THE UK ICO'S 10 CRITERIA FOR DPIAS

*'Article 35(1) says that you must do a DPIA where a type of processing is **likely to result in a high risk to the rights and freedoms of individuals** ... Article 35(3) lists three examples of types of processing that automatically requires a DPIA, and **the ICO has published a list under Article 35(4) setting out ten more**. There are also European guidelines with some criteria to help you identify other likely high risk processing.'*

UK ICO Guidance on DPIAs (our emphasis)

01 innovative technology

Processing involving the use of new technologies, or the novel application of existing technologies (including AI).

Examples: Artificial intelligence, machine learning and deep learning. Connected and autonomous vehicles. Intelligent transport systems. Smart technologies (including wearables). Market research involving neuro-measurement (i.e. emotional response analysis and brain activity). Some IoT applications, depending on the specific circumstances of the processing.

DPIA when combined with EDPB criterion

02 denial of service

Decisions about an individual's access to a product, service, opportunity or benefit that is based to any extent on automated decision-making (including profiling) or involves the processing of special category data.

Examples: Credit checks. Mortgage or insurance applications. Other pre-check processes related to contracts (i.e. smartphones).

DPIA required

03 large-scale profiling

Any profiling of individuals on a large scale.

Examples: Data processed by Smart Meters or IoT applications. Hardware/software offering fitness / lifestyle monitoring. Social-media networks. Application of AI to existing process.

DPIA required

04 biometrics

Any processing of biometric data for the purpose of uniquely identifying an individual.

Examples: Facial recognition systems. Workplace access systems/identity verification. Access control / identity verification for hardware / applications (including voice recognition / fingerprint / facial recognition).

DPIA when combined with EDPB criterion

05 genetic data

Any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the individual.

Examples: Medical diagnosis. DNA testing. Medical research.

DPIA when combined with EDPB criterion

06 data matching

Combining, comparing or matching personal data obtained from multiple sources.

Examples: Fraud prevention. Direct marketing. Monitoring personal use/uptake of statutory services or benefits. Federated identity assurance services.

DPIA required

07 invisible processing

Processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Art 14 would prove impossible or involve disproportionate effort.

Examples: List brokering. Direct marketing. Online tracking by third parties. Online advertising. Data aggregation / data aggregation platforms. Re-use of publicly available data.

DPIA when combined with EDPB criterion

08 tracking

Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.

Examples: Social networks, software applications. Hardware/software offering fitness/lifestyle/health monitoring. IoT devices, applications and platforms. Online advertising. Web and cross-device tracking. Data aggregation / data aggregation platforms. Eye tracking. Data processing at the workplace. Data processing in the context of home and remote working. Processing location data of employees. Loyalty schemes. Tracing services (tele-matching, tele-appending). Wealth profiling – identification of high net-worth individuals for the purposes of direct marketing.

DPIA when combined with EDPB criterion

09 Targeting children / vulnerable individuals

The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.

Examples: Connected toys. Social networks.

DPIA required

10 risk of physical harm

Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.

Examples: Whistleblowing/complaint procedures. Social care records.

DPIA required