No. 64418
November 2019

STATE COURANT

Official edition of the Kingdom of the Netherlands since 1814.

Decision on the list of processing operations of personal data for which a data protection impact assessment (DPIA) is mandatory, Authority Personal data

Decision

The Dutch Data Protection Authority,

having regard to Article 35, fourth paragraph, viewed in conjunction with Article 57, first paragraph, under k, of the General data protection regulation;

having regard to the "Guidelines on data protection impact assessments and determination of whether a processing "probably involves a high risk" within the meaning of Regulation 2016/679" dated April 4 2017, last amended and adopted on October 4, 2017, of the European Data Protection Board (hereinafter: the Guidelines);

considering:

that the Guidelines set out nine criteria to be taken into account in the assessment of whether a data protection impact assessment (DPIA) should be carried out, know in the event of:
1. Evaluation or scoring
2. Automated decision-making with legal effect or similar material effect
3. Systematic monitoring
4. Sensitive data or data of a very personal nature
5. Widely processed data
6. Matching or merging datasets
7. Data related to vulnerable data subjects
8. Innovative use or application of new technological or organizational solutions
9. the situation in which as a result of the processing itself endata subjects cannot exercise a right exercise or cannot rely on a service or an agreement";

that for all types of processing of personal data that are on the list, it is indicated which criterion from the Guidelines has been taken into account;

that for all types of processing of personal data that are on the list, it applies in full that must comply with all obligations under the General Data Protection Regulation states;

that the list contains descriptions of types of processing, based on the principle that the controller is obliged to carry out a data protection impact assessment (DPIA) before commencing the processing of personal data;

that the list is not exhaustive and that the processing of personal data may not be listed, but poses a high risk given its nature, scope, context and purposes for the rights and freedoms of natural persons and thus a data protection effect judgment (DPIA) must be done;

that the Dutch Data Protection Authority pursuant to Article 35(6) of the General Regulation Algemene data protection the in Article 63 of the General Data Protection Regulation has applied the said coherence mechanism;

that this coherence mechanism has led to the addition of an additional category of processing operations of personal data, namely biometric data, as well as to some textual changes;

determines

that for the following processing of personal data a data protection impact assessment ling (DPIA) is mandatory:

1. Covert Investigation

Large-scale processing of personal data and/or systematic monitoring where information is collected through research without informing the data subject in advance (for example: covert investigation by private detective agencies, investigation in the of fraud prevention and research on the internet in the context of, for example, online enforcement of royalty). A data protection impact assessment (DPIA) is also mandatory in case of covert camera surveillance by employers in the context of theft or fraud prevention by employees (for this latter processing, a data protection policy must also be impact assessment (DPIA) due to the unequal balance of power between the data subject (employee) and the controller (employer)). [3], [5], [7]

2. Blacklists

Processing involving personal data relating to criminal convictions and criminal offenses facts, data about unlawful or disruptive behavior or data about bad payment behavior by companies or private individuals are processed and shared with third parties (Article 33(4), opening words and under c, of the General Data Protection Regulation (Implementation Act) (black lists or warning lists, such as those used, for example, by insurers, catering companies, retailers, telecom providers as well as blacklists related to illegal behavior of employees, for example in healthcare or by employment agencies). [4], [6], [7], [8]

3. Fraud Fighting

Large-scale processing of (special) personal data and/or systematic monitoring in the framework of anti-fraud measures (e.g. anti-fraud measures by social services or by fraud of insurers). [3], [4], [5], [9]

4. Credit Scores

Large-scale data processing and/or systematic monitoring leading to or using of estimates of the creditworthiness of natural persons, expressed for example brought into a credit score. [1], [2], [3], [4], [5], [9]

5. Financial situation

Large-scale processing and/or systematic monitoring of financial data from which the income or wealth position or the spending pattern of people can be deduced (for example, statements of bank transfers, statements of the balances of one's bank accounts or overviews of mobile or debit card payments). [3], [4], [5]

6. Genetic Personal Data

Large-scale processing and/or systematic monitoring of genetic personal data (for example DNA analyzes for the purpose of mapping personal characteristics, bio-databases). [3], [4], [5]

7. Health Data

Large-scale processing of health data (for example by institutions or health or social services, occupational health and safety services, reintegration companies, (special) educational institutions, insurers, and research institutes) including large-scale electronic exchange of health data (note: individual doctors and individual healthcare professionals are, pursuant to recital 91 of the General Regulation data protection excluding the obligation to carry out a data protection impact assessment (DPIA) to perform). [4], [5], [7]

8. Partnerships

Sharing personal data in or through partnerships in which municipalities or other governments with other public or private parties special personal data or personal data sensitive nature (such as data on health, addiction, poverty, problematic debts, unemployment, social problems, criminal law data, involvement of youth care or social work) with each other, for example in neighborhood teams, safety houses or information nodes. [6], [7], [8]

9. Camera Surveillance

Large-scale and/or systematic monitoring of publicly accessible areas using cameras, webcams or drones. [3], [5]

10. Flexible CCTV Surveillance

Large-scale and/or systematic use of flexible camera surveillance (cameras on clothing or helmet of fire or ambulance personnel, dashcams used by emergency services). [3], [5]

11. Control employees

Large-scale processing of personal data and/or systematic monitoring of activities of employees (e.g. checking e-mail and internet use, GPS systems in (truck) cars of employees or camera surveillance for the purpose of combating theft and fraud). [3], [5], [7]

12. Location Data

Large-scale processing and/or systematic monitoring of location data from or traceable to natural persons (for example by (scan) cars, navigation systems, telephones, or processing location data of travelers in public transport). [3], [5]

13. Communication data

Large-scale processing and/or systematic monitoring of communication data including metadata can be traced back to natural persons, unless and insofar as this is necessary for protection of the integrity and security of the network and service of the provider concerned, or the end-user peripheral. [3], [5]

14. Internet of Things

Large-scale processing and/or systematic monitoring of personal data that are generated by devices that are connected to the Internet and that are connected via the Internet or otherwise send or exchange data ('internet of things' applications, such as smart televisions, smart home appliances, connected toys, smart cities, smart energy meters, medical tools, etc.). [3], [5], [8]

15. Profiling

Systematic and comprehensive assessment of personal aspects of natural persons based on automated processing (profiling), such as, for example, assessment of occupational performance, student performance, economic situation, health, personal or interests, reliability or behavior. [1], [3]

16. Observing and Influencing Behavior

Large-scale processing of personal data whereby systematically via automated sed processing behavior of natural persons observed or influenced, or data are collected and/or recorded about this, including data that is used for the purpose of online behavioral advertisements are collected. [1], [5]

17. Biometrics

Large-scale processing and/or systematic monitoring of biometric data for the purpose of identify a natural person.
Under the General Data Protection Regulation, the processing of biometric data with the aim of uniquely identifying a natural person, is in principle prohibited. In In the Netherlands, additional conditions have been set in Article 29 of the General Implementation Act data protection regulation. Only if the processing is strictly necessary for authentication or security purposes, the processing of biometric data is allowed. [3], [5], [8]

The Hague, 19 November 2019

Authority Personal Data,
A. Wolfsen
chairman