Processing operations subject to the requirement of a data protection impact assessment

1. Introduction

Some data processing activities always require a data protection impact assessment.

The supervisory authority has an obligation to establish and to make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to article 35(4). Such an assessment must be carried out before the processing of personal data is initiated.

This list includes processing activities that the Norwegian DPA considers likely to result in a high risk to the rights and freedoms of data subjects. The Working Party 29's analysis in the Guidelines on Data Protection Impact Assessment (WP 248) is a core element for ensuring consistency across the Union. The document containing our list is based on these guidelines and the criteria set out in the guidelines.

Please note that the list only includes processing activities that, according to the Norwegian DPA, are likely to represent a high risk to the data subjects *by default*. This list is non-exhaustive by nature.

Data controllers still have the obligation to assess whether their processing activities are likely to represent a high risk to the rights and freedoms of the data subjects, even though the processing is not included in this list.

2. Criteria included in the Working Party 29 Guidelines (WP 248)

According to the WP 29 Guidelines, a processing meeting two or more of these criteria would normally require a data protection impact assessment. In some cases a processing meeting only one criteria can also require such an assessment.

- Evaluation or scoring
- Automated-decision making with legal or similar significant effect
- Systematic monitoring
- Sensitive data or data of a highly personal nature
- Data processed on a large scale
- Matching or combining datasets
- Data concerning vulnerable data subjects
- Innovative use or applying new technological or organisational solutions

3. Processing activities included in the Norwegian DPA's list

- Data collected via third parties in conjunction with at least one other criterion.

- For example collecting and combining personal data from third parties in order to decide whether the data subject shall be offered, continue to receive, or shall be denied a product, service or offer. (*Vulnerable data subject and evaluation/scoring*).

- Processing of biometric data for identification purposes in conjunction with at least one other criterion.

    - For example, processing of biometric data for identification purposes on a large scale (*Sensitive data or data of highly personal nature and large scale)*

- Processing of genetic data in conjunction with at least one other criterion.

    - For example processing of genetic data on a large scale, including gene sequencing (*Sensitive data or data of highly personal nature and large scale*)

- Processing of personal data using innovative technology in conjunction with at least one other criterion.

    - For example processing of health data using innovative welfare technology solutions like health implant aids (*Innovative use and sensitive data*)

- Processing of personal data involving measures for systematic monitoring of employee activities.

    - For example, monitoring the employees internet activity, electronic communication or camera surveillance for the purposes of employee monitoring (*Vulnerable subject and systematic monitoring*)

- Processing of personal data without consent for scientific or historical purpose in conjunction with at least one other criterion.

    - For example processing of health data without consent for research purposes (*Evaluation and sensitive data or data of highly personal nature*)

- Processing of location data in conjunction with at least one other criterion.

    - For example combining data subject's location or traffic data from telephone records in a systematic manner, or processing of personal data about the subscriber's use of the telenet or telecom operators services. (*Sensitive data or data of highly personal nature and systematic monitoring)*

- Processing of personal data for the purpose of evaluating learning, coping and well-being in schools or kindergartens. This includes all levels of education, from preschool, elementary, high school to university levels. (*Vulnerable data subjects and systematic monitoring*)

- Systematic monitoring, including camera surveillance, on a large scale, in areas accessible by the public. (*Systematic monitoring and large scale*)
- Camera surveillance in schools or kindergartens during opening hours. *(Systematic monitoring and vulnerable data subjects*)
- Processing of sensitive or highly personal data on a large scale for training of algorithms (*Large scale and sensitive or highly personal data*)
- Processing of personal data to systematically monitor proficiency, skills, scores, mental health and development. (*Sensitive data or data of highly personal nature and systematic monitoring*)
- Processing personal data with the purpose of providing services or developing products for commercial use that involve predicting working capacity, economic status, health, personal preferences or interests, trustworthiness, behavior, location or route (*Sensitive data or data of highly personal nature and evaluation/scoring*)
- Collection of personal data on a large scale through the use of "internet of things" solutions or welfare technology solutions (*Large scale and sensitive or highly personal data*).