List regarding Data Protection Impact Assessments according to article 35.4 of the Data Protection Regulation

According to article 35.1 of the Data Protection Regulation, a personal data controller must carry out an impact assessment if a type of processing is likely to result in a high risk to the rights and freedoms of natural persons. The impact assessment must be carried out prior to the processing.

The controller must always make their own independent assessment of the intended processing in order to determine if an impact assessment is required in each individual case.

The controllers' obligation under article 36 to consult the Swedish Data Protection Authority is linked to the controllers' obligation under article 35 to carry out an impact assessment. However it should be noted that the obligation to request a prior consultation with the Swedish Data Protection Authority only applies if the impact assessment shows that the processing would result in a high risk and this risk is not reduced by appropriate measures taken by the controller.

Article 35.3 lists certain specific situations where an impact assessment is required. Moreover, the supervisory authority shall establish and make public a list of the kind of processing operations that are subject to such an assessment according to article 35.4.

The Swedish Data Protection Authority has, based on guidelines from the Article 29 Working Party[1] and the criteria developed by the Working Party, adopted the following list of where an impact assessment is required.

An impact assessment must be carried out if at least two of the criteria below are met regarding the intended processing operation. At the end of the list, there are also some examples of when at least two of the criteria shall be deemed to be met and where, therefore, an impact assessment must be carried out. The list reflects the criteria developed by the Article 29 Working Party in their guidelines and includes examples that complement and further specify the guidelines.

The list is however not exhaustive and may be updated and supplemented with more examples in the future. The list applies both to personal data processing that takes place in Sweden and to personal data processing that is regarded as cross border according to the definition in article 4.23 of the Data Protection Regulation.

An impact assessment is not required for processing operations that have been checked by a supervisory authority or the data protection official in accordance with article 20 of Directive 95/46/EC and that are performed in a way that has not changed since the prior checking. As a matter of good practice, an impact assessment should however be continuously reviewed and regularly re-assessed.

Where a processing operation that takes place pursuant to article 6.1 c) or e) has a legal basis in EU or Member State law, where the law regulates the specific processing operation and where an impact assessment has already been carried out as part of the establishment of that legal basis, no further impact assessment is necessary according to article 35(10). It may however be necessary to review an impact assessment that is carried out at the stage of elaboration of the legislation, if the adopted legislation differs from the proposal in ways that affect privacy and data protection issues.

[1] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, revised and adopted on 4 October 2017, WP 24 rev. 01.
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

List of when a data protection impact assessment is required according to Article 35.4

In addition to the cases provided for in Article 35.3 GDPR, and taking into account the exception provided for in Article 35.10 GDPR, carrying out a DPIA shall be compulsory if the processing operation meets at least two of the following criteria:

1. Evaluates or rates data subjects, e.g. an organisation that offers genetic tests directly to consumers in order to assess and predict disease and health risks, a credit rating agency or a company that profiles internet users
2. Processes information in order to make automated decisions with legal or similar significant effects
3. Systematically monitors data subjects, e.g. through video surveillance of a publicly accessible area or by collecting data about internet usage in publicly accessible areas
4. Processes sensitive data according to article 9[2] or data of a highly personal nature, e.g. a hospital that stores patients' medical records, a company that collects location data or a bank that handles financial information
5. Processes data on a large scale
6. Combines data from two or more data processing operations in a way that would exceed the reasonable expectations of the data subject e.g. when two filing systems are run against each other
7. Processes data concerning data subjects who can be considered to be in a position of dependence or disadvantage and who are therefore vulnerable, e.g. children, employees, asylum seekers, elderly and patients
8. Uses new technological or organisational solutions, e.g. Internet of Things applications (IoT)
9. Processes data for the purpose of preventing data subjects from using a service or entering into a contract, e.g. when a bank screens its customers against a credit reference database in order to decide whether to offer them a loan

The carrying out of an impact assessment is only mandatory where processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35.1 illustrated by article 35.3 and complemented by article 35.4). A processing operation may fulfil two or more of the criteria above but the controller may still consider the processing not to be "likely to result in a high

[2] Sensitive data includes, according to article 9, biometric data that is processed for the purpose of uniquely identifying a natural person.

risk". In such cases the controller should justify and document the reasons for not carrying out an impact assessment and include the views of the data protection officer.

Examples of processing operations that require an impact assessment to be carried out (please note that this is not an exhaustive list)

In the worklife

- An employer systematically monitors how the employees use the internet and e-mail. (Criteria 3 and 7)
- An employer introduces an entrance control system for employees, which includes processing of biometric data for the purpose of uniquely identifying a natural person, e.g. finger print reading. (Criteria 3,7 and 8)
- An organisation introduces a joint system in which it is possible to report misconduct at the workplace – a so called whistle blowing system. (Criteria 4 och 7)
- Recruitment companies that set up candidate or competence databases. (Criteria 1 and 4)
- Organisations that carry out background checks for recruitment purposes. (Criteria 1,4 and 6)

Marketing

- A company uses its clients' location data, which for example can be collected via a mobile app, for the purpose of sending targeted marketing to the client or for the purpose of planning their marketing strategy. (Criteria 3 and 4)
- A company collects data from social media in order to make profiles of natural persons and subsequently address targeted marketing to certain selected groups of individuals. (Criteria 1 and 3)
- A search engine on the Internet collects data about individuals that use the search engine, for the purpose of creating profiles and targeted marketing. (Criteria 1 and 3)

Sensitive data

- Organisations that offer genetic tests to individuals in order to assess and predict the risk of medical diseases or health conditions or to provide information about ethnic origin. (Criteria 1 and 4)
- A health/medical care provider's processing of personal data except if only on a small scale. Small scale is, for example, a sole medical practitioner who processes data about his/her patients. (Criteria 4, 5 and 7)

- Processing, including storage for archiving purposes, of pseudonymised sensitive personal data that refers to data subjects from research projects or clinical trials. (Criteria 4 and 7)
- Organisations that collect and store sensitive data in order to serve as a basis for future research purposes. (Criteria 4 and 7)

Other examples in the private sector

- A bank or a financial institute which makes automated decisions regarding of whether to grant a loan or not. (Criteria 1,2 and 9)
- A company processes financial data about natural persons on a large scale in order to transfer these data to third parties for credit rating purposes (credit rating activity). (Criteria 4 and 9)
- A company that provides a platform for communication (social media) – where the platform is directed to the public and where users can publish text, images or sound – and collects detailed information about the use of the service. (Criteria 3 and 5)
- A company that, on a large scale, processes data about their clients previous misconduct (a so called black list) for the purpose of determining whether the person should be accepted again as clients or not. (Criteria 4,5 and 9)

The public sector

- A municipality collects personal data including i.a. location data in order to use these for urban planning or transport planning etc. (Criteria 3,4 and 5)
- Processing of childrens' personal data in school activity, if a large number of data subjects are concerned. (Criteria 5 and 7)
- A municipality processes personal data in social welfare, if a large number of data subjects are concerned. (Criteria 4,5 and 7)
- A public authority who, alone or together with other controllers, provides service to the public through digital platforms which entails large scale processing of personal data. (Criteria 4,5 and 8)

Technology

- A company provides products for consumers' homes that are connected via the Internet (smart home products) - for example in order to remotely control heating, ligthing or sound - and collects detailed data about the clients' use of the services. (Criteria 3,4 and 8)
- Organisations within social welfare that use welfare technology, such as robots or video surveillance, in people's homes. (Criteria 3,4 and 8)
- Organisations that use a system for intelligent video analysis in order to distinguish cars and automatically recognise number plates for the

purpose of monitoring driving behaviour on highways. (Criteria 3, 4 and 8)

- A parking company that uses video surveillance which can distinguish number plates in order to charge parking fees. (Criteria 3 and 8)
- Organisations that collect personal data, including location data, that are created through the use of smart cars, e.g. in order to develop technology. (Criteria 3, 4 and 8)
- Organisations that set up smart meters in the homes of electricity consumers in order to develop, transfer and analyse data regarding the consumers on a detailed level. (Criteria 3 and 8)
- Organisations that make big adjustments in their technological infrastructure and process personal data within, for example, health and medical care or social welfare. (Criteria 4, 7 and 8)