Personal data referred to above should be stored no longer than is necessary for the purposes for which the personal data was processed; it should be erased afterwards. Where sectorial rules applicable on the withdrawal date provide for specific maximum mandatory storage periods, the data should be automatically erased upon the expiry of that period. The personal data in question could only be transferred to non-EU27 countries and to international organizations if the transfer is carried out in accordance with the conditions set forth in Chapter V of Regulation (EU) 2016/679.

The data subjects concerned should also be able to enforce their rights in accordance with the relevant provisions of Union law applicable on the withdrawal date, in particular Chapter

[1] Article 4(2) of Regulation (EU) 2016/679 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) defines processing as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

VIII of Regulation (EU) 2016/679, for as long as the personal data in question continues to be processed in the United Kingdom after the withdrawal date.

(2) Personal data of data subjects in the United Kingdom processed before the withdrawal date by the Union institutions, agencies, offices and bodies or in the EU27 will continue to be protected in accordance with the Union law applicable on the withdrawal date.

(3) The Withdrawal Agreement should allow for the orderly completion of investigations or procedures for the monitoring of compliance with personal data protection provisions between the United Kingdom authorities and EU27 authorities or Union institutions, agencies, offices and bodies (such as the European Data Protection Board) which are ongoing on the withdrawal date, in particular those provided for in Chapter VII of Regulation (EU) 2016/679.

II. Protection of EUCI[2] and national classified information[3] exchanged in the interests of the EU before the withdrawal date

The following general principles should apply in accordance with Union law, as interpreted by the Court of Justice of the European Union on the withdrawal date:

(1) EUCI and national classified information received from EU27 Member States or Union institutions, agencies, offices and bodies before the withdrawal date by the United Kingdom on the basis of Union law, should continue to be protected in accordance with the provisions of Union law applicable on the withdrawal date, in particular Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information, Commission Decision 2015/444 of 13 March 2015 on the security rules for protecting EU classified information, as well as the Agreement of 4 May 2011 between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union. The same applies to information received from the United Kingdom before the withdrawal date by EU27 Member States or Union institutions, agencies, offices and bodies.

(2) The United Kingdom should continue to ensure that contractors and subcontractors as well as grant beneficiaries registered in its territory take all appropriate measures to protect EUCI and national classified information when performing a classified contract[4] or classified grant agreement[5] concluded with a Union contracting authority or Union granting authority before the withdrawal date.

---

[2] According to Article 2 of Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information: "'*EU classified information' (EUCI) means any information or material designated by a EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States*".

[3] According to Article 2 of the Agreement of 4 May 2011 between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union, "'*classified information' shall mean any information or material, in any form, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States, and which bears one of the […] EU classification markings or a corresponding classification marking as set out in the Annex".*

[4] A contract the performance of which requires or involves the creation, handling or storing of EUCI (see Commission Decision 2015/444 of 13 March 2015, Article 40(a))

[5] An agreement whereby the granting authority awards a grant the performance of which requires or involves the creation, handling or storing of EUCI (see Commission Decision 2015/444 of 13 March 2015, Article 40(c)).

(3) The United Kingdom should continue to ensure, in accordance with national laws and regulations, that contractors or subcontractors as well as grant-beneficiaries registered in its territory participating in classified contracts or classified grant agreements concluded with a Union contracting authority or Union granting authority before the withdrawal date which require access to EUCI or national classified information within their facilities in the performance of such contracts or agreements hold a Facility Security Clearance at the relevant classification level.[6]

(4) The Withdrawal Agreement should allow for the orderly completion of procedures between the United Kingdom authorities and EU27 authorities or Union institutions, agencies, offices and bodies which are ongoing on the withdrawal date, as regards the protection of EUCI or national classified information, in particular security investigations. It should also allow for the possibility to start and conduct, after the withdrawal date, cooperation procedures relating to the protection of information exchanged before the withdrawal date.

(5) The UK shall notify the EU of any incident or change in policy regarding the approval of cryptographic products used for the protection of EUCI.

III. Other restrictions of use and access to data and information obtained before the withdrawal date

The following general principle should apply in accordance with Union law, as interpreted by the Court of Justice of the European Union on the withdrawal date:

Data and information received by the United Kingdom from EU27 Member States, Union institutions, agencies, offices and bodies, or private entities established in the EU27, before the withdrawal date, which are subject to Union rules restricting the use or access to such data and information (e.g. access or purpose restrictions, limitations of storage periods) other than those referred to in sections I and II on the withdrawal date, should continue to be protected in accordance with the provisions in Union law restricting the use or access to such data and information applicable on the withdrawal date. The same principle should apply to data and information received by EU27 Member States or Union institutions, agencies, offices and bodies from the United Kingdom or entities established therein, before the withdrawal date.

Examples of such Union rules restricting the use or access to data and information other than those referred to in sections I and II include:

- Rules concerning the protection of information of the kind covered by the obligation of professional secrecy obtained in the context of Union merger, antitrust or State aid procedures;
- Rules concerning regulatory data protection of pre-clinical, clinical, and toxicological (human health and environment) studies as well as other data submitted in accordance with applicable Union law;
- Rules concerning the protection of information acquired by customs authorities.

[6] It is recalled that the withdrawal of a Facility Security Clearance by the United Kingdom would constitute sufficient grounds for the contracting or granting authority, to terminate a classified contract or grant agreement concerned.