Utrecht University

Unofficial translation of the Dutch Data Protection Authority's decision regarding the list of personal data processing operations for which a data protection impact assessment (DPIA) is mandatory

The Dutch Data Protection Authority determines that a data protection impact assessment (DPIA) is mandatory for the following personal data processing operations:

1. Secret investigation

Processing on a large scale and/or systematic monitoring during which personal data is obtained by means of investigation without informing the data subject beforehand.

For example, secret investigations by private investigators, investigations regarding anti-fraud, and investigations on the internet regarding, for instance, the online enforcement of copyright.

A data protection impact assessment (DPIA) is furthermore required for secret video monitoring by employers in order to fight theft and fraud by employees. For this, a data protection impact assessment (DPIA) might also be required because of the imbalance of powers between the employee and the controller.

2. Blacklists

Processing operations for which personal data relating to criminal convictions and offences, unlawful or troublesome behaviour, or payment behaviour, is processed or shared with third parties.

For example, blacklists or warning lists, as used by insurance companies, hospitality services, shops, telecommunication service providers. As well as blacklists relating to unlawful behaviour by employees, as used by, for example, healthcare organisations and employment agencies.

3. Anti-fraud

Large scale processing operations and/or systematic monitoring involving (special category) personal data for the purpose of anti-fraud. For example, anti-fraud by social services or by anti-fraud departments of insurance companies.

4. Credit scores

Large scale processing operations and/or systematic monitoring involving personal data which leads to, or makes use of, estimations of natural persons' financial credibility, as expressed by, for instance, a credit score.

5. Financial situations

Large scale processing operations and/or systematic monitoring involving financial data which leads to insight in people's income, wealth, or transactions. For example, statements of bank transfer, bank account balances, or mobile or card transactions.

6. Genetic personal data

Large scale processing operations and/or systematic monitoring involving genetic personal data. For example, DNA-analyses to map out personal traits, biological databases.

7. Health records

Large scale processing operations and/or systematic monitoring involving health records (for example by health care or social service organisations, occupational safety and health organisations, occupational reintegration companies, (special) education organisations, insurance companies and research institutes), including the electronic sharing of health records on a large scale.

8. Partnerships

The sharing of personal data, such as data on health, addiction, poverty, problematic debts, unemployability, social problems, criminal records, involvement in youth or social care, in or by partnerships between municipalities or other governmental bodies and other public or private parties. Examples of which are 'wijkteams', 'veiligheidshuizen', and 'informatieknooppunten'.

9. Video surveillance

Large scale processing operations and/or systematic monitoring involving publicly available spaces using cameras, webcams, or drones.

10. Flexible video surveillance

Large scale and/or systematic use of flexible video surveillance. For example, cameras on clothing, or first responders' helmets, or dashcams for first responders.

11. Employee monitoring

Large scale processing operations and/or systematic monitoring involving personal data to monitor employee activities. For example, by monitoring email and internet usage, by using GPS-systems in cars or lorries, or by using video surveillance for the purpose of anti-theft and anti-fraud.

12. Location records

Large scale processing operations and/or systematic monitoring involving location data of, or traceable to, natural persons. For example, by using (automatic vehicle

identification) cars, navigational systems, phones, or by processing locational data of public transport travellers.

13. Communication records

Large scale processing operations and/or systematic monitoring involving communicational records, including meta data traceable to natural persons, unless, and only to the extent for which, this is necessary for the protection of the integrity and safety of the network and the providers' service, or the peripheral device of the end user.

14. Internet of things

Large scale processing operations and/or systematic monitoring involving personal data generated by devices which are connected to the internet and which send or share data using the internet. For example, internet of things-applications, such as smart TV's, smart home appliances, connected toys, smart cities, smart electricity meters, medical tools, etcetera.

15. Profiling

Systematic and extensive assessment of personal aspects of natural persons based on automatic decision making (profiling). For example, assessments of occupational achievements, student progress, economic situations, health, personal preferences or interests, reliability of behaviour.

16. Monitoring and influencing behaviour

Large scale processing operations involving personal data which automatically and systematically observe or influence the behaviour of natural persons, or collects data upon this, including data for the purpose of online behavioural advertising.

17. Biometric data

Large scale processing operations and/or systematic monitoring involving biometric data with the purpose of identifying a natural person.