Appendix B: Assessing for High Risk Systems

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/

Innovative technology	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) when combined with any other criterion from WP248rev01.	• 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 (Automated Decision-Making)	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 recognition/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. A DPIA is required for any intended processing operation(s) involving genetic data when combined with any other criterion from WP248rev01	● Medical diagnosis ● DNA testing ● Medical research

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	• List brokering • Direct marketing • Online tracking by third parties • Online advertising • Data aggregation/data aggregation platforms

	combined with any other criterion from WP248rev01	• 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. A DPIA is required for any intended processing operation involving geolocation data when combined with any other criterion from WP248rev01	• 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

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