

**Data Protection Impact Assessment Report**

|  |
| --- |
| **Project Information**  |
| Project Name (and or number) |  |
| Business Area/s Affected |  |
| Information Asset Owner |  |
| Senior Responsible Officer |  |
| Project Manager |  |
| Data Protection Officer |  |

|  |
| --- |
| **Document Ownership**  |
| Author(s)  |  |
| Document Owner |  |

|  |
| --- |
| **Document Review Information** |
| **Document Location** |  |
| **Quality Reviewers** | **Name** | **Role** | **Sections Reviewed** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Version History** | **Version Date** | **Requestor of Change** | **Summary of Change(s)** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| **Distribution List**  |
| **Name** | **Department/Organisation** | **Project Role** |
|  |  |  |
|  |  |  |

**Introduction**

*Guidance notes on how to complete this DPIA can be found in Appendix A.*

The **Data Protection Impact Assessment (DPIA)** process is not only a legal requirement, as explained in Appendix B, it is also an important tool to help you identify and minimise the data protection risks of a project that involves processing personal data.

The DPIA process is relevant to initiatives involving the use of personal data and is particularly important when a new business process or technology initiative involves the collection, recording, sharing or retention of personal data.

The DPIA enables privacy and data protection considerations to be made in the early stages of a project where any identified problems can be easier to resolve rather than late or retrospective considerations where solutions can be costlier or delay implementation. A DPIA, can also identify whether the project should be continued when balanced with the rights and interests of persons affected.

The DPIA process will consider privacy in the way individual’s personal data is used. This can involve privacy about: the integrity of the individual, the person, their personal information, their personal behaviour and their personal communications.

When carried out early the DPIA process can provide the following benefits:

* meet legal requirements;
* avoid loss of trust and reputation;
* identity management and privacy principles;
* avoid disproportionate or unnecessary use of personal data;
* avoid unnecessary costs;
* avoid inadequate solutions;
* support a communications strategy.

**Who is responsible for carrying out a DPIA?**

The responsibility for conducting a Data Protection Impact Assessment (DPIA) lies with the Information Asset Owner (IAO) for a project and is produced as part of the project proposal however; this activity can be delegated to an appropriate person such as the Project Manager/Lead. When a new project/initiative involving the processing of personal information is being considered the IAO or Project Manager will contact the DPO to arrange a meeting with relevant parties to discuss the proposal. At this stage it may be identified that it is necessary to undertake an information security assessment.

The DPIA will require authorisation by:

* Information Asset Owner and Senior Responsible Officer
* Data Protection Officer
* Senior Information Risk Officer – where the DPIA has identified ‘high’ residual risks and referral to the Information Commissioner is required.

**Data Protection Impact Assessment Report**

***Remove any red text in the DPIA Report and remove the Appendix A and B guidance/advice pages from this document, once complete and before submission.***

|  |
| --- |
| **1. Outline of the project, objectives and benefits** *See Appendix A, Part 1 for guidance* |
| The project will XXXXXXXXXXXXX |

|  |
| --- |
| **2. Describe the intended use of personal data:** |
| *The following headers and sections must be completed. The bulleted lists are shown to guide the sort of information required in this section. Provide some information about each of the bullets that are relevant to the project / initiative.***a) Describe the nature of the processing:**The nature of the processingis what you plan to do with the personal data. This should include, for example:* *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 processors;*
* *retention periods;*
* *security measures;*
* *whether you are using any new technologies;*
* *whether you are using any novel types of processing; and*
* *which screening criteria you flagged as likely high risk.*

**b) Describe the scope of the processing**The scope of the processing is what the processing covers. This should include, for example:* *the nature of the personal data;*
* *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 estimated number of data subjects involved; and*
* *the geographical area covered.*

**c) Describe the context of the processing:**The context of the processing is the wider picture, including internal and external factors which might affect expectations or impact. This might include, for example:* *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 have considered and complied with any relevant Codes of*

*Practice.***d) Describe the purposes of the processing:** The purpose of the processing is the reason why you want to process the personal data. This should include:* *statutory requirement;*
* *your legitimate interests, where relevant;*
* *the intended outcome for individuals; and*
* *the expected benefits for you or for society as a whole.*
 |

|  |
| --- |
| **3. Consultation:** *See Appendix A, Part 3 for guidance.* |
| 1. The following consultation approach and stakeholder groups were incorporated into the consultation process:
2. A summary of the stakeholder views are as follows:
3. The above stakeholder views were taken into consideration and measures to support them have been included in the planned data processing activities.

*If you adopted all relevant stakeholder feedback into your planned processing activities you will not need to complete the following 2 sections which can be deleted.*1. The following stakeholders views whilst being considered were not reflected in the planned processing activities:
2. The rationale for not doing so is as follows:
 |

|  |
| --- |
| 4. Data protection compliance – assessment of necessity and proportionality of personal data processing. |
| *Complete each of the below sub-sections. They are structured to assist completion and additional guidance can be found in Appendix A, Part 4. This is the main area where you will demonstrate how the processing of personal data complies with data protection legislation and therefore a degree of engagement with the DPO will be beneficial.* **Principle 1: Use of personal data is fair, lawful, and transparent:**1. Lawful basis for the processing of personal data is stated as follows:
* Personal data:
* Special Category data:
* Criminal data:
1. Explain how individuals will be made aware of the processing: (this may be part of a Fair Processing Notice)

**Principle 2: Use of personal data is for a specified, explicit and legitimate purpose and not re-used for a purpose that is in-compatible with the original purpose:**1. If collecting personal data for primary use, explain how you have targeted only the information required:
2. If re-using personal data for further use, explain how this secondary use is compatible with the original reason you collected it:

**Principle 3: Use of personal data is adequate, relevant and no more than necessary:**1. Explain how the amount of personal data you intend to use is enough to be understood by the audience but no more than the minimum needed to achieve your purpose:

**Principle 4: Personal data must be accurate and kept up to date:**1. Explain how accurate recording of data will be achieved and how it will be kept up to date, where necessary:
2. Explain any mechanisms that will allow you to amend or append data that is found to be inaccurate (ie: DQ errors in recording):

**Principle 5: Personal data must be kept in an identifiable format for no longer than necessary:**1. Data held in the new IT System – explain how any automated and / or manual capability to delete data will be used to comply with MoPI retention rules or the NPCC Retention Schedule:
2. Data held in an unstructured manner (paper, word / excel files etc) - explain how you will use any automated and / or manual capability to delete data in line with MoPI retention rules or the NPCC Retention Schedule:

**Principle 6: Personal data must be protected against unauthorised / unlawful use, accidental loss, damage or destruction:**1. Explain any technical security measures that will be put in place to protect the data:
2. Explain how you will make data users (staff) aware of any security measures or procedures they will need to follow:

**7. Personal data will be processed in accordance with the individual’s data protection rights:** 1. Explain, where relevant, how requests from individuals wanting to exercise their rights, will be managed.

**8. Personal data will not be transferred outside the European Economic Area (EEA) without guaranteed adequate privacy protections:**1. Confirm whether personal data is being processed outside the EEA and if so where:
2. If yes to a) above - explain which of the formal / recognised ‘adequacy’ measures will guarantee privacy protection:

**9. The force must be able to demonstrate how they are complying with the Data Protection Act 2018 & GDPR:**1. Explain what (if any) governance documents will be required to support the data processing (eg: Information Sharing Agreements, Data Processor contractual clause etc):
2. Detail, where known, what governance arrangements will be in place to oversee the processing of personal data in a compliant manner when BAU:
 |

|  |
| --- |
| **5. Identifying and assessing risks** *See Appendix A, Part 5 for guidance.* |

The main focus of the risk assessment within the DPIA is to consider the risks to the interests of the individuals whose data will be processed. Risks may also be intangible (significant social or economic disadvantage) such as the risk of losing public trust. The identified risks are listed below and scored using a standardised risk assessment matrix.

The listed ‘agreed actions’ have been identified as a way to either **reduce or eliminate** risks identified as **medium or high**. Agreed measures will be factored into implementation plans and will be the responsibility of either the Project Manager or Information Asset Owner to ensure they are completed.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Describe the source of the risk, the problem it creates and the potential impact on individuals.** Focus on data protection compliance risks. Mention corporate risks only as necessary. | **Likelihood of harm** Remote, possible or probable. | **Severity of harm** Minimal, significant or severe. | **Risk score** Low, medium or high. | **Agreed action**Detail to action that will reduce the risk | **Action** **Owner & due date**Name & date | **Residual** **Risk score** Low, medium or high. |
| 1 | *Example: ‘Lack of ‘home address’ date stamp means a pay slip could be sent to the wrong recipient making the individual more vulnerable to becoming a victim of identity fraud’.* |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |

**\*If you have accepted any of the above risks you must provide a rationale for doing so in the ‘Agreed Actions’ column.**

|  |
| --- |
| **6. Authorisation of DPIA:** *See Appendix A, Part 6 for guidance.* |

DPIA copies will be retained by the DPO, Information Asset Owner and within the relevant Project Management records.

1. **Approval signatories**

|  |  |  |
| --- | --- | --- |
| **Item** | **Name / role / date** | **Notes** |
| Risk Reducing Measures approved by **Information Asset Owner:** |  | Integrate actions back into project plan, with date and responsibility for completion  |
| Residual risks approved by **Senior Responsible Officer**:  |  | Acceptance of mitigating actions. |
| Residual risks approved by **XXXXXX** (in consultation with IAO):  |  | If accepting any residual high risk, consult the ICO before going ahead  |
| **Data Protection Officer** approval of DPIA:  |  | DPO should consider any medium / high residual risks and whether processing can proceed  |
| **Summary of DPO advice:**  |

1. **Residual high risks (complete only if there are any ‘high’ residual risks):**

|  |  |  |
| --- | --- | --- |
| **Item** | **Name / role / date** | **Notes** |
| DPO advice accepted or overruled by **Senior Information Risk Owner (SIRO):** |  | If overruling the DPO’s advice you should record your rationale below |
| **SIRO Comments:** |
| **Date and name of person referring DPIA to ICO:** |  | As required by law if any high residual risks remain. |
| **Summary of ICO advice:** |

1. **Accountability – update of ‘records of processing’:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Information Management** **Name / role** | **Information Asset Register** | **Special Category Data Policy Document** | **Notes** |
|  |  |  | Add dates the records were updated. |

1. **Review of DPIA:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Item** | **Information Management****Name / role / date** | **Frequency** | **Notes** |
| DPIA will be kept under review by:  |  |  | How often dependant on the nature of processing & residual risk level |

# Appendix A: Guidance notes for persons completing the DPIA

**How to use this guidance:**

This appendix gives detailed notes to assist persons completing the DPIA. Each numbered section of the DPIA has a corresponding guidance section relating to it within this appendix. The section numbers in DPIA Report and Appendix A guidance will match. The guidance is extensive to provide wide ranging support however; not all parts of the guidance will be relevant to every project. Consider the elements that relate to your individual project.

**Where in the main DPIA report there is text shown in red or text that should be deleted if not relevant – you should remove this text on completion of your DPIA, before submission. Once you have completed the DPIA Report you should remove Appendix A (guidance pages) before submission.**

The intention of this document is to demonstrate transparency and proportionality around how personal data is processed. To that end it is intended for open source publication. There will be an opportunity to redact any commercially or operationally sensitive information and personal information prior to publication.

If you require any further assistance to complete this DPIA report please contact your DPO or Information Governance lead.

**Guidance sections**

|  |
| --- |
| Part 1. Outline of the project and objectives: |

At a high / summary level explain what type of personal data processing is involved along with the primary (and any secondary) objectives of the project. You may find it helpful to refer to your Project Charter or Business Case for a brief / summary explanation.

If this is not a new process but a change to an existing project, system, technology then describe the current process and how the proposed changes will affect this

|  |
| --- |
| **Part 2. Describe the intended use of personal data:** |

There are 4 sections (a-d) to this part, all of which will need to be completed. All necessary guidance is within the template in red text.

|  |
| --- |
| **Part 3. Consultation** |

1. **Consider who you will consult with.**

Decide which of the following groups of stakeholder need to be consulted with and how you might go about it.

* **Individuals whose personal data you are processing:**
	+ the Information Commissioner recommends that you should seek the views of individuals whose data you will be processing (or their representatives) unless there is a good reason not to. In many scenarios this is likely to involve disproportionate effort or may be inappropriate to do so. It may be worth considering whether it is helpful to consult with a liaison body or diversity team instead.
* **Internal stakeholders.**
* **External stakeholders:**
	+ the scope of external consultation should be assessed in the context of the development that is proposed.

Some examples of relevant stakeholders are listed below however it should not be assumed that you would need to consult all listed stakeholders in every project.

|  |  |
| --- | --- |
| **Internal Stakeholders** | **External Stakeholders** |
| Project BoardEngineers, developersICTProcurementCommunications TeamFrontline Staff / OfficersCorporate GovernanceSenior Management | Individuals whose data you process End UsersRepresentative GroupsInterest GroupsGeneral PublicRegulatorsPartnersSuppliers / Data Processors |

1. **Recording your consultation**

In the DPIA you should record a summary of the following:

* the consultation process used;
* which groups you consulted with and their respective views;
* list any key stakeholders you didn’t consult with and the rationale for not doing so;
* if your processing disregards the views of your stakeholders you should record your rationale for doing so.

|  |
| --- |
| **Part 4. Data Protection Compliance – assessment of necessity and proportionality.** |

You will need to look at the personal data being used and your intended data use to assess how it complies with the key principles / requirements of the GDPR and Data Protection Act 2018, as listed below. Your intended use of the data should meet the legislative requirements and where it does not you will likely need to introduce mitigating measures to reduce the risk. The detail provided against the principles below is intended to encourage you to consider the relevant aspects to your intended use - not all will be relevant to each initiative.

What should I record in the DPIA?

There are structured headings to help you and key questions to answer in the main body of the template. The aim is to describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent creeping / growing scope of the processing? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

|  |
| --- |
| **Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.** |
| Consider the following:* Is it necessary to use personal data to achieve your objective?
* You must identify the ‘lawful basis’ for processing each of the following

 (you may need the help of the DPO or IG Lead to identify lawful bases).* + Personal data
	+ Special categories of Personal data
	+ Criminal data
* If you are relying on consent as your lawful basis to process personal data; does it meet the new consent standards (freely given, specific, informed, and unambiguous positive indication of agreement)? How will you help people withdraw their consent if they wish to?
* How will you tell individuals about the use of their personal data?
	+ Are you providing a privacy notice?
	+ Can you provide information verbally as part of an existing process?
	+ Do you need to amend your existing privacy notice to cover new processing of personal data?
	+ Are you exempt from providing privacy notices because it would prejudice the forces ability to prevent / detect / investigate crime?
* If your organisation is subject to the Human Rights Act, you also need to consider:
	+ Will your actions interfere with the right to privacy under Article 8?
	+ Have you identified the social need and aims of the project?
	+ Are your actions a necessary and proportionate response to the social need?
 |

|  |
| --- |
| **Principle 2 - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes** (further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes). |
| Consider the following:* Does your project plan cover all of the purposes for processing personal data?
* Have you identified potential new purposes as the scope of the project expands?
* If your project involves the re-use of personal data already held by the force (i.e.: you are not collecting it before use), you must check that the secondary use is not incompatible with the original reason you collected the personal data. In making this assessment you can consider the following:
* any link between the reason for initial collection and the intended further use;
* the context in which the data was originally collected (in particular the balance of power in the relationship between the individual whose data it is and the force (data controller);
* the nature (sensitivity) of the data – does it involve special categories of data or criminal data;
* the possible consequences to the individuals whose data it is, from the intended further processing;
	+ the existence of appropriate safeguards which may include, pseudonymisation, encryption.
* **If you collected the personal data under the Law Enforcement rules (Part 3 Data Protection Act 2018) and the secondary use is not for the Law Enforcement Purpose (under GDPR rules) - the secondary use of personal data must be authorised under law.** You may need to seek advice from the DPO
 |

|  |
| --- |
| **Principle 3 - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.** |
| Consider the following:* Is the quality of the information good enough for the purposes it is used for?
* You should only use the minimum amount of personal data that is necessary to achieve your objective. You must consider:
	+ can I achieve my objective by only using anonymised data or pseudonymised data;
	+ if the use of personal data is necessary; what personal data could you not use, without compromising the needs of the project (the use of personal data should not be a ‘nice to have’)?
* If you are implementing a new IT system for recording **operational policing data** does it have the following required functionality:
	+ ability to log time / date / user (system audit capability) for the following data activities: recording, amendment, searching, combining / merging, deletion;
	+ is there capability for users to make a note / record of any information form the system that they have shared;
	+ does it have any capability to distinguish factual data from opinion, so far as the context of the data requires;
	+ does it have the ability to categorise the types of individuals where possible: victim, witness, suspect, convicted, other?
 |

|  |
| --- |
| **Principle 4 - Personal data shall be accurate and, where necessary, kept up to date (every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay).** |
| Consider the following:* How are you ensuring that personal data obtained from individuals or other organisations is accurate?
* Does any part of the process make it unlikely that good data quality and accuracy will be achieved? If so how can this risk be removed; process checks, guidance?
* If you are procuring new software does it allow you to amend or append data when necessary? What processes will this entail?
* If you identified inaccurate data for correction, would you be able to identify who the data had been shared with so you could make those organisations aware of the error?
* If the accuracy of personal data were contested by the individual do you have the ability to restrict the use of the data whilst the dispute is being resolved?
* If your project involves integrating or sharing of data sets how will accurate data be ensured by design and once in regular use?
 |

|  |
| --- |
| **Principle 5 - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.**(Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures to safeguard the rights and freedoms of individuals).  |
| Consider the following:* What retention periods are necessary for the personal data you will be processing – are they justifiable? If in doubt consult with the Records Manager.
* Are they in accordance with MoPI retention rules or the NPCC Retention Schedule?
* If you need to keep personal data for prolonged periods; could it be anonymised after a period of time?
* Are you procuring software that will allow you to delete information in-line with your retention periods – ideally in an automated manner?
* If storing paper or electronic records outside of an IT system (unstructured records) have you thought about storing them in a way that makes deletion quick and easy when the time comes?
 |

|  |
| --- |
| **Principle 6 - Personal data shall be 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.** |
| Consider the following:* Do any new systems provide protection against the security risks you have identified?
* If you are transferring personal data to other organisations how can you do this securely?
* Has your new, or changed, system or process been assessed by the Information Security Officer?
* What training and instructions are necessary to ensure that staff know how to operate a new system or process securely?
* What risk management procedures / policies will be in place to prevent any breach or damage/loss of data form occurring? Could include human error, hacking, network failure, theft, destruction of hardware etc.
* How will the force ensure the Data Processor (if used) will also comply with the data protection legislation?
* Are staff aware of the Security Breach reporting process in force and the need to report breaches urgently? Are any new joiners aware?
 |

|  |
| --- |
| **Principle 7 - Personal data shall be processed in accordance with the individual’s data protection rights.** |
| Consider the following:* The individuals whose data you are processing have a suite of data protection rights they can exercise. To support the exercise of these rights does your IT system or process allow for:
	+ easy searching and retrieval of an individual’s records by name, common ID characteristics, or occurrence / event URN;
	+ amending, appending or deleting inaccurate data and restricting its use whilst accuracy is being disputed, until resolved;
	+ manually deleting an individual’s record where their right to erasure has been agreed by the force;
	+ in certain situations provide an electronic copy of an individual’s data.
 |

|  |
| --- |
| **Principle 8 - Personal data shall not be transferred outside the European Economic Area (EEA) without adequate privacy protections being guaranteed.** |
| Consider the following:* Is any personal data being transferred outside the EEA – if so seek advice from the DPO as formal mechanisms to mitigate this risk may be required?
* If using a new or a different IT supplier, understand where the system is hosted, the location of servers with cloud hosting, and the location of supplier’s staff that will provide an IT Support service.
* Does your process involve individuals / users accessing and using personal data via a website where you cannot control their location within the EEA?
 |

|  |
| --- |
| **Principle 9 - The force must be responsible for, and be able to demonstrate, compliance with the data protection principles (1-8 above)** |
| Consider the following:* The force must keep sufficient records to be able to demonstrate that it is complying with data protection legislation. There will be a degree of corporate governance required around your processing and in addition certain types of processing activities will require additional governance:
	+ has the use / flow of data been captured in the forces Information Asset Register or does the existing entry need updating? Check with the Records Manager
	+ if you are using Special Category data or criminal data – is this use covered in the forces Special Category Data Policy Document? Check with the DPO
	+ has an Information Asset Owner been assigned to own the process / data once implemented as ‘business as usual’?
	+ who or what forum will ensure ongoing data protection compliance in BAU?
* If your project / process involves the following arrangements you will need additional governance:
	+ information sharing – will need an Information Sharing Agreement;
	+ use of 3rd party contractors to process force data as a ‘Data Processor’ will require mandatory clauses in the contract;
	+ shared use / access of data held in a single IT system, by more than one organisation, – will require Joint Data Controller MoU;
	+ new IT systems might require a System Operating Procedure so that users understand how to use the new tool and data within it.
 |

|  |
| --- |
| **Part 5. Identifying, assessing and mitigating risks:** |

**Assessing the risk:**

There are 3 factors to consider when assessing the risk:

1. **Impact -** consider the potential impact on individuals; and any harm or damage that might be caused by your processing – whether physical, emotional or material. In particular 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 / social disadvantage (e.g.: loss of public trust)
1. **You should include an assessment of the security risks** (including illegitimate access to, modification of or loss of personal data), including **sources of risk** (e.g.: careless / disgruntled employee, criminal gang, journalist, hacker) and the **potential impact** of each type of breach (the likely consequences of the security breach for the individuals data that have been breached, and the force).
2. **Assessing seriousness of risk:** to assess whether the risk is a ‘high’ risk, you need to consider 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. You might find it helpful to use a structured matrix to think about likelihood and severity of risks:



**Recording the ‘risk statement’:**

When you record the risk in the table in section 5 of the template you should include 3 ingredients in risk statement:

1. What is the source of the risk: (e*g: lack of visible date stamp on the ‘current address field’ means users can’t tell which is the individual’s current home address)*
2. What is the problem that could occur as a result of the risk: *(eg: individuals pay slip could be sent to an old address).*
3. What are the consequences / impact to individuals who the data is about: *(eg: individual could become a victim of identify fraud)*

The resulting risk statement will read:

* ‘Lack of ‘home address’ date stamp means a pay slip could be sent to the wrong recipient making the individual more vulnerable to becoming a victim of identity fraud’.

**Mitigating the risks:**

Identify and record any risk reducing actions or additional measures you could take to either **reduce or eliminate** risks identified as **medium or high** risk in section 6. Risk numbering in this section should correspond with risk numbers in section 6 above.

For each risk you should consider options for reducing that risk. The below list is not an exhaustive list of risk reducing measures but might be useful to consider relevant options. The DPO will provide you with some advice and you may be able to devise other ways to help reduce or avoid the risks:

* 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;
* adding a human element to review automated decisions;
* 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.

You can take into account the costs and benefits of each potential measure when deciding whether or not they are appropriate. Record the measures you are likely to adopt in the table in section 7 and also record whether it has been agreed that they will be adopted.

**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. **However, if there is still a high residual risk, you must consult the force’s Data Protection Officer who may refer the DPIA to the ICO before you can go ahead with the processing (this is a legal requirement).**

|  |
| --- |
| **Part 6. Authorisation of the DPIA and its recommendations:** |

As part of the sign-off process, the Data Protection Officer must assess the DPIA and advise as to whether the processing is compliant and can go ahead. If there are any high residual risks the Senior Information Risk Owners views should be sought and the DPIA must be referred to the Information Commissioners Office for advice.

You will also need to confirm that the information about the intended processing has been updated in the Information Asset Register.

Appendix B: The Regulation Explained

The GDPR requires a data controller to implement appropriate measure to ensure and be able to demonstrate compliance with the GDPR, taking into account among others the “the risk of varying likelihood and severity for the rights and freedoms of natural persons”

Article 35 GDPR - Data Protection Impact Assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

1. 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;

2. processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

3. a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. 2The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. 2The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

1. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

2. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

3. an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.