information management & security

Gloucestershire COUNTY COUNCIL

Data Protection Impact Assessment (DPIA) Decision Checklist

GDPR and the Information Commissioner's Office (ICO) have set out 13 situations when completing a Data Protection Impact Assessment (DPIA) is a legal requirement.

This checklist will enable you to identify those situations when you must complete a DPIA, or alternatively when it would be best practice to do so.

If you do not recognise some of the terminology below then please refer to our guidance on GDPR.

Do I need to do a DPIA?

Situations where you MUST complete a DPIA

If you can answer 'yes' to any of the following you are **legally required** to complete a DPIA.

Type of project or processing	*Applies to my project/processing*
• **New technologies:** processing data involving the use of new technologies, or the novel application of existing technologies. This involves new developments in technology in the world at large, rather than technology that is new to us. You may be planning to use innovative or existing technology in a new way, such as: • Connected and autonomous vehicles; • Intelligent transport systems; • Smart technologies (including wearables); • Research involving neuro-measurement (e.g. emotional response analysis and brain activity); and • Internet of Things (IoT).	
• **Denial of service:** Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data. Automated decision-making is where there is no human involvement in the decision, for example it could be based on algorithms automatically applied on completion of an online questionnaire. Processing examples include: • Credit or benefit entitlement checks • Mortgage or insurance applications • Pre-check processes related to contract	

Type of project or processing	*Applies to my project/processing*
• **Large-scale profiling:** any profiling of individuals on a large scale In line with our information risk assessment large scale would be considered the profiling of more than 1,000 individuals. Profiling is where automated processing of personal data is used to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Processing examples include: • Tracking individuals using a public transport system; • Data processed by Smart Meters or IoT applications; • Hardware/software monitoring fitness or lifestyle; • Social media networks; • Application of AI to existing process.	
• **Biometrics:** any processing of biometric data Biometric data is personal data that results from processing information relating to the physical, physiological or behavioural characteristics of individuals that allows for or confirms the unique identification of a person, including fingerprint or facial recognition. Processing examples include: • Facial recognition systems; • Workplace access systems/identity verification; • Access control/identity verification for hardware/applications (including voice recognition, fingerprint and 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 Genetic data is personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question. Processing examples include: • Medical diagnosis; • DNA testing; • Medical research.	
• **Data matching:** combining, comparing or matching personal data obtained from multiple sources to identify the same entity. Processing examples include: • Detecting duplicate records in a database; • Fraud prevention; • Direct marketing; • Monitoring personal use/uptake of statutory services or benefits; • Federated identity assurance services (confirming digital identity across a range of systems (single sign on)).	

Type of project or processing	*Applies to my project/processing*
• **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 (provision of a privacy notice) would prove impossible or involve disproportionate effort Invisible processing occurs when you obtain personal data from somewhere other than directly from the individual themselves, and you don't provide them with the privacy information required by Article 14 of the GDPR. The processing is "invisible" because the individual is unaware that you are collecting and using their personal data, even if you publish a privacy notice on your website. This processing results in a risk to the individual's interests as they cannot exercise any control over your use of their data. In particular, they are unable to use their data protection rights if they are unaware of the processing. This is true even if the processing itself is unlikely to have any negative effect. You may also be at risk of breaching the fairness and transparency requirements of the first data protection principle if the processing, or any outcome from it, may not be reasonably foreseen by the individual. Processing examples include: • Direct marketing; • Online tracking by third parties; • Data aggregation; • 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 Geolocation tracking refers to the use of location technologies such as GPS or IP addresses to identify and track the whereabouts of connected electronic devices. Because these devices are often carried on an individual's person, geolocation is often used to track the movements and location of people and surveillance. Behavioural tracking is defined as the tracking of a consumer's online activities over time, including searches made, webpages visited and content viewed. Processing examples include: • 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 and data aggregation platforms; • Eye tracking; • Monitoring activity at the workplace; • Monitoring activity in the context of home and remote working; • Processing location data of employees; • Loyalty schemes; • Tracing services; • Wealth profiling.	

Type of project or processing	*Applies to my project/processing*
• **Targeting of children or other 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 Processing examples include: • Social networks/information society services (ISS); • Connected toys and gaming; • Direct marketing and online retail.	
• **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 Processing examples include: • Social care records; • Lone working procedures; • Key safe schemes; • Whistleblowing/complaints procedures.	
• **Systematic and extensive profiling with significant effects:** "any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person." European guidelines state that systematic means that the processing: • Occurs according to a system; • Is pre-arranged, organised or methodical; • Takes place as part of a general plan for data collection; or • Is carried out as part of a strategy The term 'extensive' implies that the processing also covers a large area, involves a wide range of data or affects a large number of individuals. Processing examples include: • Predicting patients' health or the likelihood of treatment being successful for a particular patient based on certain group characteristics • Online provision of insurance quotes; • Assessment of suitability for a credit card or loan.	

Type of project or processing	*Applies to my project/processing*

• **Large scale use of sensitive data:** "processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10."
In line with our information risk assessment large scale would be considered the processing of data relating to more than 1,000 individuals.
Examples include:
  • Where the council (but not an individual officer or team) is processing social care data;
  • The collection and use of equalities monitoring information, such as in SAP.	

• **Public monitoring:** "a systematic monitoring of a publicly accessible area on a large scale." This includes the procurement and use of all CCTV or surveillance camera systems, such as body worn cameras. The Surveillance Camera Commissioner requires organisations to complete DPIAs where CCTV is planned or has been implemented. For more information please see our CCTV Staffnet pages.	
• **Use of Generative Artificial Intelligence (GenAI):** using a system or machine learning application that processes personal data to perform tasks such as reorganisation and classification or to generate content such as text, audio, images or videos.	

Situations where it is best practice to complete a DPIA

There are many situations where completing a DPIA may not be a legal requirement but it would be best practice to do so. In these situations you should contact the Information Governance team for further advice.

If you can answer 'yes' to any of the following questions you should consider completing a DPIA. *Please note this list is not exhaustive.*

Type of project or processing	Should a DPIA be completed?	*Applies to my project/processing*
1. Will your project or service provision involve processing the personal data of more than 100 but less than 1,000 individuals?	You should consider completing a DPIA if you will be processing personal data about hundreds of individuals	
2. Will your project or service provision involve the regular processing of special category data, criminal offence data or data to which a duty of confidence is owed?	You should consider completing a DPIA if you will be regularly processing even small amounts of data of a highly sensitive nature; this would include any type of social care data.	

Type of project or processing	Should a DPIA be completed?	*Applies to my project/processing*
3. Will your project or service provision involve the long term or permanent processing of personal or special category data?	You should consider completing a DPIA if you intend to process personal and/or special category data over an extended period.	
4. Will the processing involve any evaluation or scoring of individuals?	You should consider completing a DPIA if the decisions will have a significant impact on the individuals. For example, if you are processing to determine whether or not an individual can receive a service or how much they should pay for that service (e.g. payments for social care) then you should complete a DPIA.	
5. Does the project involve the implementation of a system that will be used by different parts of the organisation? For example, a system used by all services in the council, or a social care system used by both Children's and Adults Social Care.	You should complete a DPIA **IF** there is a need to demonstrate how you will ensure information is not being accessed inappropriately or by the wrong services (e.g. via the use of role-based access)	
6. Will the processing involve obtaining consent from the data subject?	You should consider if a DPIA is needed in a situation where you might not allow someone to withdraw consent. If you are collecting consent purely for sending newsletters or email updates, then you will not need to complete a DPIA.	
7. Would the loss of the confidentiality, integrity or availability of the data being processed have an adverse impact on the reputation of the organisation or result in damage/distress to staff or individuals?	You should consider completing a DPIA if any associated security breach would have a negative impact on the organisation, its staff, or the individuals it provides a service to.	

Type of project or processing	Should a DPIA be completed?	*Applies to my project/processing*
8. Will the processing involve the collection of financial information and/or payment card details?	You should consider completing a DPIA if you intend to collect any sort of financial information associated with an individual. If you intend to procure a service that collects financial information on the council's behalf, the successful provider must have PCI DSS accreditation or be able to demonstrate equivalency. For more information please visit our Contracts, Procurements and Projects Staffnet page.	
9. Will you or your potential service provider being using any AI applications, such as a transcribing service or forecasting software?	Any use of AI is considered new technology, and a DPIA should be considered if there is potential that this could capture personal data. For example, a transcription application could process the personal information of other attendees at the meeting being transcribed, or the personal data of any subjects of conversation.	