Commission Decision (EU) 2018/1961 of 11 December 2018 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 purpose of internal audit activities

COMMISSION DECISION (EU) 2018/1961

of 11 December 2018

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 purpose of internal audit activities

THE COMMISSION,

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

Whereas:

(1) Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council[(1)] requires each Union institution to establish an internal audit function which shall be performed in compliance with the relevant international standards. Internal audit activities in the Commission are carried out by the Internal Audit Service ('the Service'), which was established on 11 April 2000. Internal audit activities are also carried out by the Service in Union decentralised agencies and other autonomous bodies receiving contributions from the Union budget.

(2) The Service conducts internal audit activities in accordance with Articles 117 to 123 of Regulation (EU, Euratom) 2018/1046 and its mission charter[(2)]. In this respect, the Service has complete independence and full and unlimited access to all information required in the conduct of its internal audit activities in relation to all the activities and departments of the Union institution concerned.

(3) The Service advises other Commission departments, executive agencies, as well as Union decentralised agencies and other autonomous bodies receiving contributions from the Union budget on how to deal with risks, i.e. any event or issue that could occur and adversely impact the achievement of the Commission's political, strategic and operational objective, by issuing independent opinions on the quality of management and control systems and by issuing recommendations for improving the conditions of implementation of operations and promoting sound financial management, in accordance with Articles 117 to 123 of Regulation (EU, Euratom) 2018/1046. Therefore, the internal audit activities of the Service do not typically target natural persons as such. Nevertheless, during the course of its activities, personal data within the meaning of Article 3(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council[(3)] are inevitably processed. The internal audit activities carried out by the Service involve assessing the suitability and effectiveness of internal management systems and the performance of departments in implementing policies, programmes

Changes to legislation: *There are currently no known outstanding effects for the Commission Decision (EU) 2018/1961. (See end of Document for details)*

and actions, the efficiency and effectiveness of the internal control and audit systems applicable to each budget implementation operation. Therefore, they contribute to the safeguarding of important economic and financial interests of the Union and of the Member States. The Service is a controller for the processing operations it carries out in accordance with Articles 118 and 119(2) of the Financial Regulation.

(4) The internal audit activities performed in the Commission and its executive agencies, and in the Union decentralised agencies and other autonomous bodies vary in form and content, ranging from assurance (including risk assessments) and consulting engagements, to reviews with a limited scope and follow-up engagements.

(5) The Audit Progress Committee (APC), in accordance with its Mission Charter updated on 21 November 2018 (C(2018)7707), is an advisory body[4] that assists the Commission in fulfilling its obligations under the Treaties and other statutory instruments [Regulation (EU, Euratom) 2018/1046] by ensuring the independence of the Internal Audit Service, by monitoring the quality of internal audit work, and by ensuring that internal and external audit recommendations are properly taken into account by the Commission services and that they receive appropriate follow-up. In this way, the APC contributes to the overall further improvement of the Commission's effectiveness and efficiency in achieving its goals and facilitates the College's oversight of the Commission's governance, risk management, and internal control practices. The APC is a controller for the processing operation(s) it carries out in accordance with Article 123 of the Financial Regulation.

(6) For the purpose of its activities under Articles 118 and 119(2) of Regulation (EU, Euratom) 2018/1046, whether acting on its own initiative or on the basis of received input, the Commission processes personal data acquired or received from legal persons, natural persons, Member States and international bodies and organisations. During such internal audit activities, the Service may also process personal data acquired or received from publicly available sources, from anonymous or from identified sources that require protection of their identity.

(7) The Commission may, in turn, exchange personal data with the Union institutions, bodies, offices and agencies, with competent authorities of Member States and, within the framework of the Commission relevant international or cooperation agreements, with third countries and international organisations.

(8) Personal data processing activities, within the meaning of Article 3(3) of Regulation (EU) 2018/1725, carried out in the course of an internal audit activity, may take place even before the Commission formally initiates it, continue throughout the performance of the audit activity and may continue even after the formal closure of the audit activity (for example, for reasons of monitoring of implementation of recommendations, assessing the need for initiating new internal audit activities).

(9) The categories of personal data processed by the Commission include identification data, contact data, professional data and data related to or brought in connection with the subject matter of the activity. These categories of personal data are stored in a secured electronic environment to prevent unlawful access or transfer of data to persons who do not have a need to know. The personal data are retained for a maximum period of

***Changes to legislation:** There are currently no known outstanding effects for the Commission Decision (EU) 2018/1961. (See end of Document for details)*

ten years. At the end of the retention period, the information related to the internal audit activity, including personal data is transferred to the historical archives of the Commission[(5)] or destroyed.

(10) While carrying out internal audit activities, 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 Union and by Article 16(1) of the Treaty, as well as the rights provided for in Regulation (EU) 2018/1725. At the same time, the Commission is required to comply with strict rules of confidentiality referred to in the international internal audit standards, in accordance with Article 117 of Regulation (EU, Euratom) 2018/1046.

(11) In certain circumstances, it is necessary to reconcile the rights of data subjects pursuant to Regulation (EU) 2018/1725 with the needs of internal audit activities, and confidentiality of exchanges of information with natural and legal persons as well as with full respect for fundamental rights and freedoms of other data subjects. To that effect Article 25(1)(c), (g) and (h) of Regulation (EU) 2018/1725 provides the Service with the possibility to restrict the application of Articles 14 to 17, 19, 20 and 35, as well as the principle of transparency laid down in Article 4(1)(a), insofar as its provisions correspond to the rights and obligations provided for in Articles 14 to 17, 19, 20 and 35 of that Regulation.

(12) In order to ensure the effectiveness of internal audit activities, while respecting the standards of protection of personal data under Regulation (EU) 2018/1725, which replaced Regulation (EC) No 45/2001 of the European Parliament and of the Council[(6)], it is necessary to adopt internal rules under which the Commission may restrict data subjects' rights in accordance with Article 25(1)(c), (g) and (h) of Regulation (EU) 2018/1725.

(13) The internal rules should cover all processing operations carried out by the Commission in the performance of its internal audit activities, whether acting on its own initiative or on the basis of received input, whenever the exercise of data subjects' rights may jeopardise the conduct of internal audit activities. Those rules should apply to processing operations carried out prior to the formal initiation of an engagement, during the engagement as well as during the monitoring of the follow-up to its outcome.

(14) In order to comply with Articles 14, 15 and 16 of Regulation (EU) 2018/1725, the Commission should inform all individuals of its activities involving processing of their personal data and of their rights in a transparent and coherent manner by means of a data protection notice published on the Commission's website. Where relevant, the Commission should adduce additional safeguards to ensure that the data subjects are informed individually in an appropriate format.

(15) On the basis of Article 25 of Regulation (EU) 2018/1725, the Commission is also able to restrict the provision of information to data subjects and the exercise of other rights of data subjects in order to protect its own internal audit activities, audits of public authorities of the Member States, the audit tools and methods, as well as the rights of other persons related to its internal audit activities.

Changes to legislation: *There are currently no known outstanding effects for the Commission Decision (EU) 2018/1961. (See end of Document for details)*

(16) In addition, in order to maintain effective cooperation it may be necessary for the Commission to restrict the application of data subjects' rights in order to protect processing operations of Commission services or other Union institutions, bodies, offices and agencies or of Member States' authorities and international organisations, as well as of the Audit Progress Committee. To that effect, the Commission should consult those services, institutions, bodies, offices, agencies, authorities and organisations, as well as the Audit Progress Committee on the relevant grounds for imposing restrictions and the necessity and proportionality of the restrictions.

(17) The Commission may also have 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 third countries or international organisations, in order to cooperate with those countries or organisations and thus safeguard an important objective of general public interest of the Union. However, in some circumstances the interest or fundamental rights of the data subject may override the interest of international cooperation.

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

(19) Pursuant to Article 25(8) of Regulation (EU) 2018/1725, controllers may defer, omit or deny provision of information on the reasons for the application of a restriction to the data subject if providing that information would in any way compromise the purpose of the restriction. This is, in particular, the case of restrictions to the rights provided for in Articles 16 and 35 of Regulation (EU) 2018/1725.

(20) Where other rights of data subjects are restricted, the controller of the Internal Audit Service should assess on a case-by-case basis whether the communication of the restriction would compromise its purpose.

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

(22) Regulation (EU) 2018/1725 replaces Regulation (EC) No 45/2001, without any transitional period, from the date on which it enters into force. The possibility to apply restrictions to certain rights was provided for in Regulation (EC) No 45/2001. In order to avoid jeopardising the lawfulness of internal audit activities, this Decision should apply from the date of entry into force of Regulation (EU) 2018/1725.

(23) The European Data Protection Supervisor delivered an opinion on 27 November 2018,

HAS ADOPTED THIS DECISION:

Article 1

Subject-matter and scope

1 This Decision lays down the rules to be followed by the Commission to inform data subjects of the processing of their data in accordance with Articles 14, 15 and 16 of Regulation

***Changes to legislation:** There are currently no known outstanding effects for the Commission Decision (EU) 2018/1961. (See end of Document for details)*

(EU) 2018/1725, when conducting its internal audit activities in accordance with Articles 117 to 123 of Regulation (EU, Euratom) 2018/1046.

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), (g) and (h) of that Regulation.

2 This Decision applies to the processing of personal data by the Commission for the purpose of or in relation to the activities carried out in order to fulfil its tasks pursuant to Articles 118 and 119 (2) of Regulation (EU, Euratom) 2018/1046.

3 This Decision applies to the processing of personal data within the Commission, in so far as the Commission processes personal data contained in information which it is required to process for the purpose of, or in relation to, the activities referred to in this Article.

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, the Commission may restrict the application of Articles 14 to 17, 19, 20 and 35 of Regulation (EU) 2018/1725, as well as the principle of transparency laid down in Article 4(1)(a) of that Regulation, in so far as its provisions correspond to the right and obligations provided for in Articles 14 to 17, 19, 20 and 35 of that Regulation, where the exercise of those rights and obligations would jeopardise the purpose of the Commission's activities under Articles 118 and 119 (2) of Regulation (EU, Euratom) 2018/1046, including by revealing its audit tools and methods or would adversely affect the rights and freedoms of other data subjects.

3 Subject to Articles 3 to 7, the Commission may restrict the rights and obligations referred to in paragraph 2 of this Article in relation to personal data obtained from other Union institutions, bodies, agencies and offices, competent authorities of Member States or third countries or from international organisations in the following circumstances:

a where the exercise of those rights and obligations could be restricted by other Union institutions, bodies, agencies and offices on the basis of other acts provided for in Article 25 of Regulation (EU) 2018/1725 or in accordance with Chapter IX of that Regulation or in accordance with Regulation (EU) 2016/794 of the European Parliament and of the Council[7] or Council Regulation (EU) 2017/1939[8];

b where the exercise of those rights and obligations could be restricted by competent authorities of Member States on the basis of acts referred to in Article 23 of Regulation (EU) 2016/679 of the European Parliament and of the Council[9], or under national measures transposing Articles 13(3), 15(3) or 16(3) of Directive (EU) 2016/680 of the European Parliament and of the Council[10];

c where the exercise of those rights and obligations could jeopardise the Commission's cooperation with third countries or international organisations in the conduct of internal audit activities.

Before applying restrictions in the circumstances referred to in points (a) and (b) of the first subparagraph, the Commission shall consult the relevant Union institutions, bodies, agencies, offices or competent authorities of the Member States unless it is clear to the Commission that the application of a restriction is provided for by one of the