úřad pro ochranu osobních údajů
the office for personal data protection

List of processing operations subject to data protection impact assessment

Office for Personal Data Protection of the Czech Republic

This document develops on the WP29 Guidelines on Data Prtoection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. This paper is neither definitive nor exhaustive and can be subject to eventual amanedments to keep up with the technology development, changes in the legal environment, etc. Each controller should carry out an analysis of the data processing operations. The method of such analysis is explained below.

Method

When drafting the solution, the Czech SA proceeded from the *Guidelines on Data Prtoection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* which describe the method of how to identify data processing operations entailing high risks to the rights and freedoms of data subjects on the grounds of defined characteristics.

When evaluating the degree of risk related to a data processing, it is necessary to capture the nature of the operation by means of of characteristics which enable to describe every data processing operation and subsequently to determine on the basis of values of these characteristics whether the processing belong to the high-risk category or not. A pre-defined scale or range, i.e. a list of values or intervals of values (hereinafter "the values") that each individual characteristics can acquire shall be used. Each processing thus can be described by a unique set of values. Then the values per characteristics shall be sorted into three (at maximum) groups according to the level, where each group is marked differently, i.e. critical values in red, siginificant values in yellow and low values in green. A processing qualifies as a high-risk operation, if the value of two or more characteristics attains red (critical) or one parameter hits red (critical) and, at the same time, five values at least hit yellow (significant):

- Each characteristics shall be included by taking into account only one single level (the highest one)
- If the level (intensity) of two or more characteristics hit a critical limit, the DPIA shall be carried out
- If one characteristics hits critical level and, at the same time, five characteristics at least reaches a siginificant level, the DPIA shall be carried out then.

(Note: It is not possible, in drafting the method, to presume compliance with specific prerequisites (for instance meeting of some technical or organizational measures like data pseudonymisation) or influence of specific factors (for instance taking into account threats with effect on the processing). These considerations shall be part of the DPIA itself, which is a subsequent step (where on the basis of an analysis one arrives at the conclusion that the data processing entails high risks to the rights and freedoms of data subjects)).

Method recommended to controllers –controllers should look, if the processing in question happens to be on the list of operations for which no DPIA is required. In other words, the controller should determine in the first place, whether the intended or already performed processing is covered by an exemption from the obligation to carry out a DPIA (for example, in case of processing carried out by a public authority on a legal basis, could it be possible that the processing brings about a high level of risk, but a full-bodied DPIA might have been done during the legislative consultation procedure, and consequently, the controller, in accordance with the list of processing operations that are not subject to DPIA, does not need to carry out this exercise). If the controller´s processing is not exempt (it cannot be found on the list of processing opertions not subject to DPIA), then a DPIA pursuant the criteria presented in this document is mandatory.

If the analysis shows the processing is likely to result in a high risk to the rights and freedoms of data subjects, the controller will have to do a DPIA (identification of risks, threats and technical and organizational measures intended to reduction or elimination of those risks). The controller obtains through the elaboration of a DPIA sufficient information that help introduce appropriate technical and organizational measures. It will be furthermore secured that the adopted measures are not insufficient (not providing sufficient protection of personal data) or, the other way round, not unnecessarily stringent (thus needlessly expensive in most cases).

Analysis of data processing operations

Processing including monitoring of data subjects (criterion 3 in the guidelines)

Data subjects are identifiable/identified and localizable ●
(*Note: It concerns foremost the processing of data capturing physical movement or location of identified/identifiable data subjects, namely through their geographic coordinates. A normal use of a simple footage and other monitoring of employees will qualify for this category only in case that the employee monitoring shall determine their movements or continuously monitor their activity (possible interference with the Labour Code). In such a case the condition presented at the beginning must be met (at least one other characteristics on the critical level (red) or five characteristics on siginficant level (yellow) are necessary to ground the render a DPIA mandatory). Localization of movement by means of a range of cameras, even of varying controllers, is above all a competence of security corpses not bound by the Regulation 2016/679. Taking audio records for contractual purposes* is beyond this scope as well.

Data subjects are identifiable/identified and recognizable ●
(*Note: It concerns namely the processing of image records of identified/identifiable data subjects for purposes of property protection and improved security of persons, i.e. a common video surveillance system)*.

Data subjects are identifiable/identified and otherwise monitored ●
(*Note: It concerns subjects that are identified or identifiable by means of unique identification data or set of other data and other records of activity. This includes for instance recorded monitoring of vital functions of patients, time and attendance systems, audio records, records of a data subject´s activity in the web*).

Processing of critical data, data facilitating direct identification, and/or revealing highly personal aspects of data subjects (criterion 4 in the guidelines)

Critical data ●
Special category of data concerning matters related to criminal convictions and offences
(Note: The processing includes data on racial or ethnic origin, political opinions, religion, philosophical beliefs, trade union membership, health, sex life or orientation of a natural person, genetic data, biometric data processed for the purposes of unique identification of a natural person (including biometric cameras and similar devices), data concerning criminal convictions and offences, etc.).

Data of highly personal nature

(*Note: For example data from logs, history of visited websites, data on phone calls, data from electronic mail, data from devices (e.g. ICT) used by data subject, financial data (which includes data on property, amount of financial means, debts or loans, payment moral, etc.*).

Significant data ●

Data enabling to act/negotiate on behalf of a data subject in relation to matters of harm to honour, reputation, characater, integrity

(*Note: The processing includes user name, password/PIN, role, pseudonym, registered offences or penalties, participation in specific events, etc.).*

Data enabling to consume on behalf of the data subject´s account services, goods, or to withdraw money

(*Note: The processing includes data like name of subject (jointly name and surname), date of birth, credit card number, password/PIN, customer number, phone number, e-mail address, address of stay, property ownership, means of transport ownership, etc.).*

Unique identification data

(*Note: The processing includes name of subject (jointly name, surname, titles, date of birth), birth number, social security number, health insurance number, identity card number, passport number, driving licence number, etc.*).

Common data ●

Data linked to data subejct´s behaviour

(Note: The processing includes data related to participation in common events, education, experience record, interests, membership, etc.).

Other personal data including certain specific cases

(*Note: The processing includes softbiometric data (weight, height, dress size, hair colour, eye colour, sex, age, etc.), simple image records, identifiers of subjects that are not unique, shopping data, etc.*).

Processing including personal data exposing data subjects to vulnerability-provoking environment (Criterion 7 of the guidelines)

Upon classification pursuant this characteristics of the processing, it is necessary to take into account, if the processing focuses solely on subjects from a specified group (pupils, patients, migrants).

Permanent vulnerability ●

(*Note: Subjects are classable as members of a specified group pursuant nationality, religion, sexual orientation, physical or mental handicap, conviction for criminal offence, etc.*).

Limited vulnerability ●

Timely limited vulnerability

(*Note: Subjects are classable as members of a specified group depending on whether they are migrants, ill people, old people, children, teenagers, etc.*).

Conditioned-by-situation vulnerability

(*Note: Subjects are classable as members of a specified group depending on whether they are applicants towards public administration, employees in relation to their employer, recipients in relation to the health or social services providers, consumers of medicaments or of erotic aids*).

Without specific vulnerability ●

Processing of personal data on a large scale (Criterion 5 of the guidelines)

Data processing on a large scale ●

For specification of this category, it is rcommended (in accordance with the guidelines WP243 and WP248) to reflect above all the following factors (number of data subjects concerned, volume of data and/or extent of data processed, duration of the processing operation, and territorial extent of the processing) so that the determination will be done on a case-by-case basis.

(Note: The European Data Protection Board insists on leaving out any explicit quantifiers related to processiong operations pursuant Article 35(6) (specific processing operations carried out on several member

states). As a support for controllers who decide to carry out an analysis of their processing operations (namely those established and runnnig their operations on the Czech Republic´s territory), we recommend considering the following figures when determining, if a processing is of large scale:

- *from 10001 data subjects or more than 1,0 ‰ of the Czech Republic´s population or that of the countries concerned,*
- *and/or more than 20 persons with access/employees of the controller,*
- *and/or more than 20 locations where processing takes place /branches,*
- *plus simultaneously the state level (NUTS 1) from the viewpoint of origin/place of stay of data subjects).*

Data processing on mid-sized scale ●

For specification of this category, it is rcommended (in accordance with the guidelines WP243 and WP248) to reflect above all the following factors (number of data subjects concerned, volume of data and/or extent of data processed, duration of the processing operation, and territorial extent of the processing.
(Note: The European Data Protection Board insists on leaving out any explicit quantifiers related to processiong operations pursuant Article 35(6) (specific processing operations carried out on several member states). As a support for controllers who decide to carry out an analysis of their processing operations (namely those established and runnnig their operations on the Czech Republic´s territory), we recommend to consider the following figures when determining, if a processing is of mid-sized scale:

- *from 5001 to 10000 data subjects or in the interval of 0,5-1,0 ‰ of the Czech Republic´s population or that of the countries concerned,*
- *and/or from 2 to 20 persons with access/employees of the controller,*
- *and/or with 5-20 locations where processing takes place /branches,*
- *and a level of at least a region (NUTS2) or a district (NUTS3) from the viewpoint of origin/place of stay of data subjects).*

Data processing on small scale ●

For specification of this category, it is rcommended (in accordance with the guidelines WP243 and WP248) to reflect above all the following factors (number of data subjects concerned, volume of data and/or extent of data processed, duration of the processing operation, and territorial extent of the processing.

- *(Note: The European Data Protection Board insists on leaving out any explicit quantifiers related to processiong operations pursuant Article 35(6) (specific processing operations carried out on several member states). As a support for controllers who decide to carry out an analysis of their processing operations (namely those established and runnnig their operations on the Czech Republic´s territory), we recommend to consider the following figures when determining, if a processing is of small scale:from 5000 data subjects or less than 0,5 ‰ of the Czech Republic´s population or that of the countries concerned*
- *and/or up to 2 persons with access/employees of the controller,*
- *and/or with 1-4 locations where processing takes place /branches,*
- *plus level of at least a municipality from the viewpoint of origin/ place of stay of data subjects).*

<u>Processing including video surveillance of publicly-accessible areas (Criterion 3 of the guidelines)</u>

Detailed level – publicly accessible places ●

(Note: It concerns public spaces, malls, airports, etc. – if video surveillance systmes monitor public spaces on a large scale).

Detailed level – areas with limited public access or unaccessible ●

(*Note: It concerns owner´s property, interior of objects like apartment buildings, industrial plants, shops and public spaces, if in a very limited extent (1-1,5m), closely attached to the monitored object – it relates to other video surveillance systems).*

<u>Procesing of personal data in situations of data subject´s limited capacity of influence (Criterion 9, criterion 1 of the guidelines)</u>

Data processing or transfer that a data subject cannot influence ●

(*Note: It concerns processing that a data subject can influence only in to very limited extent, i.e. operations, on which a data subject can only partially exercise the right provided by the Regulation 2016/679 or some*

rights even cannot be actionable at all (the right to erasure of personal data). Typically, these are processing operations which are performed by the controller on the basis of a legal provision or as a result of automated decision-making).

Data processing or transfer that a data subject can influence to a limited extent ●
(*Note: It concerns processing that a data subject can influence only partially, i.e. operations, where a data subject can exercise only some of the rights provided by the Regulation 2016/679, or in case of other rights (the right to erasure of personal data), a data subject can exercise them only partially, hence for instance, over a limited period of time only or under certain conditions. These are processing operations, where data are necessary for application of rights and obligations ensuing from a law (if not directly anchored in the law, for example entering into contracts).*

Data processing or transfer that a data subject can influence ●
(*Note: It concerns processing in relation to which a data subjects can exercise their rights pursuant the Regulation 2016/679 without problems*).

Processing of publicly available personal data (partially criteria 4 and 9 of the guidelines)

Data are publicly accessible to an unlimited number of subjects ●
(Note: It concerns data disclosed to the public by the controller, e.g. on basis of legal regulations).

Data are publicly accessible to a limited number of subjects ●
(Note: It concerns data disclosed to the public by the controller to a limited (selected beforehand) groupd of subjects).

Data are not publicly accessible ●
(Note: It concerns data accessible solely to the controller or the processor, or as the case may be, to public authorities on basis of legal regulations).

●

Processing of personal data in technically complex or advanced infrastructures or platforms (partially criteria 6, 5, and 1 of the guidelines)

Automated expert systems including artificial intelligence ●
(Note: Systems serving for analysing or profiling).

System linked to other processing operations performed by the same controller or data obtained from other controllers ●
(*Note: It concerns namely processing operations bringing about matching/combining of data obtained for varying purposes*).

Simple or complex system without linkage to other processing carried out by the same controller ●
(Note: It concerns a simple canetation of operations or operations with differing or multiple links).

Processing interconnected with other controllers or processors (partially criterion 6 and criterion 9 of the guidelines)

Link to controller not specified unambiguously ●
(Note: The linkage occurs for instance only via the category of controllers, e.g. public administration authorities, hospitals, schools, members of business associations with the reasoning that the list cannot be specified exhaustively or it is variable).

Link to controller/processor specified unambiguously ●
(Note: It is possible to provide an exhaustive list of controllers and/or processers).

No link to other controllers and/or processors ●

Processing applying new technological and/or organizational solutions (criterion 8 of the guidelines)

Completely new solution (personal data processing not executed so far) ●
(*Note: It concerns solutions that are new for the controller, nowhere applied so far, with which no experience is available*).

New solution (of a personal data processing already known) by the controller ●
(*Note: It concerns solutions that are new, but the controller can profit from experience of another consortium member (including members within EEC) or of other subject (a supplier, for instance).*

Similar solution by the controller already applied elsewhere or deployed newly, but it is a repeated solution (offered at the market by a supplier with scalable setting) ●
(*Note: It concerns solutions which the controller already has experience with or solutions deployed and tested on multiple occassions – "box solutions" or "turnkey solutions", delivered and adjustable following the controller´s needs*).