COMMISSION DECISION (EU) 2021/2243

of 15 December 2021

laying down internal rules concerning the provision of information to data subjects and the restriction of certain of their rights in the context of the processing of personal data for the purposes of the security of information and communication systems of the Commission

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 249(1) thereof,

Whereas:

(1) While carrying out its tasks, the Commission is bound to respect the rights of natural persons in relation to the processing of personal data recognised by Article 8(1) of the Charter of Fundamental Rights of the European and by Article 16(1) of the Treaty on the Functioning of the European Union. It also has to respect the rights provided for in Regulation (EU) 2018/1725 of the European Parliament and of the Council ([1]). At the same time, the Commission must handle IT security incidents in accordance with the rules laid down in Article 15 of Decision (EU, Euratom) 2017/46 ([2]).

(2) In order to ensure IT security, meaning the preservation of confidentiality, integrity and availability of communication and information systems and the data sets that they process, as regards people, assets and information, the Commission, notably through its Directorate-General for Informatics, has taken measures as provided for in Decision (EU, Euratom) 2017/46 and in Decision C(2017) 8841 final ([3]). Those measures include monitoring the IT security risks and the IT security measures implemented, requesting system owners to take specific IT security measures in order to mitigate IT security risks to the Commission's communication and information systems, and managing IT security incidents.

(3) The Directorate-General for Informatics provides IT security operations and services to the Commission and needs to process several categories of personal data in order to:

— communicate alerts and warnings relating to IT security events and incidents;

— respond to and contain IT security events and incidents;

— facilitate tools and operations through security audits, security assessments and vulnerability management;

— increase the awareness of Commission staff in the field of cybersecurity;

— monitor, detect and prevent the occurrence of IT security events and incidents;

— review privileged user accounts.

(4) IT security incidents that could undermine the security of the Commission's information and communication systems can occur in any processing operation carried out by the Commission. They can involve any category of personal data processed by the Commission.

([1]) 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 EU 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 (OJ L 295, 21.11.2018, p. 39).

([2]) Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission (OJ L 6, 11.1.2017, p. 40).

([3]) Commission Decision (C(2017) 8841) of 13 December 2017 laying down implementing rules for Articles 3, 5, 7, 8, 9, 10, 11, 12, 14, 15 of Commission Decision (EU, Euratom) 2017/46 on the security of communications and information systems in the Commission.

(5) In certain circumstances, it may prove necessary to reconcile the rights of data subjects under Regulation (EU) 2018/1725 with the Commission's need to effectively carry out its tasks of ensuring the IT security of persons, assets and information in the Commission under Decision (EU, Euratom) 2017/46, and in full respect for the fundamental rights and freedoms of other data subjects. To that effect, Article 25(1) of Regulation (EU) 2018/1725 authorises the Commission to restrict the application of Articles 14 to 17, 19, 20 and 35 of that Regulation, and the principle of transparency laid down in Article 4(1)(a), thereof, insofar as its provisions correspond to the rights and obligations provided for in Articles 14 to 17, 19 and 20 of that Regulation.

(6) This Decision should apply to all processing operations carried out by the Commission as data controller in the performance of its tasks to ensure IT security of persons, assets and information in the Commission pursuant to Decision (EU, Euratom) 2017/46. Therefore, it should concern the data subjects of the categories of personal data covered by all those processing operations, i.e. individuals who interact with any of the Commission information and communication systems.

(7) Personal data are stored in a secured electronic environment to prevent unlawful access by persons outside the Commission. Different data retention periods apply to different processing operations, depending on the type of personal data involved. The retention of files in the Commission is regulated by the Common Commission-Level Retention List (SEC(2019) 900), a regulatory document in the form of a retention schedule that sets out the retention periods for different types of Commission files to limit data retention to what is necessary.

(8) The Commission could have to restrict the application of the rights of data subjects in order to safeguard its internal security pursuant to Article 25(1)(d), of Regulation (EU) 2018/1725 (i.e. to preserve confidentiality, integrity and availability of its communication and information systems and the data sets that they process, its assets and information). In particular, the Commission could have to do so when:

— communicating alerts and warnings relating to IT security events and incidents;

— responding to and containing IT security events and incidents; facilitating tools and operations through security audits, security assessments and vulnerability management;

— increasing the awareness of Commission staff in the field of cybersecurity;

— monitoring, detecting and preventing the occurrence of IT security events and incidents;

— reviewing privileged user accounts.

(9) For the purpose of handling IT security incidents, as referred to in Article 15 of Decision (EU, Euratom) 2017/46, the Directorate-General for Informatics may exchange information with the Cyber Attack Response Team of the Directorate-General responsible for Human Resources and Security.

(10) To comply with Articles 14, 15 and 16 of Regulation (EU) 2018/1725, the Commission should inform all individuals of the activities that involve processing their personal data and that affect their rights. It should do so in a transparent and coherent manner by publishing a data protection notice on the Commission's website. Where relevant, it should apply additional safeguards to inform data subjects individually in an appropriate format.

(11) Complying with Articles 14, 15 and 16 of Regulation (EU) 2018/1725, could reveal the existence of IT security measures, vulnerabilities or incidents taken under Article 15 of Decision (EU, Euratom) 2017/46. Revealing those IT security measures, vulnerabilities and incidents increases the risk that the exposed IT security measure would then be circumvented, that the exposed vulnerability would then be abused, and that an ongoing IT security incident analysis could be undermined because artefacts might be manipulated accidentally or intentionally by a user or malicious actor. This could seriously impair the Commission's capability to ensure its IT security and in particular to handle IT security incidents effectively in the future.

(12) Under Article 25(1)(h), of Regulation (EU) 2018/1725, the Commission is also authorised to restrict the application of data subjects' rights in order to protect the rights and freedoms of other individuals related to IT security incidents that could undermine IT security operations.

(13) The Commission may need to restrict the provision of information to data subjects and the application of other rights of data subjects in relation to personal data received from non-EU countries or international organisations, in order to fulfil its duty of cooperation with those countries or organisations. This is part of the Commission's duty to safeguard an important objective of EU general public interest, as referred to in Article 25(1)(c) of Regulation (EU) 2018/1725. However, in some circumstances the interest of the data subject's fundamental rights may override the interest of international cooperation.

(14) The Commission has therefore identified the grounds listed in Article 25(1)(c), (d) and (h) of Regulation (EU) 2018/1725 as grounds for restrictions that may be necessary to apply to data processing operations carried out by the Directorate-General for Informatics related to providing IT security operations and services to the Commission.

(15) Any restriction, applied under this Decision should be necessary and proportionate taking into account the risks to the rights and freedoms of data subjects.

(16) The Commission should handle all restrictions in a transparent manner and register each application of restrictions in the corresponding record system.

(17) Under Article 25(8) of Regulation (EU) 2018/1725, data controllers may defer, omit or deny the provision of information based on the reasons for the application of a restriction to the data subject if providing that information would in any way undermine the effect of the restriction. In particular, this applies to the restrictions of the obligations provided for in Articles 16 and 35 of Regulation (EU) 2018/1725. The Commission should regularly review the restrictions imposed in order to ensure that the data subject's rights to be informed in accordance with Articles 16 and 35 of Regulation (EU) 2018/1725 are restricted only as long as such restrictions are necessary to enable the Commission to ensure its IT security and in particular to handle IT security incidents.

(18) Where the Commission restricts the application of the rights of data subjects other than those referred to in Articles 16 and 35 of Regulation (EU) 2018/1725, the data controller should assess on a case-by-case basis whether the communication of the restriction would undermine its purpose.

(19) The Commission's Data Protection Officer should carry out an independent review of the application of restrictions, with a view to ensuring compliance with this Decision.

(20) In order to allow the Commission to immediately restrict the application of certain rights and obligations in accordance with Article 25 of Regulation (EU) 2018/1725, this Decision should enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

(21) The European Data Protection Supervisor issued an opinion on 16 September 2021,

HAS ADOPTED THIS DECISION:

Article 1

Subject-matter and scope

1. This Decision lays down the rules that the Commission must follow to inform data subjects of the processing of their personal data in accordance with Articles 14, 15 and 16 of Regulation (EU) 2018/1725 when carrying out its tasks pursuant to Decision (EU, Euratom) 2017/46.

It also lays down the conditions under which the Commission may restrict the application of Articles 4, 14 to 17, 19, 20 and 35 of Regulation (EU) 2018/1725, in accordance with Article 25(1)(c), (d) and (h), of that Regulation, when carrying out its tasks pursuant to Decision (EU, Euratom) 2017/46.

2. This Decision applies to the processing of personal data either by or on behalf of the Commission for the purpose of, or in relation to activities carried out to ensure the IT security of persons, assets and information in the Commission pursuant to Decision (EU, Euratom) 2017/46.

Article 2

Applicable exceptions and restrictions

1. Where the Commission exercises its duties with respect to data subjects' rights under Regulation (EU) 2018/1725, it shall consider whether any of the exceptions laid down in that Regulation apply.

2. Subject to Articles 3 to 7 of this Decision, where the exercise of the rights and obligations provided for in Articles 14 to 17, 19, 20 and 35 of Regulation (EU) 2018/1725 in relation to personal data processed by the Commission which would undermine the purpose of providing IT security operations and services, inter alia, by revealing the Commission's investigative tools, vulnerabilities and methods, or would adversely affect the rights and freedoms and the security of other data subjects, in particular for the processing of personal data in order to:

— communicate alerts and warnings relating to IT security events and incidents;

— respond to and contain IT security events and incidents;

— facilitate tools and operations through security audits, security assessments and vulnerability management;

— increase the awareness of Commission staff in the field of cybersecurity;

— monitor, detect and prevent the occurrence of IT security events and incidents;

— review privileged user accounts.

the Commission may restrict the application of:

(a) Articles 14 to 17, 19, 20 and 35 of Regulation (EU) 2018/1725;

(b) the principle of transparency laid down in Article 4(1)(a), of Regulation (EU) 2018/1725, in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 17, 19 and 20 of Regulation (EU) 2018/1725.

The Commission may do so in line with Article 25(1)(c), (d) and (h) of Regulation (EU) 2018/1725.

3. Subject to Articles 3 to 7, the Commission may restrict the rights and obligations referred to in paragraph 2 of this Article:

(a) where the exercise of those rights and obligations in respect of the personal data obtained from another EU institution, body, agency or office could be restricted by that other EU institution, body, agency or office on the basis of legal acts provided for in Article 25 of Regulation (EU) 2018/1725, or pursuant to Chapter IX of that Regulation, in accordance with Regulation (EU) 2016/794 of the European Parliament and of the Council ([4]) or in accordance with Council Regulation (EU) 2017/1939 ([5]);

(b) where the exercise of those rights and obligations in respect of the personal data obtained from the competent authority of a Member State could be restricted by competent authorities of that Member State on the basis of legislative measures referred to in Article 23 of Regulation (EU) 2016/679 of the European Parliament and of the Council ([6]), or under national measures transposing Article 13(3), Article 15(3) or Article 16(3) of Directive (EU) 2016/680 of the European Parliament and of the Council ([7]);

([4]) Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the EU Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

([5]) Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO') (OJ L 283, 31.10.2017, p. 1).

([6]) 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) (OJ L 119, 4.5.2016, p. 1).

([7]) Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

(c) where the exercise of those rights and obligations would undermine the Commission's cooperation with non-EU countries or international organisations on common cybersecurity threats.

Before applying restrictions in the circumstances referred to in the first subparagraph, (a) and (b), the Commission shall consult the relevant EU institutions, bodies, agencies, offices or Member State authorities concerning the potential grounds for imposing restrictions and the necessity and proportionality of the restrictions concerned, unless this would undermine the activities of the Commission and unless it is clear to the Commission that the application of a restriction is provided for by one of the acts referred to in those points or that consultation would undermine the purpose of its activities under Decision (EU, Euratom) 2017/46.

The first subparagraph, (c), shall not apply where the interests or fundamental rights and freedoms of the data subject override the interest of the Commission to cooperate with non-EU countries or international organisations.

4. Paragraphs 1, 2 and 3 shall be without prejudice to the application of other Commission Decisions laying down internal rules governing the provision of information to data subjects and the restriction of application of certain rights under Article 25 of Regulation (EU) 2018/1725.

5. Any restriction of the rights and obligations, referred to in paragraph 2 shall be necessary and proportionate to the risks to the rights and freedoms of data subjects.

6. A necessity and proportionality test shall be carried out on a case-by-case basis before restrictions are applied and restrictions shall be limited to what is strictly necessary to achieve the intended purpose.

Article 3

Provision of information to data subjects

1. The Commission shall publish on its website a data protection notice that informs all data subjects of its activities that involve processing their personal data for the purpose of fulfilling its tasks pursuant to Decision (EU, Euratom) 2017/46, including a description of the categories of personal data involved. Where it is possible to do so without compromising IT security, the Commission shall ensure that the data subjects are informed individually in an appropriate format.

2. Where the Commission restricts, wholly or partly, the provision of information to data subjects, whose personal data it processes for the purpose of fulfilling its tasks pursuant to Decision (EU, Euratom) 2017/46 it shall record and register the reasons for the restriction in accordance with Article 6 of this Decision.

Article 4

Right of access by the data subject, right to erasure and right to restrict data processing

1. Where the Commission restricts, wholly or partly, the right of access to personal data by data subjects, the right to erasure, or the right to restrict data processing, as referred to in Articles 17, 19 and 20 of Regulation (EU) 2018/1725, it shall inform the data subject concerned, in its reply to the request for access, erasure or restriction of data processing:

(a) of the restriction applied and of the principal reasons for doing so;

(b) of how to lodge a complaint with the European Data Protection Supervisor or how to seek judicial remedy in the Court of Justice of the European Union.

2. The Commission may defer, omit or deny the provision of information on the reasons for the restriction referred to in paragraph 1 for as long as this would undermine the purpose of the restriction.

3. The Commission shall record and register the reasons for the restriction in accordance with Article 6.

4. Where the right of access is wholly or partly restricted, data subjects may exercise their right of access by contacting the European Data Protection Supervisor, in accordance with Article 25(6), (7) and (8) of Regulation (EU) 2018/1725.

Article 5

Communication of a personal data breach to data subjects

Where the Commission restricts the communication of a personal data breach to the data subject, as referred to in Article 35 of Regulation (EU) 2018/1725, it shall record and register the reasons for the restriction in accordance with Article 6 of this Decision. The Commission shall communicate the record to the EDPS at the time of the notification of the personal data breach.

Article 6

Recording and registering of restrictions

1. The Commission shall record the reasons for any restriction applied pursuant to this Decision including a reference to the legal ground(s) applied for the restriction and an assessment of the necessity and proportionality of the restriction, taking into account the relevant elements set out in Article 25(2) of Regulation (EU) 2018/1725.

2. The record shall state how the exercise of a right by the data subject would undermine the purpose of providing IT security operations and services to the Commission in line with Decision (EU, Euratom) 2017/46, or of restrictions applied pursuant to Article 2(2) or (3) of this Decision, or would adversely affect the rights and freedoms of other data subjects.

3. The Commission shall register these records and any documents containing underlying factual and legal elements. They shall be made available to the European Data Protection Supervisor on request.

Article 7

Duration of restrictions

1. The restrictions referred to in Articles 3, 4 and 5 shall continue to apply as long as the reasons for them remain valid.

2. When the reasons for a restriction referred to in Articles 3, 4 and 5 are no longer valid, the Commission shall:

(a) lift the restriction;

(b) inform the data subject of the principal reasons for the restriction;

(c) inform the data subject of how they can lodge a complaint with the European Data Protection Supervisor at any time or seek judicial remedy in the Court of Justice of the European Union.

Article 8

Safeguards and storage periods

1. The Commission shall review the application of the restrictions referred to in Articles 3, 4 and 5 6 months after their adoption, and at the closure of the individual IT security operation. Thereafter, the Commission shall review and monitor the need to maintain any restriction on an annual basis.

The review shall include an assessment of the necessity and proportionality of the restriction, taking into account the relevant elements set out in Article 25(2) of Regulation (EU) 2018/1725.

2. The Commission has adopted technical and organisational measures to avoid any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed such as access rights management, backup policy and any other measure in line with the Decision (EU, Euratom) 2017/46.

3. The Commission shall record the applicable retention periods in line with the Common Commission-Level Retention List and shall make available to the data subjects the relevant retention periods for these processing activities in its data protection notice.

Article 9

Review by the Data Protection Officer of the Commission

1. The Commission's Data Protection Officer shall be informed, without undue delay, whenever data subjects' rights are restricted in accordance with this Decision. Upon request, the Data Protection Officer shall be given access to the record and any documents containing underlying factual and legal elements.

2. The Data Protection Officer may request a review of the restrictions and shall be informed of the outcome of the requested review.

3. The Commission shall document the involvement of the Data Protection Officer whenever data subjects' rights are restricted in accordance with this Decision.

Article 10

Entry into force

This Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Done at Brussels, 15 December 2021.

For the Commission
The President
Ursula VON DER LEYEN