**NHS DORSET**

Guidance on Completing a Data Protection Impact Assessment

# introduction

## The GDPR introduces a new obligation to complete a Data Protection Impact Assessment (DPIA) before carrying out types of processing of personal information likely to result in high risk to individuals’ interests.

## NHS Clinical Commissioning Group (CCG) has encouraged staff to complete privacy impact assessments (PIAs) for a number of years. A PIA is a good practice measure to identify and minimise privacy risks associated with new projects. DPIAs are very similar to PIAs. The DPIA simply replaces the PIA process to ensure compliance with General Data Protection Regulation (GDPR) requirements for content and process.

## DPIAs are now a mandatory requirement in some cases.

# what is a dpia?

## A DPIA is a way of analysing any processing of personal identifiable data to help identify and minimise data protection risks at an early stage.

## A DPIA looks at compliance risks, and also risks to the rights and freedoms of individuals. The focus is on the potential for harm, both to individuals and to society, whether it is physical, material or non-material. The DPIA assesses the level of risk by considering both the likelihood and the severity of any impact on individuals.

## The outcomes of a DPIA should be integrated back into the project plan. A DPIA is not just a one-off exercise, it should be a living document that is kept under review and assessed if anything changes.

## DPIAs are a legal requirement for any processing that is likely to be high risk

# when should a DPIA be completed?

## A DPIA should be done right at the start of any new project or change to an existing service, before beginning any type of processing which is likely to result in a high risk. The DPIA should run alongside the planning and development process of the project.

## Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for **any major new project involving the use of personal data**.

## GDPR requires a DPIA to be done if you plan to:

### use systematic and extensive profiling with significant effects;

### **large scale processing of special category\*** **or criminal offence** **data** - this includes health records processed by hospitals / health clinics, and social care records; or,

### systematically monitor publicly accessible places on a large scale – this includes **audio/video surveillance of public areas**.

**\* Special category data**

This is more sensitive personal data and so needs more protection. It includes information about an individual’s:

* race;
* ethnic origin;
* politics;
* religion;
* trade union membership;
* genetics;
* biometrics (where used for ID purposes);
* health;
* sex life; or
* sexual orientation.

## The Information Commissioner’s Office (ICO) also lists a further ten types of processing that automatically require a DPIA:

### **New technologies**: processing involving the use of new technologies such as smart technologies, or a different application of existing technologies (including AI).

### **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 e.g. credit checks.

### **Large-scale profiling**: any profiling of individuals on a large scale e.g. hardware / software offering fitness / lifestyle monitoring, social media networks, or application of AI to existing process.

### **Biometrics**: any processing of biometric data e.g. access control / identity verification for hardware / applications (including voice recognition, fingerprint or 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.

### **Data matching**: combining, comparing or matching personal data obtained from multiple sources e.g. fraud prevention, or monitoring personal use / uptake of statutory services or benefits, or direct marketing.

### **Invisible processing**: processing of personal data that has collected from a source other than directly from the individual, without providing them with a privacy notice.

### **Tracking**: processing which involves tracking an individual’s geolocation or behaviour, including but not limited to the online environment e.g. social networks, software applications, hardware / software offering fitness / lifestyle / health monitoring, data processing at the workplace, data processing in the context of home and remote working.

### **Targeting of children or other vulnerable individuals**: the use of children’s personal data or personal data from other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children such as 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 e.g. social care records, or whistleblowing/complaint procedures.

## The ICO also suggests that a DPIA should be done for **any** **other** processing that:

### is large scale;

### involves profiling or monitoring;

### **decides on access to services** or opportunities; or,

### **involves sensitive data** **or vulnerable individuals**.

## If in doubt, the recommendation is to carry out a DPIA.

## **If you are looking to process personal information and decide not to carry out a DPIA, you must document your reasons and seek approval from the DSP Group**.

# completing the DPIA form

## **Step 1 – Identify the need for a DPIA**

## If you are not sure whether or not you need to do a DPIA, ask the Data Security and Protection (DSP) team or the Data Protection Officer (DPO) for advice. If you are in any doubt, advice from the ICO is that you should complete a DPIA.

## Carry out a screening exercise using the DPIA screening checklist suggested by the ICO which can be found at the end of this document (Appendix A), alongside the notes contained in Section 3 of this guidance.

## If, following the screening exercise, you decide that you do not need to do a DPIA, you **must** document your decision and the reasons for it (including the advice from the DPO / DSP team) by keeping an annotated copy of the screening checklist.

## **Step 2 – Describe the processing**

## **The nature of the processing**

## You should state in this section what you plan to do with the personal data, including:

### how you collect the data;

### how you store the data;

### how you use the data;

### who has access to the data;

### who you share the data with;

### whether you use any data processors;

### retention periods;

### security measures;

### whether you are using any new technologies;

### whether you are using any new types of processing; and

### which screening criteria you flagged as likely high risk.

## **The scope of the processing**

## This is where you document what the processing covers, including:

### what is the personal data you are collecting;

### the volume and variety of the personal data;

### the sensitivity of the personal data;

### the extent and frequency of the processing;

### the duration of the processing;

### the number of data subjects involved; and

### the geographical area covered.

## **The context of the processing**

## This is where you should describe the wider picture and incorporate internal and external factors which might affect expectations or impact, including:

### the source of the data;

### the nature of your relationship with the individuals;

### the extent to which individuals have control over their data;

### the extent to which individuals are likely to expect the processing;

### whether they include children or other vulnerable people;

### any previous experience of this type of processing;

### any relevant advances in technology or security;

### any current issues of public concern; and

### whether you comply with any GDPR codes of conduct or GDPR certification schemes;

### whether you have considered and complied with relevant codes of practice.

## **The purposes of the processing**

## This is where you document the reason why you want to process the personal data, and should include:

### the intended outcome for individuals;

### the expected benefits for the CCG or for society as a whole; and

### the legitimate interests of the CCG, where relevant (you may need to consult the DPO to identify whether there is a legitimate interest).

## **Step 3 – Consultation process**

## This section of the DPIA form allows you to set out the consultation process you have used to seek the views of individuals or their representatives.

## Generally, you should be able to consult individuals in some form. However, if you decide that it is not appropriate to consult individuals, then this decision should be recorded as part of the DPIA, along with a clear explanation. For example, you might be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.

## If the DPIA covers the processing of personal data of existing patients, service users or employees, you should design a consultation process to gather the views of those particular individuals or their representatives.

## If the DPIA covers a plan to collect the personal data of individuals you have not yet identified, you may need to carry out a more general public consultation process, or targeted research. This could take the form of carrying out market research with a certain demographic, or contacting relevant campaign or consumer groups for their views.

## If your DPIA decision is not the same as the views of individuals, you must document your reasons for disregarding their views.

## If you use a data processor, you may need to ask them for information and assistance.

## You should consult all relevant internal stakeholders, in particular anyone with responsibility for information security.

## In some circumstances, you may need to seek legal advice or advice from other independent experts.

## **Step 4 – Assess necessity and proportionality**

## This section of the DPIA is where you need to consider whether your plans are actually necessary i.e. do they help to achieve your purpose, or is there any other reasonable way to achieve the same result.

## You also need to look at how you will ensure data protection compliance, which is a good measure of necessity and proportionality. To do this, you should document:

### your lawful basis\*\* for the processing i.e. the legal basis for processing the data in order to comply with the Data Protection Act 2018;

### how you will prevent function creep i.e. how you will stop the scope of the project growing beyond the purpose for which it was originally intended;

### how you intend to ensure data quality;

### how you intend to ensure data minimisation i.e. ensure that data collected and processed is not held or further used unless this is essential for reasons that are clearly stated in advance to support data privacy;

### how you intend to provide privacy information (privacy notice) to individuals;

### how you implement and support individuals rights;

### measures to ensure your processors comply; and

### safeguards for international transfers where applicable.

**\*\* Lawful basis for processing**

You must have a valid lawful basis in order to process personal data. There are six available lawful bases for processing:

1. **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose.
2. **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).
4. **Vital interests**: the processing is necessary to protect someone’s life.
5. **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (**This cannot apply if you are a public authority processing data to perform your official tasks**.)

When processing **special category data**, you must apply **a further condition** to demonstrate lawful processing; the DSP team can help you identify this.

## **Step 5 – Identify and assess risks**

## In this section you need to consider the potential impact on individuals and any harm or damage that might be caused by your processing – whether physical, emotional or material. Also look at whether the processing could possibly contribute to:

### inability to exercise rights (including but not limited to privacy rights);

### inability to access services or opportunities;

### loss of control over the use of personal data;

### discrimination;

### identity theft or fraud;

### financial loss;

### reputational damage;

### physical harm;

### loss of confidentiality;

### re-identification of pseudonymised data; or

### any other significant economic or social disadvantage.

## You should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data).

## To assess whether the risk is a high risk, you need to consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk.

## You must make an ‘objective assessment’ of the risks – further information on risk assessment can be found in the CCG’s Risk Management Framework. It is worth considering corporate risks as well, such as the impact of regulatory action, reputational damage or loss of public trust.

## **Step 6 – Identify measures to reduce risk**

## Against each risk identified, record the source of that risk and then consider options for reducing the risk. This might include:

### deciding not to collect certain types of data;

### reducing the scope of the processing;

### reducing retention periods;

### taking additional technological security measures;

### training staff to ensure risks are anticipated and managed;

### anonymising or pseudonymising data where possible;

### writing internal guidance or processes to avoid risks;

### using a different technology;

### putting clear data sharing agreements into place;

### making changes to privacy notices;

### offering individuals the chance to opt out where appropriate; or

### implementing new systems to help individuals to exercise their rights.

## The above list is not an exhaustive list, and there may be other ways to help reduce or avoid the risks.

## You should also record whether the measure would reduce or eliminate the risk. You can take into account the costs and benefits of each measure when deciding whether or not they are appropriate.

## **Step 7 – Sign off and record outcomes**

## The final step in completing your DPIA is to record:

### what additional measures you plan to take;

### whether each risk has been eliminated, reduced, or accepted;

### the overall level of ‘residual risk’ after taking additional measures; and

### whether you need to consult the ICO.

## You do not always have to eliminate every risk. You may decide that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of mitigation. This would need to be approved by the DSP Group. However, if there is still a high risk, you need to consult the ICO before you can go ahead with the processing. The DSP team and the DPO will make contact with the ICO when required.

## As part of the sign-off process, you should ask the DPO to advise on whether the processing is compliant and can go ahead. If you decide not to follow DPO advice, you need to record your reasons. You should also record any reasons for going against the views of individuals or other consultees.

# oversight and ongoing monitoring of the DPIA

## Final scrutiny of the DPIA will be made by the DSP Group who will review every DPIA and Screening Exercise.

## The outcomes of the DPIA should be integrated back into your project plans. You should identify any action points and who is responsible for implementing them. You can use the usual project management process to ensure these are followed through.

## You should monitor the ongoing performance of the DPIA. You may need to cycle through the process again before your plans are finalised.

## If you have decided to accept a high risk, either because it is not possible to mitigate or because the costs of mitigation are too high, you need to consult the ICO before you can go ahead with the processing (see Section 6).

## The DSP team will publish all DPIAs on the CCG Website. If there is concern that publication might reveal commercially sensitive information, undermine security or cause other risks, consideration will be given to redacting or removing sensitive details, or publishing a summary.

## You need to keep your DPIA under review, and you may need to repeat it if there is a substantial change to the nature, scope, context or purposes of your processing.

# consulting the ICo

## If you have carried out a DPIA that identifies a high risk, and you cannot take any measures to reduce this risk, you need to consult the ICO. You cannot go ahead with the processing until you have done so. Contact with the ICO will be made by the DSP team.

## The focus is on the ‘residual risk’ after any mitigating measures have been taken. If your DPIA identified a high risk, but you have taken measures to reduce this risk so that it is no longer a high risk, you do not need to consult the ICO.

## Please note: the ICO will screen your DPIA to confirm that it does identify a high risk that has not been mitigated, and will confirm whether your DPIA has been accepted for consultation within ten days of sending it to them.

## The ICO will review the DPIA and consider whether:

### the processing complies with data protection requirements;

### risks have been properly identified; and

### risks have been reduced to an acceptable level.

## In most cases the ICO will get back to you within eight weeks. In complex cases this may be extended to a maximum of 14 weeks.

## If the intended processing operation would impact on data subjects in EU member states, the ICO may be required to co-operate with other data protection authorities before providing written advice. Where this occurs, it may mean that the case cannot be resolved in 14 weeks. The ICO will notify the CCG if this occurs and keep us updated.

## Further information on DPIAs can be found in the [ICO Guidance](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/).

## Appendix A

## **DPIA SCREENING CHECKLIST**

We always carry out a DPIA if we plan to:

☐ Use systematic and extensive profiling or automated decision-making to make significant decisions about people

☐ Process special category data or criminal offence data on a large scale

☐ Systematically monitor a publicly accessible place on a large scale

☐ Use new technologies

☐ Use profiling, automated decision-making or special category data to help make decisions on someone’s access to a service, opportunity or benefit

☐ Carry out profiling on a large scale

☐ Process biometric or genetic data

☐ Combine, compare or match data from multiple sources.

☐ Process personal data without providing a privacy notice directly to the individual

☐ Process personal data in a way which involves tracking individuals’ online or offline location or behaviour

☐ Process children’s personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them

☐ Process personal data which could result in a risk of physical harm in the event of a security breach

We consider whether to do a DPIA if we plan to carry out any other:

☐ Evaluation or scoring

☐ Automated decision-making with significant effects

☐ Systematic

☐ Processing of sensitive data or data of a highly personal nature.

☐ Processing on a large scale.

☐ Processing of data concerning vulnerable data subjects.

☐ Innovative technological or organisational solutions

☐ Processing involving preventing data subjects from exercising a right or using a service or contract.

We consider carrying out a DPIA in any major project involving the use of personal data.

If we decide not to do a DPIA, we document the reasons and **advise the DSP Group**.

We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

We have taken advice from our Data Protection Officer or Data Security and Protection team. **The advice is documented on the other side of this checklist**. **→**