DATA PROTECTION IMPACT ASSESSMENTS

POLICY AND GUIDANCE

Owner	Benjamin Watts
Date	12 November 2019
Version Number	1.6
Date for Review	12 November 2020

Contents

Introduction

This Policy and Guidance is intended to help Kent County Council (KCC) staff to understand what their roles and responsibilities are to carry out meaningful Data Protection Impact Assessments (DPIAs).

DPIAs are a tool that can help Kent County Council assess the impact of data processing activities on the protection of personal data and identify the most effective way of complying with its data protection obligations. An effective DPIA will allow KCC to identify and fix problems at an early stage, reducing the associated costs and damage to reputation that might otherwise occur. DPIAs are an integral part of "data protection by design" activity which can help KCC demonstrate its compliance and accountability obligations under data protection law.

Since 25 May 2018 conducting DPIAs has been mandatory in certain circumstances and this guidance will help you to determine when a DPIA must or should be carried out. It will be a key part of KCC's evidence that it is complying with obligations under the GDPR, including demonstrating that privacy was an important consideration when processing operations are being designed.

Non-compliance with DPIA requirements can lead to significant fines being imposed by the Information Commissioner's Office.

Information Commissioner's Guidance

The Information Commissioner's Office has produced detailed Guidance for conducting a DPIA, which replaces the previous Code of Practice on conducting privacy impact assessments. Any staff carrying out a DPIA is advised to follow the ICO's Guidance and refer to it for more detailed information and guidance. The ICO's DPIA Guidance can be found by clicking here.

What is a DPIA?

A DPIA is a process which is designed to help you to systematically identify and minimise any data protection risks in relation to any proposed data processing. It will help you to look at the objective of any project where you plan to process personal data, what the benefits to KCC and to data subjects are, to identify any data protection risks, and whether they can be mitigated and minimised, compliance risks and ultimately whether or not the level of risk is justified in the circumstances. DPIAs are an integral part of 'data protection by design', another general legal obligation under GDPR, which is an approach that ensures privacy and data protection issues are considered at the early design stages of any system, product, service, or business practice, and then throughout its lifecycle.

DPIAs are a legal requirement and must be carried out where the data processing is likely to result in a high risk to the rights and freedoms of individuals. This is an essential part of demonstrating compliance with KCC's accountability obligations under GDPR.

For more information on 'data protection by design and default', please see the ICO's guidance here.

When you need to carry out a DPIA

You must carry out a DPIA for any type of data processing which is '***likely to result in a high risk to the rights and freedoms of individuals'***.

The term 'risk' in this context is about risk to individuals' interests and risks to their rights and freedoms, which includes risks to privacy and data protection rights and effects on other fundamental rights and interests (e.g. freedom of speech, prohibition of discrimination, etc.). A DPIA should therefore look at the risks from the data subject's perspective. GDPR states:

> *"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where 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, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data….."*

When assessing risk, and whether it is **high** risk, you will need to look at the likelihood and the severity of any potential harm to individuals. Something might be considered high risk because the potential harm is more likely, or the potential harm is more severe, or both.

When looking at the question of whether the processing is **likely** to result in high risk, you need to consider whether the proposed processing has any features which indicate a potential for high risk. If there are features which indicate a potential for high risk, then a DPIA will need to be carried out which will then analyse the risks and the likelihood and severity of any potential harm.

When you must carry out a DPIA

GDPR sets out three types of processing that automatically require you to carry out a DPIA. These are where you plan to:

- carry out any systematic and extensive profiling, on which decisions are based, which has legal effects or significantly affect individuals.

- Process special category data or personal data relating to criminal convictions or offences on a large scale.

- Systematically monitor publicly accessible areas on a large scale, e.g. (CCTV)

  Note: *Officers completing a DPIA for CCTV and/or surveillance systems should complete sections 2, 11 and 12 of the DPIA template at Appendix 3 of this Policy only* ***and*** *must also complete and attach the template DPIA on the Surveillance Camera Commissioner's website as found here, sending* ***both*** *DPIAs to the DPO for advice (dpo@kent.gov.uk).*

  A toolkit and further guidance is also available on the Surveillance Commissioner's website. These should be reviewed, and the Surveillance Commissioner's Code of Practice self-assessment tool completed, as evidence of KCC's compliance and added as an appendix to the Surveillance Commissioner's completed template DPIA. You must also read and comply with KCC's Code of Practice and Policy for the Operation of KCC CCTV and Overt Surveillance Systems, available on KNET.

Other criteria which may indicate a likely high risk

Guidelines have also been published by the Article 29 Working Party ("the European Guidelines") with criteria which may indicate likely high risk. These are:

- Evaluation or scoring: profiling and predicting behaviours. For example, screening customers against a credit reference database.

- Automated decision-making with legal or similar significant effect: for example, profiling which may lead to the exclusion of, or discrimination against, individuals.

- Systematic monitoring: for example, an employee monitoring program. The risk is increased where:

  - The individual may not be aware who is collecting their data or how it will be used; or

  - It is difficult for the individual to avoid being subject to such processing if the monitoring is in a public space.

- Sensitive data or data of a highly personal nature: the processing of sensitive personal data including special categories of data as defined in Article 9 GDPR or data which more generally increases risks for individuals or impacts exercise of a fundamental right, such as location data or financial data. Article

9 defines special category data as data which relates to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health, sex life or sexual orientation. You should also consider personal data relating to criminal allegations, proceedings or convictions to fall within this criteria.

- Data processed on a large scale: the number of individuals concerned, the volume or range of different data items, the duration of the processing and its geographical extent are all potential components of this risk factor.

- Matching or combining datasets: where the datasets originate from different processing operations and data subjects could not reasonably expect them to be combined.

- Data concerning vulnerable data subjects: in cases where there is an imbalance in the relationship between the data controller and the data subject, meaning they may not be able to easily consent to or oppose the processing of their personal data. Vulnerable individuals may include children, individuals with mental or physical impairments, patients or the elderly. **Note that employees also fall within the definition of vulnerable data subject in this context because of the imbalance in the relationship between employer and employee.**

- Innovative use of technological or organisational solutions: the use of new technologies with novel forms of data collection and use.

- The processing prevents an individual from exercising a right or using a service or contract: including processing aimed at allowing, modifying or refusing individuals access to a service or entry into a contract. For example, a bank screens customers against a credit reference database to decide whether to offer a loan.

If at least 2 of the above criteria are met, this will be an indicator that a DPIA is required and you will need to carry out one.

However, a DPIA may still be required even if the processing meets only one of the above criteria where it is enough to pose a likely high risk of harm to the rights and freedoms of individuals. You should seek advice from the DPO in this regard.

The list above is not exhaustive. If there are other processing operations that may pose similar high risks, a DPIA should be conducted.

<u>What the ICO considers likely to result in high risk</u>

The ICO has published a list of processing operations which also requires a DPIA, which complements and adds to the criteria set out in the European Guidelines above. Some of the specified operations automatically require a DPIA, and some

only when in combination with one of the other items, or any of the European Guidelines criteria:

- Innovative technologies (use of innovative technology or the novel application of existing technologies (including AI)) – A DPIA is required when combined with any of the criteria from the European Guidelines
- Denial of a service (decisions about access to a service, product or opportunity based on automated decision-making (including profiling) or involves special category data) – A DPIA is required
- Profile individuals on a large scale – a DPIA is required
- Process biometric data – A DPIA is required when combined with any of the criteria from the European Guidelines
- Process genetic data (other than by an individual GP or health professional for provision of health care to the data subject) – A DPIA is required when combined with any of the criteria from the European Guidelines
- Data matching (combining, comparing or matching personal data obtained from multiple sources) – A DPIA is required.
- Invisible processing (obtaining personal data from a source other than the individual without providing them with a privacy notice, if it is considered that do so would prove impossible or involve disproportionate effort) – A DPIA is required when combined with any of the criteria from the European Guidelines
- Track individuals' location or behaviour (including but not limited to the online environment) – A DPIA is required when combined with any of the criteria from the European Guidelines
- Targeting of children or other vulnerable individuals (use of personal data of children or vulnerable individuals for marketing, profiling or automated decision-making, or to offer online services to children) – a DPIA is required
- Risk of physical harm (where a personal data breach could jeopardise an individual's physical health or safety). – A DPIA is required

The ICO has produced within its DPIA Guidance a list of processing operations for which the ICO requires you to carry out a DPIA as they are likely to result in high risk. You should refer to this list of non-exhaustive examples to help better understand when a DPIA is required.

When a DPIA may not be required

A DPIA may not be required where:

- The processing is not likely to result in a high risk
- The processing is on the basis of a legal obligation or public task, but only if:

- There is a clear statutory basis for the processing;
- The legal provision or a statutory code specifically provides for and regulates the processing operation in question;
- There are no other obligations to complete a DPIA derived from specific legislation, such as Digital Economy Act 2017; and
- A data protection risk assessment was carried out as part of the impact assessment when the legislation was adopted (the ICO recommends a DPIA is carried out in the absence of any clear and authoritative statement on whether such an assessment was done).

- The nature, scope, context and purpose of the processing are very similar to processing for which a DPIA has already been carried out;
- The processing is included on a list produced by the ICO of processing operations for which no DPIA is required - The ICO has not yet produced such a list but may do so in future.

If you establish that you are not obliged to carry out a DPIA, you must still continuously assess the risks around your processing activities to identify when a type of processing is likely to result in a high risk to the rights and freedoms of individuals and keep it under review.

You should complete the screening tool at **Appendix 1** to help you determine whether the proposed processing is of a type that is likely to result in a high risk and, therefore, if you are required to carry out a DPIA. Even if no mandatory obligation to carry out a DPIA applies, you must still properly consider whether the proposed processing is likely to result in a high risk and, if it is considered it has features which indicate a likely high risk, you should carry out a DPIA. If you are not sure whether the processing is likely to result in a high risk, you should carry out a DPIA regardless.

The Data Protection Officer's advice should be sought on whether you need to do a DPIA. Your completed screening tool should therefore be sent to the dpo@kent.gov.uk mailbox and, once a response is received from the DPO, the DPO's advice must be documented on the screening tool and must be retained as a record, particularly where a decision is made that a DPIA will not be carried out.

DPIAs and Data processing prior to GDPR

Where your data processing already existed prior to GDPR coming into force, you will need to review those processing operations to identify whether they would be considered likely to result in a high risk under GDPR. You can use the DPIA screening tool to do this. If the risks have not already been adequately assessed, then you may need to carry out a DPIA now, to ensure the processing is compliant with GDPR. If you have already considered the relevant risk and safeguards of your

data processing, whether that was through a 'privacy risk assessment' or other type of risk assessment process, then you may not need to carry out a DPIA, unless the nature, scope, context or purposes of the processing have significantly changed since that previous assessment was completed. In case of any challenge, you should keep a written record of the review carried out and any reasons for determining that a new DPIA is not being carried out.

How to carry out a DPIA and the information a DPIA should contain

The DPIA process

The flowchart at **Appendix 2** sets out the key steps that will need to be taken in the DPIA process with some guidance notes on what you will need to do and consider at each step, but you should refer to the ICO's DPIA Guidance for more detailed guidance.

The DPIA should be started as early as possible in the design stages of the proposed processing and must be carried out prior to the start of the processing. The DPIA should be carried out alongside the planning and development of the project and updated throughout the lifecycle of the project. How much time and resources you put into the DPIA will depend on the nature of the project.

In some circumstances not all the necessary information may be available at the start of the project and certain decisions can only be made at a later date, or the project may be being undertaken in phases. The DPIA must therefore be kept under review and be regularly reassessed and should be considered a living document which may need regular updating.

A DPIA is a continual process from the start of any project planning and throughout the life of the project, and so it is not acceptable to postpone or not carry out a DPIA because it might need to be updated once the processing has begun.

DPIAs must also be considered if any changes are being made to an existing system. If any significant changes to the processing, or new/increased risks to individuals are identified then the DPIA should be reviewed and advice from the DPO should be sought.

A DPIA will normally relate to one project/processing operation. However, there may be scenarios where a single DPIA can be used to assess multiple processing operations that are similar in terms of nature, scope, context purpose and risks. For example, where similar technology is used to collect the same sort of data for the same purposes, for example, for ANPR cameras in various car parks.

Roles and responsibilities in the DPIA process

The data controller is responsible for a DPIA, so where KCC is a data controller, it will be responsible for considering whether a DPIA is required and ensuring that a DPIA is carried out.

A DPIA may be outsourced or carried out by a data processor if they will be doing the processing on behalf of KCC, but KCC ultimately remains responsible for it and it must still be sent to the dpo@kent.gov.uk inbox for review and advice.

If a processing operation involves a joint data controller, the respective obligations of the data controllers will need to be precisely defined and the DPIA will need to clearly set out which data controller is responsible for the particular measures identified to address any risks identified. Each data controller should express their requirements/needs and share information without compromising secrets or confidential business information or disclosing vulnerabilities.

In most cases, it is likely that it will be most appropriate for project or operational managers to carry out the DPIA, with senior managers having oversight of the project and signing them off, but potentially other staff may need to carry out DPIAs. There are, however, others who you should involve and consult with, depending on the nature of the project, which might include:

- Data Processors – where the processing is partly or wholly performed by a data processor, the processor should assist KCC and provide any necessary information to KCC in carrying out the DPIA.

- Information security teams (for example, ICT Compliance and Risk if there are technical aspects to the project or high risk processing)

- Legal advisers

- Other experts, such as IT experts or any other professional

- Data subjects or their representatives – you must seek the views of data subjects or their representatives where appropriate. This could be done through various means (e.g. a study or survey, questions to staff), ensuring that you have a lawful basis for processing the personal data when seeking the views of data subjects. If you do not seek the views of data subjects, you must record the reason why in the DPIA, for example, seeking the views of data subjects would compromise confidentiality of business plans, or would be disproportionate or impracticable. If your views/decision are different from the data subjects' views, then you must record the reasons for going against their views in the DPIA.

- Other internal business units or external stakeholders involved with the project
- The Data Protection Officer (in all cases - see below)

The role of the Data Protection Officer (DPO)

When carrying out a DPIA you must seek the advice of the DPO. The DPO should be consulted on deciding how to approach a DPIA. The DPO will provide you with advice on:

- whether you need to do a DPIA
- how you should do a DPIA
- whether to outsource the DPIA or do it in-house
- measures and safeguards to mitigate risks
- whether the DPIA has been done correctly
- the outcome of the DPIA and whether the processing can go ahead.

The advice given by the DPO must be documented within the DPIA, together with the decision of KCC. If you decide to go against the advice of the DPO then this must be justified and the reasons for doing so must also be clearly recorded in the DPIA outcome.

It is also the DPO's role to monitor the performance of the DPIA.

You should contact the DPO as early as possible in the process for advice regarding a DPIA. Referrals should be made by email to dpo@kent.gov.uk. It is not acceptable to seek advice from the DPO on a DPIA at the point you intend to start the processing as this goes against the principle and legal requirement of data protection by design.

What a DPIA must include

As a minimum the DPIA should include:

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller. You should include enough detail for the data flow to be easily understood and scrutinised for any further possible mitigation measures which will improve data protection.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.

- An assessment of the risks to individuals.
- The measures in place to address and mitigate any risk, including security and to demonstrate that you comply with GDPR (e.g. staff training, pseudonymisation or anonymisation of data according to KCC's anonymisation and pseudonymisation policy and any particular IT security measures in place. These should cover organisational and technical measures that are both generally in place within KCC and those that are specific to the particular project).

A template for a DPIA can be found at **Appendix 3** for your use. When the DPIA is completed you should send it to the DPO at dpo@kent.gov.uk for consideration and advice on whether the processing can proceed. Your DPIA will be reviewed by the DPO support function to ensure it is completed correctly before being sent to the DPO. If you decide not to follow the advice of the DPO, you must justify this position and record your reasons in the DPIA.

Once the DPO has provided any advice, you should integrate the outcomes and action points in the DPIA into your project planning and ensure the actions are implemented.

If you identify that any high risks assessed cannot be mitigated, then you must consult the ICO before any data processing starts (see section below).

You will need to keep the DPIA under review throughout the life of the project and processing and monitor its performance. Remember, if there is any significant change in the nature, scope, context or purposes of the processing, then the DPIA must be reviewed and repeat the steps in the DPIA process.

Whilst any risks will be documented within the DPIA, project managers will also need to record any material privacy-related risks as part of the project or service/divisional risk register and have regular monitoring arrangements in place. If you require any advice in this regard, you can refer to the KCC Risk Management Toolkit on KNet.

When you must consult with the Information Commissioner's Office (ICO)

If you have carried out a DPIA which reveals a high risk to individuals which cannot be reduced or mitigated, or because the costs of mitigation are too high, the Information Commissioner's Office **must** be consulted **before** you can go ahead with the processing. The DPO will refer the matter to the ICO.

Upon accepting a DPIA for consultation, the Information Commissioner's Office will then have 8 weeks to provide a written advice, which can be extended by a further 6 weeks if the processing is complex. The DPIA cannot be approved before a response has been received from the ICO.

Examples of when there might be a high residual risk include:

- Where the data subjects may encounter significant, or irreversible, consequences, which they may not overcome
- When it seems obvious the risk will occur

The ICO may take the view that the processing can proceed, or they could provide advice on how the risks can be further mitigated before the processing starts. If the ICO is concerned that the proposed processing is likely to contravene GDPR, then they will issue an official warning, together with recommended steps on how to avoid any contravention of GDPR. If the ICO has more significant concerns, they may impose a limitation or ban on the proposed processing.

Documenting the DPIA

A record of the DPIA should be retained for the lifetime of the system or project/processing and be regularly reviewed and updated, when necessary.

Where it is determined that a DPIA does not need to be carried out, a record should be kept of the reasons why a DPIA was not considered necessary. This can be done on the DPIA screening tool and retained as a record.

Appendix 1 - DPIA Screening Form

PLEASE READ THE GUIDANCE ON PAGES 2-12 AND THE FURTHER INFORMATION PAGES BELOW BEFORE COMPLETION OF THIS SCREENING TOOL

Summarise what the project and proposed data processing is about	*[include brief details of the project and the data processing you are proposing to design/redesign. You can add the business case if you have one.]*

1	**Does the activity involve…**	**YES**	**NO**	**DPIA Necessary?**
Processing of personal data?				If no, a DPIA will not be necessary. If yes, please continue.
2	**Are you planning to…**	**YES**	**NO**	
Use systematic and extensive profiling or automated decision-making to make significant decisions about people.				If you answer 'yes' to any of these questions, you **must** carry out a DPIA.
Process special category data or criminal offence data on a large scale.				
Systematically monitor a publicly accessible area on a large scale.				
3	**Or are you planning to…**			
Make decisions on someone's access to a service, product opportunity or benefit which is based on automated decision-making (including profiling) or involves the processing of special category data.				If you answer 'yes' to any of these questions then you **must** carry out a DPIA.
Carry out profiling on a large scale.				
Combine, compare or match data from multiple sources.				
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 personal data breach.				
4	**Or are you planning to…**			
Process biometric data.				If you answer 'yes' to 2 or more of the criteria in this section 4, a DPIA **must** be carried out. **OR** If you answer 'yes' to any of these questions, and at least one criteria from section 5 below applies, then you must carry out a DPIA. Even if no additional criteria below apply, **you may still need to do a DPIA**
Process genetic data (other than by a GP or health professional to provide healthcare)				
Use innovative technology.				
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.				

				depending on the nature of the processing planned.
5	**Are you planning to carry out any other….**	**YES**	**NO**	
Evaluation or scoring.				Where two or more criteria are met, the activity may present a high risk to the rights and freedoms of data subjects and you should conduct a DPIA. Even if only one criteria is met, you may still need to conduct a DPIA if it is considered to present a likely high risk to the rights and freedoms of an individual. If uncertain about whether the risk is likely to be high, conduct a DPIA regardless.
Automated decision-making with legal or significant effects.				
Systematic monitoring				
Processing of sensitive data or data of a highly personal nature.				
Processing on a large scale.				
Matching or combining datasets				
Processing of data concerning vulnerable data subjects.				
Innovative use or applying new technological or organisational solutions.				
Processing involving preventing data subjects from exercising a right or using a service or contract.				
6	**Other**	**YES**	**NO**	
Are you planning any major project involving the use of personal data?				If so, you should consider carrying out a DPIA as good practice.
7	**Has there been a change…**			
In the nature, scope, context, or purposes of existing processing operations				You should carry out a new DPIA.

Conclusion	**YES**	**NO**	**Rationale**
Is a DPIA required?			*[please do not set out here the steps you have taken to mitigate your risks – that is the purpose of the DPIA. If you have ticked the relevant 'yes' boxes and the criteria for a DPIA is met, you MUST carry one out – THIS IS A LEGAL REQUIREMENT]*
If no, will a DPIA be conducted anyway?			
Summary of DPO advice:			

When you have completed this screening tool please send it to the DPO for logging and advice: dpo@kent.gov.uk

Further Information

Personal Data

Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

If the person can be identified alongside other information that is held by, or is likely to be held, by KCC, we must also consider this to be personal data.

Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person, remains personal data.

Examples of personal data include:

- a name and surname;
- date of birth;
- gender;
- a home address and postcode;
- an email address, such as name.surname@company.com;
- an identification card number;
- location data (for example the location data function on a mobile phone);
- an Internet Protocol (IP) address;
- an image
- a cookie ID.

Special Category Data

Special categories include:

- sex life
- sexual orientation
- religious or philosophical beliefs
- racial or ethnic origin
- health (physical or mental)
- trade union membership
- political opinion
- genetic data
- biometric data

Sensitive personal data includes any information that presents an elevated risk to rights and freedoms. An example is that processing financial information may lead to a higher risk of fraud. You should also consider if the data may increase the chances of discrimination under this criterion.

It should be noted that ‘protected characteristics’ information is a definition from the Equality Act 2010 and means information about age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation. It is not the same as special category data, although some protected characteristics will be classed as special category data

Criminal Offence data

Criminal offence data is personal data relating to criminal convictions and offences, or related security measures. This includes data relating to the alleged commission of offences by the data subject, or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

Vulnerable Individuals

Using the personal data of vulnerable people increases the risk of a power imbalance between KCC and the data subject. Vulnerability should be judged according to the context of an individual's ability to oppose, prevent or understand the processing. For example, children and vulnerable adults. **Employees should also be classed as vulnerable in the context of their employer**.

Systematic and extensive

'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.

'Extensive' implies the processing also covers a large area, involves a wide range of data or affects a large number of individuals.

Automated Decision Making

When decisions are made without any human involvement they are considered to be automated. An individual might input the data, but unless they contribute to the decision that is made, it will still be automated. Where the decision is reviewed by a human and the potential for intervention is built into the process, this would not count as automated decision making.

Profiling

Profiling is an automated process which evaluates individuals based on certain personal data. Information commonly used for this purpose includes, performance at work, economic situation, health, personal interests, and, behaviour or location. The production of a score or rating based on personal data is a good indication that profiling has taken place.

Even if profiling has not taken place, any activity that results in a prediction should be considered a risk. E.g. banks screening customers against an existing credit reference database. A local authority decision that could lead to changes in service provision could significantly affect individuals.

Combining Data

Where data already exists, it is important to ensure that the data is still being used in line with its original purpose. Even if some of the data is collected specifically for the activity, combining it with existing data may increase the risk. An important consideration is whether the individual would reasonably expect the operation to take place and if they may object.

Transfers outside of the EU

Significant safeguards must be in place when data is transferred to places where the GDPR does not apply. It might not be obvious at first that data is being moved outside of the EU because much information now moves digitally, it may be that external providers are hosting servers outside of the EU. An example is MailChimp.

Large Scale Processing

When determining the scale of the activity you should consider four factors:

1. The number of data subjects concerned – consider this alongside the relevant population and the proportion affected by the processing. E.g. the population of Kent, a district, a demographic group or service users.
2. The volume and/or range of data used – consider if all the data is from a single category e.g. finance and how much detail is required.
3. The duration of the activity – some processing activities have a clear end whereas others would be continuous.
4. The geographic extent of the activity – consider where the activity takes place, local, regional, national etc.

There is no set measure of large scale but any one of these factors could trigger high risks to data subjects. You may wish to document the justification for judgements made about the scale of processing operations.

Some examples given by the ICO include:

- A hospital (not an individual doctor) processing patient data
- Tracking individuals using a city's public transport system
- A fast food chain tracking real-time location of its customers
- An insurance company or bank processing customer data
- A search engine processing data for behavioural advertising
- A telephone or internet service provider processing user data

Data Controller

A data controller is a natural or legal person, public authority, agency or other body, which, along or jointly with others, determines the purposes and means of the processing of personal data, i.e. data controllers decide what data to process, why and how. Data controllers are responsible for the compliance of their data processors.

Joint Data Controllers

Where two or more data controllers jointly determine the purposes and means of the processing of the same personal data for the same or shared purposes. They will not be joint data controllers if they are processing the same personal data but for different purposes.

Data Processor

A data processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller. A data processor processes personal data only on the instructions of the data controller.

Innovative technologies

Innovative technology concerns new developments in technological knowledge in the world at large, rather than technology that is new to you, and its use can trigger the need to carry out a DPIA. The personal and social consequences of deploying a new technology might not be known and a DPIA will help you to understand risks. The ICO has provided some examples which include:

- Artificial intelligence, machine learning and deep learning
- Connected and autonomous vehicles
- Intelligent transport systems
- Smart technologies (including wearables)
- Market research involving neuro-measurement (e.g. emotional response analysis and brain activity)
- Some 'internet of things' applications, depending on the specific circumstances of the processing

It may also include implementing existing technology in a new way. Unless a DPIA is carried out, high risks may not be identified.

Significantly affect

In the context of profiling, this means it will have a noticeable impact on an individual and can significantly affect their circumstances, behaviour or choices.

A legal effect is something that affects a person's legal status or legal rights. A similarly significant effect might include something that affects an individual's financial status, health, reputation, access to services or other economic or social opportunities.

Invisible processing

This is where you obtain personal data about an individual from another source and not directly from the individual, and you do not provide the individual with privacy information as required by Article 14 GDPR. The individual is therefore unaware their personal data is being collected and used by you. GDPR only permits 'invisible processing' where providing privacy information would prove impossible (for example, there are no contact details for the individuals and there are no reasonable means of obtaining them) or involve disproportionate effort. You must be able to justify any reliance on the disproportionate exception, and take other measures to protect individuals' rights, for example, still publishing privacy information on KCC's

website and carrying out a DPIA. This will help to assess whether you are taking a proportionate approach and what other measures could be taken to support the exercise of individuals' rights.

Appendix 2 – DPIA process flowchart

Identify need for a DPIA

Think about:

- Is the processing likely to result in a high risk to the rights and freedoms of individuals?
- Use the screening tool to determine if a DPIA needs to be carried out
- Seek DPO advice and record the advice on the screening tool
- If you decide a DPIA is not required, record your reasons

↓

Describe the processing

Think about:

- The context of the processing, eg source of the data, relationship with individuals, can individuals control their data, are they likely to expect processing, does it include children or vulnerable people, previous experience of the type of processing, advances in technology or security, current issues of public concern, codes of conduct or codes of practice. Consider relationship between parties/partners, eg data controllers/processors/sub-processors/joint controllers, etc.
- The nature of the processing, eg how you collect, store and use the data, who has access to it and who its shared with, any data processors, security measures and retention periods, is it novel, is it a new technology, and the screening criteria flagged.
- The scope of the processing, eg, the nature of the data, sensitivity, volume and variety of data, extent and frequency of processing, duration of processing, number of data subjects and geographical area.
- The purpose of the processing, eg any legitimate interests, intended outcome for individuals, expected benefits for KCC or society.

↓

Consider consultation

Think about:

- Individuals or their representatives (unless there is good reason not to do so and explain your reasons), eg using existing contact information, or by targeted research
- Data processors or contractors
- Internal teams, eg ICT Risk and Compliance, or any other teams involved in the project
- Any experts, eg IT, legal or other professional
- How will you consult?
- When will you consult?

↓

Assess necessity and proportionality

Think about:

- Do your plans help to achieve your purpose?
- Is there another way to achieve the same result?

↓

Identify and assess risks

Think about:

- Individuals – the potential impact of any harm that might be caused by the processing, physical, emotional or material (eg discrimination, identity theft, reidentification of pseudonymised data, financial loss, reputational damage, loss of confidentiality, inability to access a service or exercise rights, any other significant social or economic disadvantage etc.)
- Security risks and potential impact of a breach (eg loss of data)
- Corporate risks for KCC, eg reputational damage, loss of public trust, action taken against KCC
- Are the risks high, medium or low, considering the likelihood and severity of potential harm?

↓

Identify measures to mitigate risk

Think about:

- For each risk identified, consider the options of reducing that risk (eg anonymisation of data, staff training, additional security measures, data sharing agreements, not collecting certain data, etc.)
- Have the measures eliminated or reduced the risks?
- What are the residual risks?
- Ask DPO for advice on any measures

↓

Sign off, DPO advice and outcomes

Think about:

- Record additional measures planned, whether risks are eliminated, reduced or accepted, and the level of residual risk.
- Do you need to consult the ICO? If yes, DO NOT start processing until outcome received from ICO
- Seek advice from the DPO on whether the processing is compliant and can proceed and record the summary of the advice
- If you don't follow DPO advice, record the reasons why
- Record reasons for going against views of individuals or other consultees, or why their views have not been sought.

↓

Integrate outcomes into plan

Think about:

- Any actions identified in the DPIA should be integrated into your project planning.
- Who is responsible for the actions?
- Consider whether the risks identified need to be fed into the project or service/divisional risk register, depending on whether project or broader organisational objectives are threatened.

↓

Keep DPIA under review

Think about:

- If there are any substantial changes to the nature, scope, content or purposes of the processing, or to the risks, review the DPIA and repeat these steps if necessary.

Appendix 3 – DPIA Template

PLEASE READ THE POLICY AND GUIDANCE BEFORE COMPLETING THIS TEMPLATE – IF YOU ARE STILL UNSURE HAVING READ THE GUIDANCE NOTES IN THIS POLICY AND GUIDANCE, READ THE DETAILED ICO GUIDANCE HERE

THEN DELETE THE POLICY SECTIONS AND SEND ONLY THE COMPLETED SCREENING TOOL AND THIS DPIA (APPENDICES 1 AND 3 ONLY) TO DPO@KENT.GOV.UK

DATA PROTECTION IMPACT ASSESSMENT

Undertaking a DPIA should be thought of as a process. This standard document is a template to be used to draw together information gathered through the DPIA process, to document the outcome of the DPIA and to record the actions to be taken as a result of the DPIA.

When carrying out a DPIA it is helpful to draw together all relevant facts into one place, so that when drawing a conclusion about the outcome of the DPIA, the facts relied on to reach the outcome are available to hand. For that reason, when completing the DPIA it would be prudent to complete the fact-gathering sections first before completing the analysis sections (in particular, Section 8 and 9), with the executive summary (Section 3) being the final section to be completed.

1. Document History			
Version Number	**Summary of change**	**Reviewed by (name and role)**	**Date**
[insert number]	*[insert a short summary of the change/update]*	*[name and title/role]*	*[insert date this version was agreed]*

2. Administrative information	
Name of organisation	*[i.e. KCC, or other joint data controller]*
Service unit responsible for the project	*[eg. HR, Finance, Procurement, etc]*
Senior Officer responsible for the project	*[name, title, contact number]]*
Project Manager	*[name, title, contact number]*
Data processor (if applicable)	*[full name and contact details of any data processor assisting KCC in completing this DPIA eg Cantium Business Services Limited]* *[Example of data processor is a service provider processing data on KCC's behalf. Employees are not data processors]*
Data Protection Officer	*[name and contact number]*
[Other key personnel involved in the project]	*[name, title, contact number]*

3. Executive Summary (complete this section last)
[Please include brief details of the following:

- *Summary of the project description*
- *Summary of the scope of processing, purposes of the processing and the legal basis for processing*
- *Summary of the intended benefits for data subjects, third parties and KCC*
- *Summary of the privacy risks and any proposed solutions to mitigate them.*

Please ensure you do not include anything of a commercially sensitive nature, or anything that might put the project or KCC at risk, into this section]

4. Identify the need for a data protection assessment (DPIA) (complete the screening tool and attach a copy to this DPIA)	
What type of processing is involved?	*[include the types of processing as identified in the screening tool, eg , public monitoring, large scale use of sensitive data, data concerning vulnerable data subjects, invisible processing, etc.. Include any other relevant factors]*
Reasons a DPIA is required	[*Summarise the reasons for deciding to carry out a DPIA. Is it automatically required by GDPR or the ICO, or do the features of the processing indicate a likely high risk. Refer to the screening tool and DPO advice.]*

5. Description of the Processing (you may wish to use or attach a data flow and attach to this DPIA)	
Description of the Project/Processing	[*Describe the project in detail, eg new IT system for storing and accessing personal data, or proposal to identify people in a particular group or demographic to predict their needs. Does it cover a single processing operation or multiple?]* *[Insert the aim of the processing, eg Improve the quality and accuracy of employee personal data and implement an improved process for deleting data that is no longer required]* *[refer or link to relevant documents, eg project proposal or business case]*
What is the scope of the processing?	
Types of personal data	*[identify the categories of data that will be collected/processed, eg is it personal data, special category data, or criminal offence data?* *'Special category data' means racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health data or data about someone's sex life or sexual orientation.* *It should be noted that 'protected characteristics' information is not the same definition, but is a definition from the Equality Act 2010 and means information about age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation. Some protected characteristics may be classed as special category data.* *Criminal offence data is personal data relating to criminal convictions and offences, or related security measures. This includes data relating to the alleged commission of offences by the data subject, or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.*
How many individuals will be affected and what geographical area will it	

cover?	
How much data will be collected and used?	
Length and frequency of processing	*[How long will you be collecting the data for, what is the frequency of collection?]*
How long will the data be retained for?	*[Set out the retention period, how the data will be archived, etc. State the actual retention period for the data in the project or (if you have multiple retention periods, cite the relevant sections of the retention schedule. Do not simply link to KCC's retention schedule as the DPIA needs to demonstrate the period is known and applied and identify where the period may not be relevant.* *Detail how KCC will adhere to the fifth data protection principle that all personal data is kept for no longer than is necessary for the purposes for which the personal data are processed]*
What is the nature of the processing?	
How will the data be collected and what is the source of the data?	*[How is the data collected? Will it be collected directly from data subjects or other sources, etc.]*
How will the data be used and stored	*[Set out exactly how the data will be used and stored.*
How is the data secured and processed in a manner that ensures appropriate security (including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)?	*What are the practical safeguards (eg access management arrangements, training and awareness, due diligence arrangements re third parties, monitoring of arrangements with third parties)? What security measures will there be (eg. encryption, data breach notifications)? Will there be any mechanisms to protect the personal data (eg. anonymisation, arrangements for destruction, data back up)? How will the ongoing confidentiality, integrity availability and resilience of the processing system be ensured and what is the process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring security? GDPR requires appropriate technical and organisational measures to ensure a level of security appropriate to the risk and specifically includes encryption or pseudonymisation, an ability to ensure the ongoing confidentiality and integrity of information, the ability to access information in the event of a breach and a process for regularly testing assessing and evaluating the effectiveness of security measures. (e.g. worth mentioning ISO compliance adherence or requiring that Processors have certifications etc)]*
How will the data be deleted/disposed of?	*[How the data will be deleted at the end of the retention period]*
Will the data be shared/disclosed to third parties?	Yes/No *[If yes, include details of who the data will be disclosed to (eg. partnerships or contractors), what data will be disclosed and why, whether there are any information sharing agreements in place, and who will be responsible for the monitoring arrangements or contract management, and whether there is a need or not for a separate DPIA.]*
What types of processing identified as likely high risk are involved?	*[link back to those identified in your screening tool]*
What is the context of the processing?	
What are the categories of	*For example, children, employees, customers, etc]*

data subject, and do they include children or vulnerable groups?	
What is the nature of the relationship with individuals?	*A local authority is regarded as being in a position of power in relation to data subjects.*
How much control will they have?	
Would they expect you to use their data in this way?	*[Yes/No]* *[state the reasons why]*
Are there prior concerns over this type of processing or security flaws?	
Is it novel in any way?	
What is the current state of technology in this area?	
Are there any current issues of public concern that you should factor in?	
Are you signed up to any approved code of conduct or certification scheme?	
What is the purpose of the processing?	
What do you want to achieve?	
What is the intended effect on individuals?	*[set out the intended outcome for individuals]*
What are the benefits of the processing for KCC, and more broadly?	*[set out the expected benefits for KCC, individuals, or society as a whole]*

6. Consultation			
Who will you consult?	**When will you consult?**	**How will you consult?**	**Responses**
[Project management team]	[*State at what stage of the project you will consult with consultees]*	[*State how you will consult them]*	*[Summary of the response or advice provided, including the date given]*
[*ICT Risk and Compliance]*			
[Procurement]			
[Potential suppliers and data processors]			
[Other experts, eg. IT,			

legal or other professionals]			
[Insert anyone else with an interest in the project]			
Data subjects or their representatives	[*State how you will consult—eg studies or questionnaires, speaking to groups]* *[The views of individuals affected should be sought unless there is good reason not to and in most cases it should be possible to consult individuals in some form. However, if it is decided that it is not appropriate to consult individuals then this should be recorded in this section with a clear explanation as to why and how it would undermine security or be disproportionate or impracticable or compromise commercial confidentiality]*	[*State at what stage of the project you will consult*]	*[Summarise the response or advice, including the date given. Nb. If the data controller's final decision is different from the view of the data subjects, reasons must be provided]*

7. Assess necessity and proportionality	
What is the lawful basis for processing?	*[It is useful to state the power or duty your activities fall within but this section MUST include your GDPR Article 6 legal basis and any exception relied on under Article 9 (where you are using special category data). This will be identified in the privacy notice given to data subjects. The Article 6 legal bases for processing personal information are consent, legal obligation, contract, vital interests, public task, legitimate interests.* *The Article 9 GDPR exceptions for processing special category data are (1) explicit consent, (2) employment/social security/social protection, (3) vital interests, (4) legitimate activities by foundation, association or not-for-profit body with political, philosophical, religious or trade union aim, (5) data manifestly made public by data subject, (6) legal claims, (7) substantial public interest, (8) for health and social care, (9) for public health, or (10) for archiving purposes in the public interest, scientific or historical research purposes. Where required, depending on the Article 9 exception relied upon, ALSO ADD any condition relied on under Schedule 1 Data Protection Act 2018 PLUS any additional safeguards (eg appropriate policy document). Examples of commonly used conditions include: for employment, health or social care, safeguarding, equality of opportunity or treatment, public health.* *If you are relying on the health or social care purposes or the management of health or social care purposes exception please note:* *S11(1) states: 'For the purposes of Article 9(2)(h) of the GDPR (processing for health or social care purposes etc), the circumstances in which the processing of personal data is carried out subject to the conditions and safeguards referred to in Article 9(3) of the GDPR (obligation of secrecy) include circumstances in which it is carried out –* *(a)by or under the responsibility of a health professional or a social work professional, or*

	(b) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.' *Please note these legal bases should be consistent with the relevant privacy notice you identify within the DPIA.]*
Legitimate interests	[*Where you intend to rely on legitimate interests as the lawful ground for processing under the GDPR, describe those legitimate interests and also confirm that a legitimate interest assessment has been undertaken and what the outcome of the assessment is.]*
What information will you give to individuals?	*[Demonstrate that you meet the fair processing requirements, eg. Information provided to the data subject (add a link the relevant privacy notice here and state how it will be delivered to data subjects), or cookies notice]*
Does the processing achieve your purpose?	
Is there another way to achieve the same outcome?	
How will you prevent function creep and preserve the second data protection principle: 'purpose limitation' (ie only using the data for specific, explicit and legitimate purposes (as set out in a privacy notice) and not further processing the data in a manner that is incompatible with those purposes	*[i.e. how will you prevent the use of the data going beyond the purpose for which it was originally intended and obtained.]*
How will you ensure data quality and minimisation?	*[Identify considerations given to data minimisation (such as certain types of data subject not included in the scope, data collected being minimised, anonymisation being used, etc.) Data minimisation is a fundamental principle of the GDPR: 'Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'). State how this is being addressed in the processing.]*
How will you ensure personal data is accurate and, where necessary, kept up to date	
How will you support data subject rights?	*[What are the arrangements to ensure data subjects' rights are protected (eg. Right to be informed, right of access, right to erasure, data accuracy, data portability, etc.). The degree to which all these rights may be relevant will depend very much on the nature of the processing. Also set out any particular special arrangements for vulnerable subjects or where there is an 'imbalance of power'. Consider who the data subjects are, eg children, vulnerable adults, employees, general public, and how you will support the rights of those specific types of data subjects. For example, having easy read privacy notices for children/vulnerable adults, or, if your Article 6 legal basis is consent, will you regularly review that consent.]*
What measures do you	*You should as a minimum confirm that any data processing contract*

take to ensure processors comply?	*contains the Article 28 mandatory terms. These should be incorporated in Annex 1/a data protection clause, but if in doubt check with the lawyer who has drafted the service contract on KCC's behalf.* *Also consider how these requirements are to be managed (eg to only act on KCC's instructions, to inform KCC if a sub processor is to be appointed etc)*
How do you safeguard international transfers?	*[e.g. a software supplier is US based but is signed up to the EU-US Privacy Shield.]*

8. Identify and assess risks
(you can refer to the attached risk matrix to help assess the level of risk)

Risks to INDIVIDUALS

(Remember, a DPIA is focussed on the potential harm to data subjects and should be considered from the data subject's point of view.)

Risk Description	Likelihood of harm	Severity of harm	Overall risk
Examples (please tailor/add/delete as necessary): *[Inadequate disclosure controls, increasing the likelihood of information being shared inappropriately.]*	*[Very unlikely, unlikely, possible, likely, or very likely]*	*[Minor, moderate, significant, serious, major]*	*[High, medium or low]*
[The context in which information is used or disclosed may change over time, leading to it being used for different purposes without people's knowledge or consent.]			
[New surveillance methods may be an unjustified intrusion on their privacy.]			
[Measures taken against individuals as a result of collecting information about them might be seen as intrusive.]			
[The sharing and merging of datasets may allow us to collect a much wider set of information than individuals might expect.]			
[Identifiers might be collected and linked which prevent people from using a service anonymously.]			
[Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.]			
[Collecting information and linking identifiers might mean that we no longer use information that is safely anonymised.]			
[Information may be collected and stored unnecessarily, or not properly managed so that duplicate records are created, presenting a greater security risk.]			

[Failure to establish appropriate retention periods might mean information is used for longer than necessary.]			
[*Insert any other risk to individuals' privacy*.]			
Organisational risks			
Examples (please tailor/add/delete as necessary): *[Non-compliance with the GDPR or other legislation, which can lead to sanctions, fines and reputational damage.]*			
[Problems may only be identified after the project has launched and will then be more likely to require expensive fixes.]			
[The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with KCC.]			
[Information may be collected and stored unnecessarily, or not properly managed so that duplicate records are created—meaning the information is less useful to the business.]			
[Public/client/customer distrust about how information is used may damage KCC's reputation.]			
[Data losses which damage individuals could lead to claims for compensation.]			
[Insert any other risk to the organisation]			
Legal compliance risks			
Examples (please tailor/add/delete as necessary): *[Non-compliance with the GDPR -* i.e. *will the processing meet the principles in Article 5 GDPR, i.e.* • *Fair, lawful, transparent* • *Specified, explicit, legitimate purposes* • *Adequate, relevant and not excessive* • *Accurate and up to date* • *Not kept longer than necessary* • *Processed in accordance with rights of data subjects* • *Protection against unauthorised or unlawful processing, loss, destruction or damage* • *Not transferred outside EEA unless adequately protected.]*			

[Non-compliance with the Privacy and Electronic Communications Regulations 2003 (PECR 2003), e.g. if KCC wish to send electronic marketing messages (by phone, email or text), use cookies, or provide electronic communication services to the public]			
[Non-compliance with sector specific legislation or standards.]			
[Non-compliance with human rights legislation, eg breaching an individual's Article 8 right to private and family life. You must also ensure your personal data processing has a legitimate aim]			
[*Insert any other legal compliance risk, e.g. creating datasets may increase risks/costs through disclosing requirements under the Freedom of Information Act 2000*]			

9. Identify and evaluate measures to reduce risk					
Potential solution	**Which risk(s) would this action address?**	**Effect on risk**	**Residual risk**	**Cost/benefit/ evaluation**	**Measure approved?**
Examples (please tailor/add/delete as necessary): *[Not collecting or storing [insert description] type of information.]*	[*State which of your identified risk(s) will be addressed by this action.*]	[*Is the risk eliminated, reduced or accepted?*]	*[Low, medium or high]*	[*Is the final impact on individuals a justified, compliant and proportionate response to the aims of the project?*]	*[yes/no]*
[Introducing retention periods to keep information for only as long as necessary.]					
[Secure destruction of information that no longer needs to be retained.]					
[Implementing appropriate technological security measures.]					
[Properly train staff and make them aware of potential privacy risks.]					
[Ensure information is safely anonymised when it is possible to					

do so.]					
[Provide guidance to staff on how to: *—use the new system, and* *—share data appropriately]*					
[Ensuring the new system: *—allows individuals to access their information more easily, and* *—makes it simpler to respond to subject access request]*					
[Ensuring individuals: *—are fully aware of how their information is used, and* *—can contact us for assistance when necessary]*					
[Selecting data processors who will provide a greater degree of security.]					
[Ensuring agreements are in place with data processors to protect information processed on our behalf.]					
[Ensuring any data sharing agreement makes it clear: *—what information will be shared* *—how it will be shared, and* *—who with]*					
[Insert any other solution you have identified]					

10. ICO consultation	
Does this assessment indicate that the processing involved in the project would present a high risk in the absence of mitigation measures?	Yes/No

If yes, can those risks be mitigated by reasonable means in terms of available technologies and costs of implementation?	Yes/No [*If no, it is necessary to consult with the Information Commissioner's Office (ICO) prior to the processing.*]
If it is necessary to consult with the ICO, has this been done?	Yes/No or Not applicable *[If yes, provide further information.]*

11. Sign off and record of outcomes		
Item	**Name/date**	**Notes**
Measures to reduce risk approved by:		*Integrate actions back into project plan, with date and responsibility for completion*
Residual risks approved by:		*If accepting any residual high risk, consult the ICO before going ahead*
DPO advice provided:		*DPO should advise on compliance, measures to reduce risk and whether processing can proceed*
Summary of DPO advice:		
DPO advice accepted or overruled by:		*If overruled, you must explain your reasons*
Comments: *[if the advice is accepted, please ensure any actions recommended by the DPO are added to the DPIA and implemented].*		
Consultation responses reviewed by:		*If your decision departs from individuals' views, you must explain your reasons*
Comments:		
This DPIA will kept under review by:		*The DPO should also review ongoing compliance with DPIA*

[I/we] confirm that [I/we] have reviewed this DPIA and [am/are] satisfied that:

- it is [not] necessary to consult with the ICO.
- the proposed project complies with the data protection principles in Article 5 of the GDPR.
- in relation to the processing of personal data, at least one of the lawful grounds in Article 6 of the GDPR applies.
- in relation to the processing of sensitive (special category) personal data, at least one of the exceptions in Article 9 of the GDPR also applies.
- all relevant privacy risks and solutions have been fed into the appropriate risk register (e.g. project risk register, or at a service or divisional level for risks with wider organisational impacts) with regular monitoring arrangements in place.
- the solutions identified in this assessment represent a targeted and proportionate response to the identified privacy risks.

Name(s)	[*Insert name of person or persons signing off and approving the DPIA*]

Job title(s)	[*Insert job title of person or persons signing off and approving the DPIA*]
Date	[*Insert date*]

12. Actions to be integrated into project plan		
Action to be taken	**Date for completion or frequency**	**Responsibility for action**
[Integrate the DPIA outcomes back into the project plan and update relevant project management paperwork/spreadsheets.]	*[insert date]*	*[insert name]*
[Implement the approved privacy risk solutions.]	*[insert date]*	*[insert name]*
[Review and update the DPIA and project plan at regular intervals.]	*[insert frequency, eg monthly]*	*[insert name]*
[Conduct consultations.]	*[insert date]*	*[insert name]*

Risk Matrix

Likelihood							
	Very likely	5	5 Low	10 Medium	15 Medium	20 High	25 High
	Likely	4	4 Low	8 Medium	12 Medium	16 High	20 High
	Possible	3	3 Low	6 Low	9 Medium	12 Medium	15 Medium
	Unlikely	2	2 Low	4 Low	6 Low	8 Medium	10 Medium
	Very Unlikely	1	1 Low	2 Low	3 Low	4 Low	5 Low
			1	2	3	4	5
			Minor	Moderate	Significant	Serious	Major
			Impact				