Bld.Gen. Gheorghe Magheru Nr. 28-30, Sector 1, Cod poştal 010336, Bucureşti ; Tel: +40.31.805.9211; Fax:+40.31.805.9602 www.dataprotection.ro; e-mail: anspdcp@dataprotection.ro

Decision no. 174 of the 18th of October 2018 on the list of kind of processing operations which are subject to the requirement for a data protection impact assessment

Considering the need to ensure an efficient protection of the rights of persons whose personal data are subject to processing, especially in the case of certain operations of processing of personal data that present risks for the rights and freedoms of the persons, due to the nature of the data processed, the purpose of the processing, the specific character of the categories of data subjects or the mechanisms used to process the data,

taking into account Article 35 paragraph (1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, hereinafter the General Data Protection Regulation, provides that, where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data,

having regard to the provisions of Article 35 paragraph (3) of the General Data Protection Regulation concerning the cases in which, in particular, the data protection impact assessment is required,

taking into consideration Article 35 paragraph (4) of the General Data Protection Regulation which provides that the supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment which it shall communicate to the European Data Protection Board, corroborated with Article 35 paragraph (6) of the General Data Protection Regulation,

bearing in mind Article 35 paragraph (10) of the General Data Protection Regulation, which provides that, where processing pursuant to point (c) or (e) of Article 6 paragrah (1) of the same regulation has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, Article 35 paragraphs 1 to 7 of the General Data Protection Regulation shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

taking into account Article 35 paragraph (11) of the General Data Protection Regulation, which provides that, where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations,

having regard to Article 63 of the General Data Protection Regulation, which provides that, in order to contribute to the consistent application of this Regulation throughout the Union, the supervisory

authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism,

taking into account Article 64 paragraph (1) letter a) of the General Data Protection Regulation, according to which the European Data Protection Board shall issue an opinion where a competent supervisory authority intends to adopt the list of the processing operations subject to the requirement for a data protection impact assessment,

having regard to the Recital (71) of the General Data Protecition Regulation, the data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

having regard to the Recital (75) of the General Data Protection Regulation, according to which the risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

having regard to the Recital (84) of the General Data Protection Regulation, according to which, in order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for

the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

having regard to the Recital (89) of the General Data Protection Regulation, according to which Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

having regard to the Recital (90) of the General Data Protection Regulation, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

having regard to the Recital (91) of the General Data Protection Regulation, the data protection impact assessment should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.

having regard to the Recital (92) of the General Data Protection Regulation, according to which there are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

having regard to the Recital (94) of the General Data Protection Regulation, according to which, where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

taking into account the Guidelines on the data protection impact assessment (DPIA) and establishment if a processing is "likely to result in a high risk" within the meaning of Regulation (EU) 2016/679 (WP 248, revised version), adopted by the Article 29 Working Group on the 4th of October 2017 and endorsed by the European Data Protection Board, including the mentions regarding to the working "on large scale" and "systematic monitoring",

taking into account that the list of operations which are subject to the requirement of a data protection impact assessment is not exhaustive,

taking into consideration the Opinion no. 19 of the 25th of September 2018 of the European Data Protection Board, communicated on the 2nd of October 2018, on the draft list of processing operations which are subject to the requirement of a data protection impact assessment [Article 35 paragraph (4) of the General Data Protection Regulation] elaborated by the National Supervisory Authority for Personal Data Processing,

based on the Referral of the International Department no. 134 of the 15th of October 2018 on the draft Decision on the list of kind of processing operations which are subject to the requirement for a data protection impact assessment

pursuant to the provisions of Article 3 paragraphs (5) and (6), of Article 10 paragraph (1) letters a) and b) of Law no. 102/2005 on the set up, organisation and functioning of the National Supervisory Authority for Personal Data Processing, with further amendments and completions, of Article 6 paragraph (2) letter b) of the Regulation on the set up and organisation of the National Supervisory Authority for Personal Data Processing, approved by Decision no. 16/2005 of the Standing Bureau of the Senate, with further amendments and completions,

the president of the National Supervisory Authority for Personal Data Processing issues this decision

Article 1
(1) The data protection impact assessment by data controllers shall be mandatory especially in the following cases:
a) the processing of personal data in order to perform a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b) processing on a large scale of special categories of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation or of personal data relating to criminal convictions and offences;
c) the processing of personal data having as purpose the systematic monitoring of a publicly accessible area on a large scale, such as: video surveillance in shopping centres, stadiums, markets, parks or other such spaces;
d) processing on a large scale of personal data of vulnerable persons, especially children and employees, through automatic means of systematic monitoring and/or recording of behaviour, including in order to carry out advertising, marketing and publicity activities;
e) processing on a large scale of personal data through the innovative use or the implementation of new technologies, especially if the respective operations limit the ability of the data subjects to exercise their rights, such as the use of facial recognition techniques to facilitate access to different spaces;
f) processing on a large scale of data generated by devices with sensors that transmit data over the Internet or other means (“IoT” applications, such as smart TVs, connected vehicles, smart meters, smart toys, smart cities or other such applications);
g) processing on a large scale and/or systematic of traffic and/or location data of natural persons (such as Wi-Fi monitoring, processing of geo-location data of passengers in public transport or other such situations) when processing is not necessary to provide a service requested by the data subject.
(2)
By exception from paragraph (1), the data protection impact assessment shall not be mandatory when the processing carried out under Article 6 paragraph (1) letter (c) or (e) of the General Data Protection Regulation has a legal basis in Union law or in the national law and an data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of the respective normative acts.

Article 2
This decision shall enter into force on the date of its publication in the Official Journal or Romania, Part I.

-****

- President of the National Supervisory Authority for Personal Data Processing,
Ancuţa Gianina Opre

Published in the Official Journal no. 919 of the 31st of October 2018