THE EDPB'S 9 CRITERIA FOR DPIAS

When is a DPIA mandatory? When processing is "likely to result in a high risk". ... Art 35(3) provides [3] examples when a processing operation is "likely to result in high risks" ... In order to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk,
*... **the following nine criteria should be considered**"*

Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)

1

EVALUATION OR SCORING

Including profiling and predicting, especially from "*aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements*".

Examples: A financial institution screens customers against a credit reference database or against an AML / CTF database. A biotech company offers genetic tests directly to consumers to assess and predict disease / health risks. A company builds behavioural or marketing profiles based on usage or navigation on its website.

ADM + LEGAL OR SIMILAR EFFECT

Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "*legal effects concerning the natural person*" or which "*similarly significantly affects the natural person*".

Examples: Processing that may lead to exclusion or discrimination against individuals.

2

3

SYSTEMATIC MONITORING

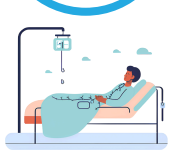
Processing to observe, monitor or control data subjects, including data collected through networks or "*a systematic monitoring of a publicly accessible area*". Data subjects may not be aware of who is collecting their data and how they will be used. May be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s): any place open to any member of the public, such as a piazza, a shopping centre, a street, a market place, a train station or a public library.

SENSITIVE OR HIGHLY PERSONAL

Includes special categories (Art 9), personal data relating to criminal convictions or offences (Art 10), and personal data increasing possible risk to individuals, 'sensitive' as commonly understood. The fact that personal data is publicly available may be a factor if it was expected to be further used for certain purposes.

Examples: A general hospital keeps patients' medical records. A private investigator keeps offenders' details. Electronic communications whose confidentiality should be protected. Location data whose collection questions the freedom of movement. Financial data that might be used for payment fraud.

4



5

LARGE SCALE

GDPR does not define 'large-scale', though recital 91 provides some guidance. The following factors, in particular, should be considered:

- the number of data subjects concerned, either as a specific number or as a proportion of the relevant population,
- the volume of data and/or the range of different data items being processed,
- the duration, or permanence, of the data processing activity, and
- the geographical extent of the processing activity.

MATCHING OR COMBINING DATASETS

Example: matching or combining datasets originating from two or more 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.

6

7

VULNERABLE DATA SUBJECTS

Processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the controller: individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights.

Examples of vulnerable data subjects: children, employees, more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, etc), and any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.

INNOVATION & NEW TECHNOLOGY

Innovative use or applying new technological or organisational solutions. Use of a new technology, defined in "*accordance with the achieved state of technological knowledge*", can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. The personal and social consequences of the deployment of a new technology may be unknown.

Examples: Combining use of finger print and face recognition for improved physical access control.Certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy.

8

9

PREVENT RIGHTS OR USE OF SERVICE

The processing in itself "*prevents data subjects from exercising a right or using a service or a contract*" (Art 22 and recital 91). Includes processing aimed at allowing, modifying or refusing data subjects' access to a service or entry into a contract.

Example: a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

Keepabl™

Subscribe to Keepabl's newsletter at keepabl.com and our YouTube channel @PricacyKitchen