STAATSCOURANT

Point 64418

27 November 2019

Official edition of the Kingdom of the Netherlands since 1814.

Decision concerning list of types of processing of personal data for which a data protection impact assessment (DPIA) is mandatory, the Dutch Data Protection Authority[1]

Decision

The Dutch Data Protection Authority,

having regard to Article 35, paragraph, in conjunction with Article 57(1)(k) of the General Data Protection Regulation;

having regard to the "Guidelines for Data Protection Impact Assessments and determining whether processing is likely to present a high risk" within the meaning of Regulation 2016/679 of 4 April 2017, as last amended and adopted on 4 October 2017, of the European Data Protection Board (hereinafter referred to as: the Guidelines);

taking into consideration:

that the Guidelines set out nine criteria to be taken into account when assessing whether a Data Protection Impact Assessment (DPIA) should be carried out, i.e. in the case of:
1. Evaluation or scoring allocation
2. Automated decision-making with legal effect or equivalent substantial effect
3. Systematic monitoring
4. Sensitive data or data of a very personal nature
5. Data processed on a large scale
6. Matching or merging of datasets
7. Data relating to vulnerable data subjects
8. Innovative use or application of new technological or organisational solutions
9. the situation in which, as a result of the processing themselves, 'the data subjects […] cannot exercise a right or have access to a service or contract';

that, for all types of processing of personal data listed, the criterion taken into account in the Guidelines is indicated;

that all types of processing of personal data on the list are subject to full compliance with all the obligations laid down in the General Data Protection Regulation;

that the list contains descriptions of types of processing operations based on the premise that the controller is obliged to carry out a Data Protection Impact Assessment (DPIA) prior to the commencement of processing of personal data;

that the list is not exhaustive and that the processing of personal data may not be included in the list but, given the nature, size, context and purposes, poses a high risk to the rights and freedoms of natural persons and thus a data protection effect assessment (DPIA);

that, pursuant to Article 35(6) of the General Data Protection Regulation, the Dutch Data Protection Authority has applied the coherence mechanism referred to in Article 63 of the General Data Protection Regulation;

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

Establishes

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

[1] *This is an unofficial translation and if there are any differences in interpretation between this document and the original decision in Dutch, the original decision is the authoritative text.*

1. Covert investigation

Large-scale processing of personal data and/or systematic monitoring where information is collected through investigation without prior notification to the data subject (e.g.: covert investigations carried out by private investigation agencies, anti-fraud investigations and research on the Internet in the context of e.g. online copyright enforcement). A data protection impact assessment (DPIA) is also required in the case of covert camera surveillance by employers in the context of theft or fraud prevention by employees (the latter processing should also be subject to a data protection impact assessment (DPIA) if it only concerns incidental cases) due to the unequal power relationship between the data subject (employee) and the controller (employer).[3], [5], [7]

2. Black Lists

Processing operations in which personal data relating to criminal convictions and offences, data on unlawful or anitisocial behaviour or data on bad payment practices by companies or private individuals are processed and shared with third parties (Article 33, paragraph 4 sub c of the Implementation Law of the General Data Protection Regulation) (black lists or alert lists, such as those used by insurers, catering companies, retail businesses, telecom providers as well as black lists relating to unlawful behaviour of employees, for example in the health care sector or by recruitment agencies).[4], [6], [7], [8]

3. Combating fraud

Large-scale processing of (special categories of) personal data and systematic monitoring in the context combating fraud (e.g. combating fraud by social services or by fraud departments of insurers).[3], [4], [5], [9]

4. Credit scores

Large-scale data processing and/or systematic monitoring that leads to or makes use of estimates of the creditworthiness of natural persons, e.g. expressed in a credit score.[1], [2], [3], [4], [5], [9]

5. Financial situation

Large-scale processing and/or systematic monitoring of financial data from which people’s income or wealth position or spending patterns can be deduced (e.g. bank transfers overviews, balance sheets of someone’s bank accounts or statements of mobile or debit card payments).[3], [4], [5]

6. Genetic Personal Data

Large-scale processing and/or systematic monitoring of genetic personal data (e.g. DNA analyses to identify personal characteristics, biodata banks).[3], [4], [5]

7. Health data

Large-scale processing of health data (e.g. by healthcare or social services institutions, health services, reintegration companies, (special) education institutions, insurers, and research institutes) including large-scale electronic exchange of health data (please note: under recital 91 of the General Data Protection Regulation, individual physicians and individual healthcare professionals are exempted from the obligation to carry out a Data Protection Impact Assessment (DPIA).[4], [5], [7]

8. Joint ventures

Sharing personal data in or through partnerships in which municipalities or other authorities exchange special categories of personal data or personal data of a sensitive nature with other public or private parties (such as data on health, addiction, poverty, problematic debt, unemployment, social issues, criminal data, involvement of youth care or social work), for example in district teams, safe houses or information hubs.[6], [7], [8]

9. Camera surveillance

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

10. Flexible camera surveillance

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

11. Control of workers

Large-scale processing of personal data and systematic monitoring of employee activities (e.g. control of e-mail and internet use, GPS systems in employees' (freight) cars 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 (e.g. by (scan) cars, navigation systems, telephones, or processing of passenger location data in public transport).[3], [5]

13. Communication data

Large-scale processing and/or systematic monitoring of communication data including metadata traceable to natural persons, unless and to the extent necessary for the protection of the the integrity and security of the network and service of the provider concerned, or the end-user peripheral device.[3], [5]

14. Internet of Things

Large-scale processing and/or systematic monitoring of personal data generated by devices connected to the Internet and capable of transmitting or exchanging data via the Internet or by other means ('internet of things' applications, such as smart televisions, smart household appliances, connected toys, smart cities, smart energy meters, medical devices, etcetera).[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 professional performance, student performance, economic situation, health, personal preferences or interests, reliability or behaviour.[1], [3]

16. Observation and Influence of Behaviour

Large-scale processing of personal data that systematically monitors or influences the behaviour of natural persons through automated processing, or collects and/or records data about it, including data collected for the purpose online behavioural advertising.[1], [5]

17. Biometric data

Large-scale processing and/or systematic monitoring of biometric data with the aim of identifying a natural person.
Under the General Data Protection Regulation, the processing of biometric data for the purpose of unique identification of a natural person is in principle prohibited. In the Netherlands, additional conditions are laid down in Article 29 of the Implementation Law of the General Data Protection Regulation. Only if the processing is strictly necessary for authentication or security purposes, the processing of biometric data is permitted.[3], [5], [8]

The Hague, 19 November 2019

The Personal Data Authority,
A. Wolfsen Chairman