DECISION OF THE EUROPEAN DATA PROTECTION SUPERVISOR OF 16 JULY 2019 ON DPIA LISTS ISSUED UNDER ARTICLES 39(4) AND (5) OF REGULATION (EU) 2018/1725

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC[1], and in particular Articles 39(4) and (5) thereof,

Having consulted the European Data Protection Board,

Whereas:

(1) The EU institutions, bodies, offices and agencies process large amounts of personal data about natural persons both inside and outside the institutions. This processing, even when done lawfully, may cause risks to the rights and freedoms of such persons. Data protection rules serve to ensure that personal data are processed responsibly in a way that minimises these risks. Documentation obligations scale with these risks – 'riskier' processing operations demand a more detailed analysis.

(2) Data Protection Impact Assessments (DPIAs) are a new concept in Regulation (EU) 2018/1725 ('the Regulation'). They are a structured process for managing data protection risks of certain processing operations causing 'high risks' to data subject and are not necessary for all kinds of processing operations.

(3) In accordance with Article 39(1) of the Regulation, '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'.

(4) Under Article 39(4) of the Regulation, the EDPS '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'.

(5) Under Article 39(5) of the Regulation, the EDPS 'may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required'.

(6) Under Article 39(6) of the Regulation, the EDPS shall, prior to their adoption, submit draft lists under Article 39(4) and (5) to the European Data Protection Board (EDPB) for examination under point (e) of Article 70(1) of Regulation (EU) 2016/679 where 'they refer to processing operations by a controller acting jointly with one or more controllers other than Union institutions and bodies.'

[1] OJ L 295, 21.11.2018, p. 39-98.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

(7) As there should be no difference in treatment between situations in which Union institutions or bodies are joint or sole controllers and situations in which they are joint controllers with one or more controllers other than Union institutions and bodies, the EDPS has decided to establish a single list for Article 39(4). However, the Article 39(5) list covers only situations in which Union institutions or bodies are joint or sole controllers without the involvement of controllers other than Union institutions and bodies, because the processing operations listed there relate to Union institutions' or bodies' processing for their internal management.

(8) In accordance with recital 5 of the Regulation, 'whenever the provisions of this Regulation follow the same principles as the provisions of Regulation (EU) 2016/679, those two sets of provisions should […] be interpreted homogeneously, in particular because the scheme of this Regulation should be understood as equivalent to the scheme of Regulation (EU) 2016/679'.

(9) Already before the applicability of Regulation (EU) 2016/679, the Article 29 Working Party has provided guidelines on Article 35 of that Regulation[2], which follows the same principles as Article 39 of the Regulation. These guidelines included a set of the criteria to be used in determining 'high risk'. During its first plenary meeting the EDPB endorsed the GDPR-related WP29 Guidelines.[3]

(10) These guidelines confirmed that such lists could not be exhaustive, but would list the criteria for assessing whether there are likely to be high risks for data subjects. Any specific processing operations mentioned are only illustrative examples. If a specific processing operation is not listed in Annex 2 that does not mean that no DPIA is necessary. Conversely, if a processing operation is not listed in Annex 3 that does not mean that a DPIA is necessary.

(11) In February 2018, the EDPS has published provisional guidance on documentation obligations[4] under the – at that time not yet adopted – Regulation. This included first indications of which kinds of processing operations would require a DPIA, following the guidance published by the Article 29 Working Party and later endorsed by the EDPB. The present list builds on the guidance given to controllers in that document.

(12) The draft list has been submitted to the EDPB on 18 March 2019; an updated version has been submitted on 21 June 2019. The EDPB issued its reply on 10 July 2019[5]. The final list as adopted takes into account all EDPB recommendations.

(13) The European Commission may adopt implementing Acts for Article 40(4) of the Regulation, establishing a list of cases in which the controllers shall consult with, and obtain prior authorisation from the EDPS. For the EDPS to have a solid basis for deciding on such consultation and authorisation, the controller should carry out a DPIA in those cases as well.

HAS ADOPTED THIS DECISION:

---

2 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, wp248rev.01, adopted 4 April 2017, as last revised and adopted on 4 October 2017.

3 EDPB Endorsement 1/2018.

4 Accountability on the ground: Provisional guidance on documenting processing operations for EU institutions, bodies and agencies, initial version published 6 February 2018.

5 Recommendation 01/2019 on the draft list of the European Data Protection Supervisor regarding the processing operations subject to the requirement of a data protection impact assessment (Article 39.4 of Regulation (EU) 2018/1725).

Article 1

Subject matter and objectives

1. This Decision further explains in which controllers subject to Regulation (EU) 2018/1725 have to conduct data protection impact assessment (DPIA) under Article 39 of that Regulation.
2. This Decision is without prejudice to the rules on data protection impact assessments and prior consultation in Articles 39 and 40 of that Regulation.

Article 2

Scope and definitions

1. This Decision applies to all controllers subject to Regulation (EU) 2018/1725.
2. For the purposes of this Decision, the definitions in Article 3 of Regulation (EU) 2018/1725 shall apply.

Article 3

Processing operations requiring a DPIA [Article 39(4) of the Regulation]

1. When assessing whether their planned processing operations trigger the obligation to conduct a DPIA under Article 39 of Regulation (EU) 2018/1725, the controller shall use the template in Annex 1 to this Decision to conduct a threshold assessment.
2. Where two or more of the criteria in the template in Annex 1 are applicable, the controller shall in general carry out a DPIA.
3. If a controller decides not to carry out a DPIA, although more than one criterion in the template in Annex 1 is applicable, the controller shall document and justify that decision.
4. If planned processing operations only trigger one criterion in the template in Annex 1, the controller may still decide to carry out a DPIA.
5. Annex 2 to this Decision lists some common processing operations likely to require a DPIA. In those cases, the controller does not have to conduct a threshold assessment, but shall directly conduct a DPIA.

Article 4

Processing operations requiring mandatory prior consultation [Article 40(4) of the Regulation]

Where the European Commission adopts implementing acts for Article 40(4) of Regulation (EU) 2018/1725 obliging controllers to consult with, and obtain prior authorisation from, the EDPS, controllers shall also carry out DPIAs for processing operations listed in such implementing acts.

Article 5

Processing operations not requiring a DPIA [Article 39(5) of the Regulation]

Annex 3 to this Decision lists some common processing operations prima facie unlikely to require a DPIA.

Article 6

Non-exhaustive character of the lists

The lists of processing operations annexed to this Decision are non-exhaustive.

Article 7

Entry into force

This Decision shall enter into force the day following its publication.

For the European Data Protection Supervisor

[signed]
Wojciech Rafał WIEWIÓROWSKI

Annex 1

List of criteria for assessing whether processing operations are likely to result in high risks

In general, if two or more of the criteria in the list apply, the controller should carry out a DPIA. If the controller considers that in the specific case at hand, risks are not 'high' even though there is more than one 'yes', the controller has to explain and justify why they think the processing is in fact not 'high risk'. Each criterion is followed by some examples and counterexample on what would likely (not) trigger each criterion.

I Header	
Name of processing operation	[name]
Controller contact point	[function and contact details]
Record of processing operations	[record reference]
DPO consultation	[date of feedback]
Approval	[name and date]
II Criteria for processing 'likely to result in high risk'	
Criterion	*Applicable? Yes [if so, describe how] / No [if borderline: why not?]*
1. Systematic and extensive evaluation of personal aspects or scoring, including profiling and predicting. *Examples: a bank screening transactions in accordance with applicable law to detect possibly fraudulent transactions; profiling staff based on their transactions in a case management system with automatic reassignment of tasks.* *Counterexamples: standard appraisal interviews, voluntary 360° evaluations for helping staff to develop training plans.*	[Y (how?) / N]
2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects *Example: automated staff appraisal ('if you're in the lowest 10% of the team for the number of cases dealt with, you'll receive a "unsatisfactory" in your appraisal, no discussion').* *Counterexample: a news site showing articles in an order based on past visits of the user.*	[Y (how?) / N]
3. Systematic monitoring: processing used to observe, monitor or control data subjects, especially in publicly accessible spaces. This may cover video-surveillance but also other monitoring, e.g. of staff internet use. *Examples: covert CCTV, smart CCTV in publicly accessible spaces, data loss prevention tools breaking SSL encryption, tracking movements via location data.* *Counterexample: open CCTV of garage entry not covering public space.*	[Y (how?) / N]

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

4. Sensitive data or data of a highly personal nature: data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for uniquely identifying a natural person, data concerning health or sex life or sexual orientation, criminal convictions or offences and related security measures or data of highly personal nature. *Examples: pre-recruitment medical exams and criminal records checks, administrative investigations & disciplinary proceedings, any use of 1:n biometric identification.* *Counterexample: photos are not sensitive as such (only when coupled with facial recognition / biometrics or used to infer other sensitive data).*	[Y (how?) / N]
5. Data processed on a large scale, whether based on number of people concerned and/or amount of data processed about each of them and/or permanence and/or geographical coverage: *Example: European databases on disease surveillance.* *Counterexample: invalidity procedures under Article 78 of the Staff Regulations in a medium-sized EUI .*	[Y (how?) / N]
6. Datasets matched or combined from different data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject. *Examples: cross-checking access control data and self-declared working hours following a suspicion of fraudulent declarations in an administrative inquiry (following the applicable rules).* *Counterexample: further use of data processed for a grant application when auditing the grant process.*	[Y (how?) / N]
7. Data concerning vulnerable data subjects: situations where an imbalance in the relationship between the position of the data subject and the controller can be identified. *Examples: children, asylum seekers.* *Counterexamples: delegates in a Council Working Party (for attendance lists), members of expert groups (for travel cost reimbursement).*	[Y (how?) / N]
8. Innovative use or applying technological or organisational solutions that can involve novel forms of data collection and usage. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. *Examples: machine learning, connected cars, social media screening of job applicants.* *Counterexample: 1:1 biometric access control using fingerprints.*	[Y (how?) / N]
9. Preventing data subjects from exercising a right or using a service or a contract. *Examples: exclusion databases, credit screening.* *Counterexample: determination of rights upon entry into service (e.g. expatriation or dependent child allowances).*	[Y (how?) / N]
III Conclusion	
Number of 'Yes' ticked above	[n]
Assessment: In general, if you tick two or more of the criteria in the list, you should carry out a DPIA. If you consider that in the specific case at hand, risks are not 'high' even though you have two or more 'yes', explain and justify why you think the processing is in fact not 'high risk'.	[explain]

Annex 2
Non-exhaustive list of some common processing operations and prima-facie indications of their risks

Positive list of processing operations prima facie requiring a DPIA (the numbers inside the brackets refer to the criteria in the template threshold assessment in Annex 1 such processing operations will likely trigger):

- Exclusion databases (2, 4, 9);
- large-scale processing of special categories of personal data (such as disease surveillance, pharmacovigilance, central databases for law-enforcement cooperation) (1, 4, 5, 8);
- internet traffic analysis breaking encryption (data loss prevention tools) (1, 3, 8);
- e-recruitment tools automatically pre-selecting/excluding candidates without human intervention (1, 2, 8).

Annex 3

Non-exhaustive list of some common processing operations not requiring a DPIA

Indicative list of processing operations prima facie not requiring a DPIA when carried out by Union institutions, bodies, offices and agencies acting as sole or joint controllers:

- Management of personal files under Article 26 of the Staff Regulations *as such*[6];
- Standard staff evaluation procedures under the Staff Regulations (annual appraisal);
- Standard 360° evaluations for helping staff members develop training plans;
- Standard staff selection procedures;
- Establishment of rights upon entry into service;
- Management of leave, flexitime and telework;
- Standard access control systems (non-biometric)[7];
- Standard CCTV on a limited scale (no facial recognition, coverage limited to entry/exit points, only on-premises, not in public space).

[6] Some procedures resulting in adding information to the personal file may require DPIAs, but not the repository of personal files as such.

[7] E.g. badges to be swiped at entry points.