

Regulation of the Data Protection Authority on processing operations for which a data protection impact assessment is required (DSFA-V)

On the basis of § 21 para. 2 of the Data Protection Act (DSG), BGBl. I Nr. 165/1999, last amended by the BGBl. I Nr. 24/2018, is decreed:

Scope of application

§ 1. The provisions of this regulation shall apply to the data protection impact assessment to be carried out by the data controller in accordance with Article 35(1) of Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data, on the free movement of such data and on the repeal of Directive 95/46/EC (General Data Protection Regulation, hereinafter referred to as the GDPR), ABl. Nr. L 119, 4.5.2016, p. 1.

Processing operations for which a data protection impact assessment is to be carried out

§ 2. (1) If the processing is lawful within the meaning of Art. 6, Art. 9 and 10 GDPR and there is no data processing pursuant to the regulation of the Data Protection Authority on Exceptions to the Data Protection Impact Assessment (DSFA-AV), BGBl. II Nr. 108/2018, a data protection impact assessment shall in any case be carried out in accordance with the following provisions.

(2) A data protection impact assessment shall be carried out by the controller if at least one of the criteria specified in subsections 1 to 6 is fulfilled:

1. processing which involves an assessment or classification of natural persons - including the compilation of profiles and forecasts - for purposes relating to the performance of the person's work, economic situation, health, personal preferences and interests, reliability or behaviour, location or movements, and which is based solely on automated processing and may have negative legal, physical or financial consequences.

2. processing of data for the purpose of evaluating the behaviour and other personal aspects of natural persons and which may be used by third parties to make automated decisions that have legal effects on the persons evaluated or similarly significantly affect them.

3. processing operations aimed at the observation, supervision or control of data subjects, in particular by means of image and related acoustic data processing; and

a) concern data collected via networks or aim at systematic, comprehensive monitoring of publicly accessible areas,

b) public places, which according to § 27 Abs. 2 Sicherheitspolizeigesetz (SPG), BGBl. Nr. 566/1991, can be entered by a group of persons not determined in advance,

c) cover roads with public transport that can be used by anyone under the same conditions in accordance with § 1 Straßenverkehrsordnung 1960 (StVO 1960), BGBl. Nr. 159/1960,

d) cover any premises which may be entered by any person as a result of an obligation to contract,

e) cover locations which, in the public interest, may be entered by any person,

f) include image processing using mobile cameras for the purpose of preventing or defending against dangerous attacks or criminal connections in public and non-public spaces,

g) include image and acoustic processing for the preventive protection of persons or property on private real estate used for residential purposes which is not used exclusively by the controller and by all authorised users living in the common household, or

h) include churches, houses of prayer, insofar as they are not already covered by lit. b and lit. e, and other institutions serving the practice of religion in the community.

4. processing of data using or applying new or novel technologies or organisational solutions which make it difficult to assess the impact on data subjects and the social consequences, in particular through the use of artificial intelligence and the processing of biometric data, provided that the processing does not involve the mere real-time reproduction of facial images.

5. merging and/or cross-checking of data sets consisting of two or more processing operations carried out for different purposes and/or by different controllers, in the framework of a data processing operation going beyond the processing operations normally expected of a data subject, where the use of algorithms makes it possible to take decisions which significantly affect the data subject.

6. processing operations carried out on a highly personal basis on persons, even if the processing is based on consent.

In the case of employment, this shall not apply where there is a works agreement or the agreement of the staff representation. Systematic monitoring is defined as those processes which take place within the framework of a system or in advance, which are organised and methodically carried out.

(3) A data protection impact assessment shall be carried out by the controller if a processing operation meets two or more of the following criteria:

1. Extensive processing of special categories of personal data in accordance with Art. 9 GDPR,
2. extensive processing of personal data on criminal convictions and offences pursuant to Art. 10 GDPR,
3. collection of location data within the meaning of Art. 92 para. 3 Z 6 Telecommunications Act 2003 (TKG 2003), BGBl. I. No. 70/2003, which are processed in a communications network or by a communications service and which indicate the geographical location of the telecommunications terminal equipment of a user of a public communications service,
4. processing data of data subjects in need of protection, such as minors, employees, patients, mentally ill persons and asylum seekers, whereby para. 2 last sentence shall be applied *mutatis mutandis*, or
5. *merging and/or cross-checking data sets consisting of two or more processing operations carried out for different purposes and/or by different data controllers, in a data processing operation going beyond the operations normally expected to be carried out by a data subject, provided that these operations are carried out for purposes for which not all the data to be processed were collected directly from the data subject.*

Personal designations

§ 3. For the personal designations used in this regulation, the form chosen shall apply to all sexes.

References

§ 4. References in this regulation to other federal laws or to regulations are to be understood as references to the respective valid version.

Entry into force

§ 5. This regulation shall enter into force at the end of the day of publication in the Federal Law Gazette.