

Data Protection Impact Assessment (DPIA) Workbook

We are required by data protection law to complete a risk assessment of a project which may involve the processing of Personal Data, both defined in the GDPR as:

“Personal data’ which means any information relating to an identified or identifiable natural person (a ‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.

“Processing” which means any operations performed on personal data (whether those operations are automated or not). Common types of personal data processing include (but are not limited to) collecting, recording, organising, structuring, storing, modifying, consulting, using, publishing, combining, erasing, and destroying data.

The “project” is defined in this DPIA as any activity involving the possible processing of personal data including the implementation of a new system or a new supplier or the review of existing systems/suppliers.

Under Article 35 of the General Data Protection Regulation 2016 (the GDPR) requires Data Protection Impact Assessment (DPIA) to be undertaken where there is a;

‘high risks to the rights and freedoms of natural persons resulting from the processing of their personal data’.

The GDPR identifies a number of situations where processing personal data could be considered high risk and where a DPIA is a legal requirement, including:

- a) profiling and automated decision making
- b) systematic monitoring
- c) the use of special categories of personal data including sensitive data (health and social care)
- d) data processed on a large scale
- e) data sets that have been matched or combined
- f) data concerning vulnerable data subjects (includes processing where the Controller could be seen to demonstrate an imbalance of power over the data subject e.g. Employer and Employee)
- g) technological or organisational solutions
- h) data transfer outside of the EU and
- i) processing which limits the exercising of the rights of the data subject

A DPIA is designed to describe the processing, assess the necessity and proportionality of the processing and to help manage the risks to data subjects. DPIAs are also important tools for demonstrating accountability, as they help controllers to comply with the requirements of the GDPR. Under the GDPR, non-compliance with DPIA requirements can lead to fines imposed by the Information Commissioners Office (ICO); this includes not carrying out a DPIA, carrying out a DPIA in an incorrect way or failing to consult the ICO where required.

For further information on DPIAs you should refer to the [DPIA Guidance](#) and [DPIA SOP](#) found on Connect or by clicking here.

The IG Team should be consulted before completing a DPIA in order to provide specialist advice and guidance.

After completion, please submit the DPIA to InformationGovernance@UHBW.nhs.uk.

**Please answer all questions up until 4.9.
If any questions are not applicable please confirm this by stating N/A as your answer.**

PLEASE NOTE: This DPIA will be disclosed if requested under the Freedom of Information Act (2000). If there are any exemptions that should be considered to prevent disclosure they should be detailed here:

DPIA

Background Information			
Project Name: For example; the name of the new system/supplier/activity.		Date of DPIA submission to the Information Governance Team: **Note: a DPIA can take several months to complete and approve depending on the nature of the project**	
Project Lead Name: Note: It is the responsibility of the Project Lead to complete this DPIA with the Information Asset Owner/Information Asset Administrator.		Project Lead Contact Details:	
Sponsor E.g. Project Board.		Lead Organisation:	
Name of individual submitting this DPIA and Key contact:			
When was the UHBW Data Protection Officer sent this DPIA for review? dd/mm/yyyy			
Brief description of of the project::		Duration of project/contract term:	
Background: What is the purpose of the project?			
Name any other organisation, including system suppliers, who are involved in the delivery of the project:			
Other Key Stakeholders and consultees (both internal and external):			
Does the DPIA link to any procurement activity For example, have we received a contract from a new supplier?	What stage of the procurement are you at? For example, are we at tender stage, getting budget approval, or reviewing the new prospective Supplier's contract etc?		
Has anything similar been undertaken before? If yes please detail:			

The screening questions must be completed for every project/proposal that is new or a change to the way personal information is processed, a “Y” to any of these questions indicates the full DPIA is required.

Screening questions

Will the processing involve a large amount of personal data and affect a large number of data subjects?	
Will the project involve the use of new technologies	
Is there the risk that the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy (e.g. health records), unauthorised reversal of pseudonymisation ¹ , or any other significant economic or social disadvantage?	
Is there the risk that data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data?	
Will there be processing of genetic data, data concerning health or data concerning sex life?	
Are the data to be processed revealing <u>racial or ethnic origin</u> , political opinions, religion or philosophical beliefs, or trade union membership? (Ethnicity – if recorded in the patient’s notes)	
Will there be processing of data concerning criminal convictions and offences or related security measures?	
Will personal data of vulnerable natural persons, in particular of children, be processed?	
Will personal aspects be evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles?	
Will the project include a 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 (e.g. a recruitment aptitude test which uses pre-programmed algorithms and criteria)?	
Will there be a systematic monitoring of a publicly accessible area on a large scale (e.g. CCTV)?	
Will any personal data be transferred outside of the European Economic Area (EEA)?	

Information/Data – Categories / Legal basis / Collection / Flows / Responsibility

1.1
What category/ies of data/information will be used as part of this proposed activity?
(indicate all that apply)

	Y/N	YES?	NO?
Personal Data		Complete DPIA	Confirm with IG if a DPIA is required.
Special Categories of Personal Data		Complete DPIA	
Pseudonymised Personal Data		Complete DPIA	
Personal Confidential Data		Complete DPIA	
Criminal Convictions and Offence Data		Complete DPIA	
Anonymised Personal Data		Complete DPIA. IG to consider at what point data is anonymised.	
Commercially Confidential Information		Confirm with IG if a DPIA is required.	
Other (please detail)		Confirm with IG if a DPIA is required.	

¹ 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

1.2 What legal basis are you proposing to rely upon to process any Personal Data?	
<p>Under Article 6 of the GDPR there are six lawful bases for processing personal data.</p> <p>Please indicate which legal basis applies to the project?</p> <p>Note: There may be more than one legal basis.</p>	Y/N
1. CONSENT - The Data Subject has given explicit consent See ICO guidance here. If Yes please complete section 1.3 to 1.5 below.	
2. CONTRACT - It is necessary for the performance of a contract to which the data subject is party See ICO guidance here. If Yes please complete 1.6 below.	
3. LEGAL OBLIGATION - It is necessary under a legal obligation to which the Controller is subject See ICO guidance here. If Yes please complete 1.7 below.	
4. VITAL INTERESTS -It is necessary to protect the vital interests of the data subject or another natural person. See ICO Guidance here. If Yes please complete 1.8 below	
5. PUBLIC TASK - It is necessary for the performance of a task carried out in the public interest or under official authority vested in the Controller. See ICO guidance here. If Yes please complete 1.9 below.	
6. LEGITIMATE INTEREST - It is necessary for the legitimate interests of the Controller or third party (can only be used in extremely limited circumstances by Public Authorities and must not be used for the performance of the public tasks for which the authority is obligated to do). See ICO guidance here. If Yes please complete 1.10 below.	
COMPLETE 1.3 – 1.5 IF RELYING ON LEGAL BASIS 1. See ICO guidance here.	
1.3 Why are you relying on explicit consent from the data subject?	
1.4 What is the process for obtaining and recording consent from the Data Subject? You should send with this DPIA a copy of the consent form you intend to use.	
1.5 How do the proposed consent statements comply with consent requirements under data protection law such as the right to withdraw consent? See 'Valid consent' guidance on the ICO website and how to record, obtain and manage consent.	
COMPLETE 1.6 IF RELYING ON LEGAL BASIS 2. See ICO guidance here.	
1.6 What contract is being referred to?	
COMPLETE 1.7 IF RELYING ON LEGAL BASIS 3. See ICO Guidance here.	
1.7 Identify the legislation or legal obligation relied upon for processing	

COMPLETE 1.8 IF RELYING ON 4. [See ICO Guidance here.](#)

1.8 How will you protect the vital interests of the data subject or another natural person?

COMPLETE 1.9 IF RELYING ON 5. [See ICO guidance here.](#)

1.9 What statutory power or duty does the Controller derive their official authority from?

COMPLETE 1.10 IF RELYING ON LEGAL BASIS 6. [See ICO guidance here.](#)

1.10 What is the legitimate interest relied upon?

1.11
If using special categories of personal data (such as health data), a condition for processing personal data under Article 9 of the GDPR must be satisfied in addition to a condition under Article 6.

Article 9 conditions are as follows:	Y/N
The Data Subject has given explicit consent	
For the purposes of employment, social security or social protection	
It is necessary to protect the vital interests of the data subject or another natural person where they are physically or legally incapable of giving consent	
It is necessary for the operations of a not-for-profit organisation such as political, philosophical, trade union and religious body in relation to its members	
The data has been made public by the data subject	
For legal claims or courts operating in their judicial category	
Substantial public interest. See ICO guidance here.	
Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards.	
Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health <u>or ensuring high standards of quality and safety of health care</u> and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy	

1.12
Is the data, subject to a duty of confidentiality (e.g. clinical records, OH details, payroll information)? If so, please specify them.

1.13
If the processing is of data concerning health or social care, is it for a purpose other than direct care?

1.14
What is the scale of the processing (i.e. (approximately) how many people will be the subject of the processing)?

1.15
How is the data/information being collected?
 E.g. verbal, electronic, paper etc.

1.16
If required, how is the data/information to be edited/updated?

--

1.17
How is the data/information to be quality checked?

1.18
What business continuity or contingency plans are in place with the Supplier to protect the data/information?
 For details on UHBW business contingency plan, please discuss with the Business Resilience Team.

1.19
If required, what training is planned to support this activity?

1.20
Who will be the data controller/s and who will be the data processor(s)?
 Where applicable, state at which point parties become data controllers/whether they are joint controllers.

1.21
Confirm all the applicable agreements and all the parties to the contracts involved in the Project?

1.22
Who is the Information Asset Manager?
Who is the Information Asset Administrator? This individual is responsible for managing the data agreement and ensuring the processing is in accordance with the agreed terms. Please confirm they have received a copy of the data agreement.

Information/Data – Linkage / Sharing / Flows / Agreements / Reports

2.1
Please detail any proposals to link data sets in order to achieve the project
 Please detail the data sets and linkages.

2.2
What are the Data Flows?
 Please attach a data flow diagram and include a step-by-step numbered guide, clearly explaining and setting out, when personal data is to be exchanged, with whom and the method used to share the data.

2.3
The Personal Data to be shared: What data/information is being shared?
 For example, patient data/employee data? Will this be their date of birth, T number, clinical diagnosis, results etc?

2.4 What data agreements are or will be in place to support this processing?

- **If we are engaging with data controller(s) have they satisfied the ICO data controller checklist ([available here](#))?**

- If we are engaging with a data controller is there or will there be a data sharing agreement in place?
- If there is a Data Processing Agreement in place does the agreement contain all the legally required clauses? [See ICO guidance here.](#)

Security – Where applicable, please consult with UHBW Cyber Security

3.1
Are you proposing to use a third party/processor/system supplier as part of the project?
If applicable, please name them here.

3.2
What security measures has the third party/processor/system supplier put in place in order to meet the necessary requirements under the GDPR?
See GDPR security principle: 'Data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'.

3.3
Is the third party/processor/system supplier registered with the Information Commissioner? If so, please provide their ICO registration number.

3.4
Provide details of the Data Security & Protection Toolkit compliance level of the third party/processor/system supplier?

3.5
How will the data/information be stored?
Include details on back-ups and copies.

3.6
How is the data/information accessed and how will user access be controlled and monitored depending on role?

3.7
Is the use of Cloud technology being considered either by your own organisation or a 3rd party supplier?

3.8
What security measures will be in place to protect the data/information
E.g. physical, electronic etc.

3.9
Are you transferring any data outside of the European Economic Area (EEA)?
If so, is there an adequacy agreement in place?

3.10
Does the contract with the third party/processor/system supplier contain all the necessary IG clauses?
For example, do the terms and conditions /contract/tender submission contain the adequate data protection provisions.

Individual Rights – Notification / Retention / Access / Erasure / Rectification / Portability

4.1

If required, what changes are proposed to the [UHBW Privacy Notice](#)?

4.2

If applicable, does the contract require data processors to immediately report and assist the data controller with any subject access requests?

4.3

If applicable, please detail how this data will be made portable if requested by the data subject. [Please see ICO guidance.](#)

4.4

If applicable, please detail how data subjects will be able to request the erasure of the data being processed. [Please see ICO guidance.](#)

4.5

How long is the data/information to be retained? For example, what is the term of the data processing/sharing agreement. [See Trust Records Management and Retention policy here.](#)

4.6

How will the data/information be archived/what is the process for the destruction of records? [Please see ICO guidance here.](#)

4.7

When applicable, how will it be possible to restrict the processing of personal data about a particular individual should this become necessary? [Please see ICO guidance here.](#)

4.8

Will any personal data be processed for direct marketing purposes? If yes please detail [referring to the ICO Direct Marketing checklist here.](#)

4.9

Will the processing result in a decision being made about the data subject solely on the basis of automated processing (including profiling)? If yes, please describe the logic involved in any automated decision-making.

Risk Management (For Information Governance, Risk and SIRO only)

5.1
 What risk and issues have you identified? (See the [Simple Guide to Risk Assessment and Management on Connect](#))

Severity → ↓ Likelihood	1 - Negligible	2 - Minor	3 - Moderate	4 - Major	5 - Catastrophic
5 - Very Likely	5	10	15	20	25
4 - Likely	4	8	12	16	20
3 - Possible	3	6	9	12	15
2 - Unlikely	2	4	6	8	10
1 - Rare	1	2	3	4	5

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood	Impact	Overall risk
	Rare - 1 Unlikely - 2 Possible - 3 Likely - 4 Very Likely - 5	Negligible - 1 Minor - 2 Moderate - 3 Major - 4 Catastrophic - 5	Low Medium High Very High

5.2
 Identify additional measures you could take to reduce or eliminate risks identified as medium, high or very high above:

Risk	Options to reduce or eliminate risk	Effect on risk	risk	Measure approved
		Eliminated, reduced or accepted	Low, medium or high	Yes/no

5.3
 Are there any known activities that will have a direct effect on this piece of work?

5.4
 Any further comments to accompany this DPIA for consideration?

Consultation

6.1
 Will any other stakeholder(s) (whether internal or external) need to be consulted about the proposed processing?

6.2
 What was/were the outcome(s) of such consultation?

6.3
 Will you need to discuss the DPIA or the processing with the Information Commissioners Office? (Are there any unmitigated high risks?)

Specialist Team Review

7.1 IG Team Comments / Observations / Specific issues	
7.2 Digital Risk Comments / Observations / Specific issues	
7.3 [Other Team 1] Comments / Observations / Specific issues	
7.4 [Other Team 2] Comments / Observations / Specific issues	

Data Protection Officer comments and observations

8.1 Comments / Observations / Specific issues	
--	--

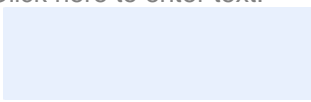
Sign Off Process

Where the mitigated risk is low or medium:

Signed and approved on behalf of **UHBW Data Protection Officer:**

Name: [Click here to enter text.](#)

Job Title: [Click here to enter text.](#)

Signature:  Date: [Click here to enter a date.](#)

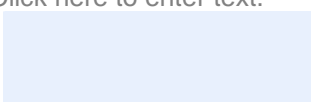
Where the mitigated risk is high:

Signed by the **UHBW Data Protection Officer and Chair of Information Risk Management Group:**

Meeting Date: [Click here to enter a date.](#) Minute Reference: [Click here to enter text.](#)

Name: [Click here to enter text.](#)

Job Title: [Click here to enter text.](#)

Signature:  Date: [Click here to enter a date.](#)

Where the mitigated risk(s) is very high:

DPIA sent to the ICO: [Click here to enter a date.](#)

Response received from the ICO: [Click here to enter a date.](#)

Summary of ICO decision: [Click here to enter text.](#)