Examples of processing 'likely to result in high risk'

The following list details processing operations for which the ICO requires you to complete a DPIA as they are 'likely to result in high risk'. It is based on guidelines adopted by the European Data Protection Board (EDPB) on DPIAs (WP248rev01). Our list therefore complements and further specifies these guidelines.

We have also included examples of existing areas of application for illustrative purposes. These should not be taken as definitive or exhaustive. In any event, this list is without prejudice to your overriding obligation in Article 35(1), which is to assess any proposed processing operation against the requirement to complete DPIAs. The ICO also considers it best practice to undertake a DPIA, whether or not the processing is likely to result in a high risk.

Type of processing operation(s) requiring a DPIA	Description	Non-exhaustive examples of existing areas of application
Innovative technologies	Processing involving the use of new technologies, or the novel application of existing technologies (including AI). A DPIA is required for any intended processing operation(s) involving innovative use of technologies (or applying new technological and/or organisational solutions) <u>when combined with any other criterion from WP248rev01</u>	• 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.

Denial of service	Decisions about an individual's access to a product, service, opportunity or benefit which are based to any extent on automated decision-making (including profiling) or involves the processing of special category data.	• Credit checks • Mortgage or insurance applications • Other pre-check processes related to contracts (i.e. smartphones)
Large-scale profiling	Any profiling of individuals on a large scale.	• Data processed by Smart Meters or IoT applications • Hardware/software offering fitness/lifestyle monitoring • Social media networks • Application of AI to existing process
Biometric data	Any processing of biometric data for the purpose of uniquely identifying an individual. A DPIA is required for any intended processing operation(s) involving biometric data for the purpose of uniquely identifying an individual, when combined with any other criterion from WP248rev01	• Facial recognition systems • Workplace access systems/identity verification • Access control/identity verification for hardware/applications • (including voice/fingerprint/facial recognition)
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 data subject.	• Medical diagnosis • DNA testing • Medical research

	A DPIA is required for any intended processing operation(s) involving genetic data when combined with any other criterion from WP248rev01	
Data matching	Combining, comparing or matching personal data obtained from multiple sources.	• Fraud prevention • Direct marketing • Monitoring personal use/uptake of statutory services or benefits • Federated identity assurance services
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 Article 14 would prove impossible or involve disproportionate effort (as provided by Article 14(5)(b) A DPIA is required for any intended processing operation(s) involving where the controller is relying on Article 14(5)(b) when combined with any other criterion from WP248rev01	• List brokering • Direct marketing • Online tracking by third parties • Online advertising • Data aggregation / data aggregation platforms • Re-use of publicly available data
Tracking	Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.	• Social networks, software applications, • Hardware/software offering fitness/lifestyle/health monitoring • IoT devices, applications and platforms • Online advertising • Web and cross-device tracking

	A DPIA is required for any intended processing operation involving geolocation data when combined with any other criterion from WP248rev01	• 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.
Targeting of children/other vulnerable individuals for marketing, profiling for auto decision making or the offer of online services	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.	• Connected toys • Social networks
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.	• Whistleblowing/complaint procedures • Social care records