Data Protection Impact Assessment Policy

Version: 1.1

Published: 01/02/2021

DOCUMENT CONTROL

Approval Table

Authority	Name / Role
Author	Melissa Ashdown-Hoff/ Information Governance Officer
Document can be reviewed by	Information Governance Officer
Document can be approved by	Executive Management Team

Document Identification

Document Title	Data Protection Impact Assessment Policy
Version Number	1.1
Date:	01/02/2021
Total Number of Pages:	8
Security Marking	OFFICIAL

Version History

Version No.	Version Issue Date	Authored / Revision by	Approved by	Reason
1.1	01/02/2021	MAH	JR	Legislation updated to reflect EU Exit and referenced to GDPR replaced with UK GDPR.

Contents

1. Introduction

1.1. The General Data Protections Regulation place an emphasis on accountability and data protection by design. This means that privacy considerations and data subject's rights should be at the forefront of an organisations planning, thinking, decision-making and design.

1.2. The Office of the Police and Crime Commissioner for West Yorkshire (OPCC) is committed to being accountable and protecting the rights of individuals with regard to the processing of their personal data. This policy is intended to embed a Data Protection by Design approach to OPCC activities by mandating the use of Data Protection Impact Assessments at appropriate points in the OPCC's operational planning, project management, procurement and commissioning workflows.

2. Legislation

2.1. **The General Data Protection Regulation** (GDPR) update and replace the previous EU Directive and Data Protection Act. GDPR provides a stronger protection to individual's personal data. It give individuals more rights and control over their personal data and increases the penalties on organisations for non-compliance. Accountability is at the heart of the GDPR and the OPCC must be able to demonstrate how it complies with the GDPR. The GDPR covers the processing of all personal information whether it is processed on computer, CCTV, manual-filing records, digital, or any other media. The GDPR does not apply to the processing of personal data for specific law enforcement Purposes.

2.2. **The Data Protection Act 2018** compliments the GDPR. It completes data protection law where the GDPR made space for individual countries to define their own legislation. It details the exemptions where the GDPR provisions do not apply. The Act details the powers of the Information Commissioner and clarifies some of the terms used in GDPR. Part 3 of the The Data Protection Act Implements the Law Enforcement Directive.

2.3. **The Law Enforcement Directive** covers the processing of personal information by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences. The OPCC is not a competent authority and all processing done by the OPCC is bound by GDPR and the Part 2 of Data Protection Act.

2.4. **The European Union Withdrawal Act 2018** directly incorporated all direct EU Legislation including the GDPR into UK Law upon the UK's Exit from the European Union.

2.5. **The Data Protection, Privacy and Electronic Communications (Amendment etc.)(EU Exit) Regulation** to be known as **UK GDPR** amended the GDPR in as far as it applies to the UK and the Data Protection Act 2018**.** The UK GDPR removes references to Members States and bodies such as the European Data Protection Board and replaces them with their UK equivalents.

3. Definitions

3.1. **Personal data** is defined as information which relates to a living individual who can be directly or indirectly identified from the data available, e.g. name, address, postcode, vehicle registration mark (VRM), ID number, payroll or collar number location data, online identifier (IP address and cookie identifier), photographic/video image, in particular by reference to an identifier. It also includes any expression of opinion about an individual and any indication of the intentions of the data controller or any other person in respect of the individual.

3.2. **Special Category data** relates to an individual's health, sexual life or orientation, racial or ethnic origin, religious beliefs, political opinion, Trade Union membership, genetic data and biometric data used for identification purposes

3.3. **Processing** in relation to personal data means the obtaining, recording, holding or performing any operation on the personal data and applies to both manual and computerised records.

3.4. **Data Subject**, the individual to whom the personal data relates.

3.5. **Data Controller** a person or organisation which determines the purpose for which and the manner in which personal data are to be processed.

3.6. **Data Processor** is any person or organisation who processes data on behalf of the controller.

4. Data Protection Impact Assessment

4.1. Data Protection Impact Assessments (DPIA) are a tool intended to allow colleagues to work through the privacy risks a particular processing activity creates for data subjects, our community, our partners and our organisation. They are designed to enable colleagues to identify, fix, mitigate or minimise the privacy issues within a range of projects or processing activities at early stage.

4.2. Identifying privacy issues early means simpler and less costly solutions can be found. It also enables the OPCC to avoid the potential for reputational damage later on. They can help build trust with our communities, partners, volunteers and colleagues by showing that we consider their privacy rights at the earliest and every opportunity.

4.3. DPIA's are mandatory before you begin any processing which will have a widespread and serious impact on the privacy rights of individuals.

4.4. Specifically, UK GDPR states that you will need to carry out a DPIA where you plan to: use systematic and extensive profiling with significant effects; process special category or criminal offence data on a large scale; or systematically monitor publicly accessible places on a large scale.

4.5. The Information Commissioner also requires you to do a DPIA if you plan to do any of the following:

- use new/ novel technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric or genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behavior;
- profile children or target services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

4.6. Where a full assessment is required it must describe the processing and the purpose for the processing, assess the necessity and proportionality, identify the risks to individuals and identify any measures to mitigate those risks and protect the data.

The OPCC has developed a three stage DPIA Process.

5. Stage 1 - Data Protection Impact Screening Tool.

5.1. All new activities, decisions, projects, policies, commissioning, procurement or operation must be assessed through the Data Protection Screening Tool (See Appendix 1) at the earliest possible planning stage.

5.2. The Data Protection Impact Screening Tool will indicate to colleagues and the Executive if their proposed activity, decision, policy, commissioning, procurement or operation will require a full DPIA to be undertaken.

5.3. Colleagues must keep a record of the screening form as it will be need to be submitted to senior leaders when the activity, policy, policy procurement or commissioning requires sign off or before any activity is operational.

5.4. A copy of the completed screening form must be returned to the Information Governance Officer (IGO) by email to DPO@westyorkshire.pcc.pnn.gov.uk who will maintain a record of the screening forms completed by colleagues.

5.5. The IGO will every 3 months review the number and frequency of the screening forms submitted from across the OPCC to identify any gaps in submissions.

5.6. The IGO will produce a 3 monthly report to the Executive detailing the number of screening forms submitted per department. Departmental heads will be asked to comment formally on/ explain the reasons for any gaps.

6. Stage 2 - Full Data Protection Impact Assessment

6.1. It is always preferable that where a project requires a full DPIA that this is done at the earliest possible stage of any activity.

6.2. You can find the full DPIA form at Appendix 2. There is lots of helpful information within the form, which should enable you to identify the information about your project, which needs to be considered and recorded. If you need any advice or assistance please contact the (IGO) at DPO@westyorkshire.pcc.pnn.gov.uk.

6.3. You will need to consider carefully and objectively the risks that the processing you are proposing creates for individuals, our communities and the OPCC.

6.4. Once completed return the form to the IGO by email at DPO@westyorkshire.pcc,pnn,gov.uk/

6.5. The IGO will assess the information provided on the DPIA and if necessary ask for further information or clarification where required. The IGO may provide advice to colleagues that a further assessment of the risks involved is required or provide advice on other mitigations to be considered.

6.6. When the IGO is satisfied that the data protection risks have been fully assessed and any risks identified have had appropriate mitigations put in place to reduce the risks to an acceptable level the IGO will recommend the DPIA for sign off by the Data Protection Officer (DPO).

6.7. Where the IGO has identified that the risks have been fully assessed and the mitigations detailed are not sufficient to reduce the risks to an acceptable level the IGO will refer the assessment up to the DPO for further consideration.

6.8. The DPO will liaise with colleagues to further examine the risks involved and identify any further mitigations. Only when the DPO is satisfied that the risks have been reduced to an acceptable level will the DPO approve the project, policy, activity, procurement commissioning exercise for the next stage of sign off.

6.9. Any mitigations identified must be integrated back into the project delivery plan, and should be kept under review to ensure they are working effectively to minimise the risks.

6.10. Where high risks have been identified that cannot be mitigated the OPCC must consult the Information Commissioner (ICO) before the activity can commence. The ICO will provide formal advice between 8-14 weeks and can issue a formal warning not to process the data or ban the processing altogether.

6.11. All activities where the screening tool has identified that a DPIA is mandatory must be signed off by the DPO prior to the commencement of the processing activity. Any processing of personal data which occurs without sign off will be in breach of the UK GDPR, and could result in large fines being imposed on the OPCC, damage the reputation of the OPCC, and put at risk individuals personal data.

6.12. The IGO will every 3 months review the number and frequency of DPIA's submitted to identify any gaps in submissions.

6.13. The IGO will keep a record of all DPIAs submitted and will produce a 3 monthly report to the Executive detailing the number of DPIA's submitted per department. Departmental heads will be asked to comment formally on/ explain the reasons for any gaps.

7. Stage 3 - Record and Review

7.1. The IGO will record the details of each Screening Tool and DPIA submitted in a secure database and each will be assigned a unique reference number.

7.2. The record will detail all mitigations identified in the DPIA's and these will be reviewed prior to the commencement of the project and biannually there after to ensure that the mitigations are effective in reducing the identified Data Protection risk.

7.3. The DPIA reference number will recorded in the Record of Processing Activities.

This form is Stage 1 of the Data Protection Impact Assessment (DPIA) process. You are advised to read the Data Protection Impact Assessment Policy found here before completing the form.

Project/ Activity name & brief description	
OPCC Department	
Your Name	

Does the proposed project, plan, activity, decision, procurement, operation or commissioning activity involve you or another party processing the Personal Data of a living identifiable individual?	Yes/No

If no personal data is being processed a Data Protection Impact Assessment will not be required. However, you will need to keep a copy of this form for your project records and forward to DPO@westyorkshire.pcc.pnn.gov.uk

If you answered yes to the question above please complete the rest of this form.

Please answer the following questions about the proposed activity, will it:	
Use special category data or criminal offence data on a large scale.	Yes/No
Involve information about individuals being disclosed or shared with organisations or people who have not previously had routine access to the information.	Yes/No
Systematically monitor a publicly accessible place on a large scale.	Yes/No
Use systematic or extensive profiling which has significant effect on individuals or profile individuals on a large scale.	Yes/No
Involve the use of personal data with new technologies or the novel use of existing technologies (will include the use of AI and facial recognition).	Yes/No
Use profiling on, special category or law enforcement data to decide on access to services.	Yes/No
Process genetic or biometric data.	Yes/No
Involve data matching, combining, comparing or matching personal data from different sources.	Yes/No
Involve invisible processing, where personal data is collected from a source other than the individual without providing them with a privacy notice, including the repurposing of information collected for one purpose for a new purpose.	Yes/No
Track individuals location or behaviour.	Yes/No
Target children or vulnerable adults, using the personal data of children or vulnerable adults for marketing purposes, profiling or other automated decision-making, or offering online services directly to children.	Yes/No
Process data that might endanger an individual's physical health or safety in the event of a security breach.	Yes/No
Have you identified that the processing poses a high risk to the privacy, rights or freedoms of individuals.	Yes/No

If you answered No to all the questions above a DPIA is not required. You will need to keep a copy this form for your project records. and forward to DPO@westyorkshire.pcc.pnn.gov.uk

If you answered yes a DPIA will be required please complete Section 2. Please contact the Information Governance Officer for advice and assistance.

Definitions

Personal Data is defined at information, which relates to a living individual from which the individual can be identified either directly or indirectly. It will include name, address, and email address. Identification numbers including national insurance number, NHS number, collar number or payroll number and online identifier such as IP address or cookie identifier, location data.

Special Category Data is information about a living identifiable individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, sex life or sexual orientation.

Profiling is where an analysis takes place by automated means of an individual's personality, behaviour, interests and habits to make predictions about them. This can include making predictions about their performance at work, economic situation, health, personal preferences, interests, reliability, and behaviour, an individual's risk of offending or becoming a victim, location or movements. You are carrying out profiling if you:

- collect and analyses personal data on a large scale, using algorithms, AI or machine-learning;
- identify associations to build links between different behaviors and attributes;
- create profiles that you apply to individuals; or
- Predict individuals' behavior based on their assigned profiles.

Large scale processing. When assessing if your processing activity is large scale the following data may be helpful. WYP has approx. 8,500 Officers and Staff and the OPCC has approximately 75 staff. The population of West Yorkshire is approximately 2.3 million and there is a large transient population. Processing would be considered large scale if it involves over 100 officer/ staff/ colleagues or more than 5000 individuals.

Please forward the completed form to the Information Governance Officer at DPO@westyorkshire.pcc.pnn.gov.uk

Office of the Police & Crime Commissioner for West Yorkshire DPIA Template

Whenever the OPCC processes personal data it creates risks to the individuals from that processing. Data Protection Impact Assessments are a useful tool to assess record and mitigate the risks that our processing causes. Please complete the screening tool found here and read the Data Protection Impact Assessment Policy found here before completing the rest of this form.

Guidance

When completing your assessment you will need to show how the processing/ using the personal data complies with the six Data Protection Principles which state that Personal Data must be:

- **Processed fairly, lawfully and in a transparent manner.**
- **Collected for specified, explicit and legitimate purposes and not further processed**
- **Adequate, relevant and limited to what is necessary**
- **Accurate and kept up to date**
- **Kept for no longer than is necessary**
- **Kept in a manner which ensures appropriate security**

In addition, you will need to specify your **lawful basis** for the processing from the following:

- **Consent – the individual has given clear consent to you to process their data for a specific purpose**
- **Contract – information necessary for a contract you have or are looking to have with the individual**
- **Legal obligation – information is necessary for you to comply with the law**
- **Vital Interest – information is necessary to protect someone's life**
- **Public task – information is necessary to perform a task in the public interest/ or basis in law**
- **Legitimate interest – information is necessary for your or a third parties legitimate interest**

Key Terms

Personal Data is defined at information, which relates to a living individual from which the individual can be identified either directly or indirectly. It will include name, address, and email address. Identification numbers including national insurance number.

Special Category Data is information about a living identifiable individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, sex life or sexual orientation.

Profiling is where an analysis takes place by automated means of an individual's personality, behaviour, interests and habits to make predictions about them. This can include making predictions about their performance at work, economic situation, health, personal preferences, interests, reliability, and behaviour, an individual's risk of offending or becoming a victim, location or movements. You are carrying out profiling if you:

- collect and analyses personal data on a large scale, using algorithms, AI or machine-learning;
- identify associations to build links between different behaviors and attributes;
- create profiles that you apply to individuals; or
- Predict individuals' behavior based on their assigned profiles.

Artificial Intelligence (AI) is an umbrella term for a range of technologies and approaches that attempt to mimic human thought to solve complex tasks, in policing AI is increasingly being used to target interventions and identify potential offenders and victims.

Automated Decision Making is where the process of making a decision is done so by solely by automated means without any human involvement.

Step 1: Assessment Administration

Version Control

DPIA Reference	Get Reference from Information Governance Officer	**Project Title:**		
Version	**Status**	**Revision Date**	**Summary of Changes**	**Author**

Sign Off & Outcomes

Item	**Name/date**	**Notes**
Measures approved by:		Integrate actions back into DPIA Log 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, step 5 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

Step 2: Identify the need for a DPIA

Please identify which of statements A-M best describe the need for a DPIA (please delete statement which are not applicable):

A. The use of **special category or criminal offence data** on a large scale.

B. Involve **sharing information** with organisations or people who have not previously had routine access to the information.

C. Systematically **monitor publicly accessible places** on a large scale.

D. Use systematic or **extensive profiling** which has a significant effect on individuals or profile individuals on a large scale.

E. Processing involving the use of **new technologies**, or the novel application of existing technologies (including Artificial Intelligence, facial recognition).

F. Use **profiling on special category or law enforcement data** to decide on access to services

G. **Biometrics** and **Genetic data** - any processing of biometric or genetic data, other than that processed by an individual GP or health professional for the provision of health care.

H. **Data matching** - combining, comparing or matching personal data obtained from multiple sources.

I. **Invisible processing** where personal data is collected from a source other than the individuals without providing them with a privacy notice.

J. **Tracking** - processing which involves tracking an individual's location or behavior

K. **Targeting of children or other vulnerable individuals** - the use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.

L. **Risk of physical harm** - where the processing is of such a nature that a personal data breach could jeopardise the physical health or safety of individuals.

M. **Other,** where you have identified that the use of the data poses a high risk to the privacy, rights and freedoms of individuals in some way – please detail

This DPIA is an assessment of a current Processing activity, which has changed scope / context, or a Pre UK GDPR Processing activity.	Yes/No
This DPIA is an assessment of intended processing activity	Yes/No
The relevant Privacy Notice, consent/ data capture forms or any other documentation are attached	Yes/No

Step 3: General Project Details

Name: (of the project or change to be delivered)	
Background/ Objectives: (why is the new system / change required?)	

Information flow diagram* (Information flow Diagrams are available here if this project relates to a new information flow please contact the OPCC Information Governance Officer)		
State who is the Data Controller		
Benefits: (explain what the project aims to achieve, what benefits to the OPCC, to individuals and to other parties)		
Consultation: (If required detail here any consultation undertaken with the public, partners, internal or external stakeholders: think about consultation with the following: The individuals affected, the public, Campaign Groups, Trade Unions, Information Governance Officer, Data Protection Officer, Information technology, West Yorkshire police, Partner agencies, Ethics Committee, Human Resources)		
Implementation date: for example the timescales required for completion, implementation date		
Relationships / Partnerships: (e.g. with West Yorkshire Police, Victims services, Third sector or private organisation, stakeholders, please also if possible state whether they are designated as data controllers or data processors)		
Project Manager:	Name:	
	Job Title:	
	Service:	
	Telephone:	
	Email:	
Information Asset Owner(s) All information assets must have an information asset owner (IAO). IAO are usually the Head of your department.	Name:	
	Job Title:	
	Service:	
	Telephone:	
	Email:	

Step 4: Data Protection Impact Assessment

	Question	Response	Guidance document
Processing			
1	Please state the purpose for the processing of the data / information: (for example, service provision, research, audit, employee administration)		
2	Please tick the data items/ information that will be processed	☐Name ☐Address/Postcode ☐Date of Birth ☐Email ☐Telephone no/email ☐Next of Kin ☐National Insurance Number ☐Employee Number ☐Image ☐Gender ☐Pseudonymised	Lawful Basis Applicable: Consent Contract Legal obligation Vital Interest Public Task Legitimate Interest
2b	Special categories and Criminal data	☐Sexual Orientation ☐Political opinions/trade union membership ☐Religion ☐Physical health ☐Mental health ☐Medical history ☐Ethnic Origin ☐Sexual life ☐Criminal conviction ☐Criminal offence ☐Police Incident ☐Custody data ☐Victim/witness data	Lawful Basis Applicable: Explicit Consent Employment Vital Interests Legitimate Activities Not for Profit Made Public by Data Subject Defence of Legal Claims Substantial Public Interest Occupational Health Public Health Archiving, Research & Statistics
2c	Other (please specify)		
3a	What is the legal basis you are relying on for the processing of the data/information? (please see guidance section above for all of question 3)		

3b	If you are relying **only** on consent, did you consider any other legal basis?	☐Yes ☐No	
3c	If using consent, how will that consent be obtained and recorded and withdrawn if requested? (please state)		
4	Will personal data items be collected which have not been collected before?	☐Yes ☐No	
5	The data of approximately how many individuals will be affected?	☐1-10 ☐10-100 ☐100-1000 ☐1000-10,000 ☐10,000+	
6	How is the personal data obtained?	☐From individual directly ☐From partner agencies ☐From 3rd Party/ Another Individuals ☐For employment purposes ☐Internal services ☐Other	
7	Have the individuals been informed of this processing?	☐Yes (explicit) ☐Yes (implicit i.e. through Privacy notice, website, leaflet etc) ☐No	If no please record as risk in Step 5
8	Does the information involve new linkage / matching of personal data with data in other collections, or is there significant changes in data linkages / matching?	☐Yes ☐No	If yes please record as a risk in Step 5
9	Does this project involve utilising data for the purposes of automated decision making, artificial intelligence or profiling? If so add details (please see guidance section above)	☐Yes ☐No	Please see guidance above
Records Management			
10	Does this project create a new Information Asset?	☐Yes ☐No	

10a	How will the information be kept up to date and checked for accuracy and completeness?		If there are no documented procedures to evidence this answer, please record as a risk in Step 5
10b	What processes are in place for data quality checking?		
11	If this project involves a new system, does it have the ability to quarantine information/restrict processing? (Contact OPCC Information Governance if required)		This is to comply with the data subjects rights of Restriction and Objection.
11a	Does the system have the ability to amend or add notes to data/information at a single data field level? (Contact OPCC Information Governance if required)		This is to comply with the data subjects rights of Erasure, Rectification.
12	What checks have been made regarding the adequacy, relevance and necessity for the collection of data?		This is to comply with the Data Minimisation principle of UK GDPR. Do your plans help you achieve your purpose? Is there another way to achieve the same result using less or no personal data? If no checks have been made please record this as a risk in Step 5
13	Where will the information be stored / accessed? (please see guidance section 4 for further information about cloud storage)	☐ Shared Network Drive ☐ Infoshare ☐ OPCC email system ☐ Paper filing system ☐ Removable media ☐ External to OPCC (cloud, web hosted) ☐ other	
14	What are the retention periods?		If there are no documented retention periods please record as a risk in Step 5
15	How will the information be destroyed when it is no longer required?		
15a	If held electronically, can the destruction be certified?		

15b	Can the information be deleted.	☐Yes ☐No	
Security			
16	Who will access the information? (i.e. Services, roles, organisations)		
17	Is there an Access Control Policy in place? (Please see guidance section 6 for further information)	☐Yes ☐No	
18	Is there an ability to audit access to the information? (Please see guidance section 6 for further information)	☐Yes ☐No	If no please record as a risk in Step 5
19	Detail what security measures have been implemented to secure access and limit the use of personal information?		
20	Does this project involve privacy invasive technologies such as AI, Facial Recognition, Large Scale Profiling, use of CCTV on a large scale? (Please see the guidance)	☐Yes ☐No If yes please detail	
21	Is there a business continuity and a disaster recovery plan in place?	☐Yes ☐No	If no please record as a risk in Step 5
22	Where external parties are accessing OPCC information has it been identified that they require Data Protection training?	☐Yes ☐No	
Sharing			
23	Will any of the information be shared with other organisations or OPCC Departments?	☐Yes ☐No	If yes please record as a risk in Step 5
23a	Please list all organisations/OPCC services involved with sharing		

23b	What is the legal basis for sharing?		Please note that your legal basis for processing may be different from your legal basis for Sharing. Please refer to guidance
24	Will there be signed information sharing agreements in place	☐Yes ☐No	If no please record as a risk in Step 5
25	Which method will be used to transport information if it is going off site?	☐Standard email ☐Secure email (e.g. GCSx) ☐Website ☐Via courier ☐By hand ☐Via external post ☐Via telephone ☐ Removable Media ☐ Secure file transfer protocol (eg. mail express) ☐ Other file transferring applications (dropbox) ☐ Social Media ☐ Providing access via OPCC systems ☐ Other (please give details)	If no please record as a risk in Step 5
26	Are you transferring any personal identifiable data/information to a country outside the United Kingdom	☐Yes ☐No	If yes please record as a risk in s Step 5

Step 5: Identify the information, privacy and related risks

Identify the key risks. Consider and detail the potential impact on individuals and any harm or damage that might be caused by your processing – whether physical, emotional or material. You should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach All risks identified from the questionnaire in step 4 should be included, plus any others of relevance. Describe the actions you could take to reduce the risks and any future steps which would be necessary (e.g. the production of new procedures or future security elements for systems).

Risk *The following are for example only. Please consider carefully and objectively given the type and volume of information you are processing and what your project involves where the risks lie in the processing and what risks this poses to individuals.* • *Data Breach Risk* • *Inability of individuals to exercise their 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;*	**Solution** *The following are examples of some of the solutions which may be considered for reducing the risk.* • *deciding not to collect certain types of data;* • *reducing the scope of the processing;* • *reducing retention periods;* • *additional technological security measures;* • *training staff* • *anonymizing or pseudonymising data* • *writing internal guidance to avoid risks;* • *using a different technology;* • *putting data sharing agreements into place;* • *making changes to privacy notices;* • *offering individuals the chance to opt out* • *implementing new systems to help individuals*	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution justified, compliant and proportionate response to the aims of the project?