EDPS comments on the European Commission's draft decision 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 (Case 2021-0710)

1. Introduction

These comments refer to European Commission's draft decision 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, pursuant to Article 25 of Regulation (EU) 2018/1725 ('the Regulation')[1].

The EDPS' comments refer to the document submitted on 13 July 2021 ('the draft Decision')[2].

These comments are provided in accordance with Article 41(2) of the Regulation.

The EDPS would also like to highlight the updated EDPS Guidance on Article 25 of the Regulation.[3]

2. General comments

The EDPS welcomes that the European Commission (EC) will only restrict data subject rights in the framework of the security of information and communication systems based on the draft Decision, which provides a clear legal basis and which, according to the Regulation, should be subject to publication in the Official Journal of the European Union.

The EDPS also takes note of the fact that the EC will record the reasons for any restriction applied pursuant to this draft Decision, including an assessment of the necessity and proportionality of the restriction and of the fact that restrictions will be lifted as soon as the circumstances that justify them no longer apply.

[1] OJ L 295, 21.11.2018, p. 39.
[2] Draft submitted by DG Informatics, Unit DIGIT S.1.
[3] Available on the EDPS website via: https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidance-art-25-regulation-20181725_en.

In order to ensure appropriate general transparency, clarity and foreseeability of these potential restrictions towards data subjects, we take note that the EC will publish data protection notices on its website informing data subjects of its activities involving processing of their personal data for the purposes of the security of EC information and communication systems.

3. EDPS recommendations

Recommendation 1: The EDPS recommends that the EC make a link regarding the processing operations with respect to which restrictions may be imposed and the legal grounds for restrictions, under Article 2 of the draft Decision. In doing so, the EC can use the relevant information mentioned in the Recitals, for e.g. Article 25(1)(c), (d) and (h) of Regulation can be used as a ground for restriction in order to communicate alerts and warnings relating to IT security events and incidents; respond to and contain IT security events and incidents, etc.

Recommendation 2: The EDPS takes note that Article 2 of the draft Decision states that any restriction of the rights and obligations, referred to in paragraph 2 of the same Article, shall be necessary and proportionate taking into account the risks to the rights and freedoms of data subjects. However, the EDPS recommends adding another paragraph in the same Article, clarifying that a necessity and proportionality test shall be carried out on a case-by-case basis before restrictions are applied and that restrictions shall be limited to what is strictly necessary to achieve their objective.

Recommendation 3: Article 2(3) of the draft Decision provides that the EC shall consult the relevant Union institutions, bodies, agencies, offices or competent authorities of the Member States, in case personal data is obtained from them. The EDPS recommends that the EC clarify in the Article that such consultation will concern the potential grounds for imposing restrictions and the necessity and proportionality of the restrictions concerned, unless this would jeopardise the activities of the EC.

Recommendation 4: Article 5 of the draft Decision states that where the EC restricts the communication of a personal data breach to the data subject it shall record and register the reasons for the restriction in accordance with Article 6 of the Decision. The EDPS recommends adding that the EC shall communicate the record to the EDPS at the time of the notification of the personal data breach.

Recommendation 5: The EDPS takes note of Article 6 of the draft Decision, which refers to the record of any restrictions applied pursuant to the Decision. The EDPS recommends

adding that reference to the legal ground(s) applied for the restriction are also mentioned in the record.

Recommendation 6: In line with Article 25(2)(d) of the Regulation, safeguards put in place in order to prevent abuse or unlawful access or transfer should be indicated in the internal rules laying down the conditions for restrictions based on Article 25 of the Regulation. This refers in particular to organisational and/or technical measures, which are necessary in order to avoid breaches or unlawful transfers such as the storage in a safe of physical documents. It may also concern periodic measures to review a given decision on restrictions.

Although the EDPS takes note of Article 7(3) of the draft Decision that provisions the review of the application of restrictions, he recommends adding a separate Article in the draft Decision, exclusively dedicated to such safeguards (including, but not limited to the review of the application of restrictions) and the expansion thereof.

Recommendation 7: In line with Article 25(2)(f) of the Regulation, the internal rules governing the conditions for restrictions based on Article 25 of the Regulation should also refer to the applicable storage periods. The EDPS therefore recommends that the EC add reference to the applicable storage periods in the draft Decision. This recommendation can be combined with Recommendation 7 and result in an Article of the draft Decision dedicated to 'safeguards' and 'storage periods'[4].

Recommendation 8: According to Articles 25(2)(b) and (e) of the Regulation, the internal rules should mention the categories of personal data processed, as well as the specification of the controller or categories of controllers. Therefore, the EDPS recommends including in the draft Decision explicit reference to the categories of personal data that the decision covers (e.g. identification data of natural persons, contact information) and the controller (e.g. IT Security Policy Unit, DG Informatics, EC).

Recommendation 9: Concerning the entry into force of the draft Decision, and given the importance of all persons concerned being aware of their provisions, the EDPS recommends a longer *vacatio legis*, namely 20 days after its adoption.

Brussels, 16 September 2021

(e-signed)

Delphine HAROU

[4] See for example Article 4 of the Model of internal rules appended to the EDPS Guidelines on restrictions.