

Data Protection Impact Assessment - Template



Please refer to the ICO Data Protection Impact Assessment advice at the following link before completing the template below:

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/>

Key Contacts	
Project Manager Name & Job Title:	Claire Dempster Senior Officer – Domestic Abuse Strategy & Interventions
Project Manager Email:	Claire.dempster@bedford.gov.uk
Project Manager Phone:	Internal: 49220 DD Tel: 01234 718600
Key Stakeholder Names & Roles:	MARAC Core Agencies listed below
Date:	
Are there any other organisations involved in this project? (Yes / No) If Yes please provide details of the other organisations involved	Yes Bedford Borough Council Children’s Services – Children’s Social Care & Early Help Bedford Borough Council Adult Social Care Bedford Borough Council Housing Bedford Women’s Centre Bedford Hospital – Community Midwife Team Bedford Borough Community Safety Partnership


Data Protection Impact Assessment - Template

	<p>Bedfordshire CCG</p> <p>Victim Support - IDVA Service</p> <p>Bedfordshire National Probation Service</p> <p>BPHA</p> <p>Bedfordshire Police</p> <p>Early Childhood Partnership Bedford – covering therapeutic Support services for women and children and also perpetrator services</p> <p>Pathway to Recovery Bedford</p> <p>CCS 0-19 Service</p> <p>Stonewater Housing</p> <p>ELFT</p> <p>IMPAKT resettlement project</p>
<p>Are there any links to other projects?</p>	<p>No</p>

Key Information – please be as comprehensive as possible.

<p>Project Name:</p>	<p>Multi-Agency Risk Assessment Conference (MARAC)</p>
<p>Description of project: Please include the project objectives and deliverables</p>	<p>MARAC is a national project and is run in every local authority within the UK. SafeLives are a national domestic abuse charity who provide advice, guidance/protocols and training for running MARAC meetings.</p> <p>MARAC is a multi-agency risk assessment conference – which is an information sharing meeting for high risk victims of domestic abuse. At the meeting the core agencies listed above will share relevant and proportionate information to those within the meeting for the purposes of protecting victims experiencing domestic abuse, safeguarding children who are within the family and are also classed as victims of domestic abuse and addressing/deterring perpetrator behaviour to reduce the risks of further criminal offences being committed.</p>

Data Protection Impact Assessment - Template

	<p>The aim of MARAC is to improve the safety, health and well-being of victims – adults and their children and this is achieved through sharing information about the risks faced by these victims, the actions needed to ensure safety and the provisions available locally are shared and used to create a risk management plan involving all agencies.</p> <p>MARAC will use data to reach safe decisions about the people referred to MARAC and their families. The data may be used by the sharing partner agencies in different ways: the Police may determine if any of the details reach the threshold to initiate or contribute to a Police investigation. Children's Services and Adult's Social Care may also consider if these details reach the threshold for a referral to their service in order to protect children, young people and vulnerable adults. This sharing is in order to increase the safety of all victims, including children, enable the protection of vulnerable people and reduce crime and disorder locally.</p> <p>There is in place a MARAC Information Sharing Agreement which is signed by all core agencies listed above which set out the legal grounds for information sharing between all agencies who have agreed to work together within the MARAC framework in accordance with the relevant legislation. (See ISA below).</p> <div style="text-align: center;">  <p>BBC Marac Information Sharing A</p> </div> <p>Through the expert guidance of SafeLives, we have developed effective, efficient, mutually beneficial and necessary working partnerships with the organisations within MARAC who all have a lawful basis for seamlessly sharing data. The protocol is reviewed regularly by the MARAC Steering Group and changes implemented accordingly.</p> <p>There is a statutory duty to deliver MARAC under partner duties within the following Acts:</p> <ul style="list-style-type: none"> • Housing Act 1996; • Mental Health Act 1983; • Health and Social Care Act 2001; • Education Act 1996; • Children's Act 1989; • NHS and Community Care Act 1990; • Sex Offenders Act 1997 • Care Act 2014 • Anti-Social Behaviour Crime and Policing Act 2014 • Mental Capacity Act 2005 • Protection of Freedom Act 2012 • Serious Crime Act 2015
--	---

Data Protection Impact Assessment - Template

Will the project involve any data from which individuals could be identified (including pseudonymised data)? (Yes/No)	Yes
Is the data about individuals being shared with the other organisations? (Yes /No)	Yes

IF NO THEN YOU DO NOT NEED TO ANSWER ANY FURTHER QUESTIONS AND A PIA IS NOT REQUIRED.

Screening Questions	YES or NO
Will the project involve the collection of new information about individuals?	Yes
Will the project compel individuals to provide information about themselves?	No
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Yes
Are you using information about individuals for a new purpose or in a new way that is different from any existing use?	Yes
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	No
Will the project result in you making decisions about individuals in ways which may have a significant impact on them? e.g. service planning, commissioning of new services	Yes
Is the information to be used about individuals' health and/or social wellbeing?	Yes
Will the project require you to contact individuals in ways which they may find intrusive?	No

Data Protection Impact Assessment - Template

If any of the screening questions have been answered "YES", then please

continue with the Privacy Impact Assessment Questionnaire (below).

If all questions are "NO", please return the document to the Information Governance Team and **do not** complete any more of this Data Protection Impact Assessment. Please email the completed screening to: dpo@bedford.gov.uk

About the Data to be Used

Use of personal information			
Description of data:			
Personal Data	Please Tick All that Apply	Special Category Personal Data	Please Tick All that Apply
Name	<input checked="" type="checkbox"/>	Racial / ethnic origin	<input checked="" type="checkbox"/>
Address (home)	<input checked="" type="checkbox"/>	Political opinions	<input type="checkbox"/>
Postcode	<input checked="" type="checkbox"/>	Religious beliefs	<input checked="" type="checkbox"/>
Email address	<input checked="" type="checkbox"/>	Trade union membership	<input type="checkbox"/>
Date of birth	<input checked="" type="checkbox"/>	Physical or mental health	<input checked="" type="checkbox"/>
National Insurance Number	<input type="checkbox"/>	Sexual life	<input checked="" type="checkbox"/>
Payroll number	<input type="checkbox"/>	Criminal offences	<input checked="" type="checkbox"/>
Driving Licence [shows date of birth and first part of surname]	<input type="checkbox"/>	Biometrics; DNA profile, fingerprints, audio	<input type="checkbox"/>
(if Documentary Evidence is required)		Bank, financial or credit card details	<input type="checkbox"/>
		Child Protection data	<input checked="" type="checkbox"/>
		Safeguarding Adults data	<input checked="" type="checkbox"/>
		Tax, benefit or pension records	<input type="checkbox"/>
		Health, adoption, employment, school, Social Services, housing data	<input checked="" type="checkbox"/>
Additional data types (if relevant)	Passport (for documentary evidence)		
Who will be providing the personal information? Select as many as you want.		Please Tick All that Apply	
The person whose information it is		<input checked="" type="checkbox"/> Shared with the professional who they have disclosed the domestic abuse to and then the professional	

Data Protection Impact Assessment - Template

	or the professional's MARAC representative makes a subsequent referral into MARAC based on the information provided
A parent or guardian	<input checked="" type="checkbox"/> will share information with service providers or children's services and this information where relevant will be shared with core agencies at MARAC
A non-parent/guardian relative	<input checked="" type="checkbox"/> will share information with service providers or children's services and this information where relevant will be shared with core agencies at MARAC
Some other third party individual	<input checked="" type="checkbox"/> another agency who may have involvement with the family, but is not classed as a core agency at MARAC
A third-party vendor collecting directly – What / who is the third party Do we have a contract with them?	<input checked="" type="checkbox"/> Core Agencies attending MARAC who may be working with any of the parties involved eg victim, child, perpetrator or other adult
A third-party aggregation service	<input type="checkbox"/>
A sensor or device (camera, location sensor, etc.)	<input type="checkbox"/>
Other – Please complete full details:	<input type="checkbox"/>
Please Tick All that Apply	
In what format will the data be collected? Select as many as you want	
Paper form	<input checked="" type="checkbox"/>
Online form	<input checked="" type="checkbox"/>
Mobile app	<input type="checkbox"/>
Video	<input type="checkbox"/>
Audio	<input type="checkbox"/>
Submitted document digital	<input checked="" type="checkbox"/>
Submitted document paper	<input type="checkbox"/>
Other, if so then please give details:	<input type="checkbox"/>



Data Protection Impact Assessment - Template

How and where will the data be stored? Select as many as you want.	Please Tick All that Apply
Hard copy in file unlocked	<input type="checkbox"/>
Hard copy in file, locked	<input type="checkbox"/>
Digital file, in folder, unencrypted device	<input type="checkbox"/>
Digital file, in folder, encrypted device	<input type="checkbox"/>
Digital file, in folder, on server, no password	<input type="checkbox"/>
Digital file, in folder, on server, password	<input type="checkbox"/>
Digital file, in cloud, common user/pass	<input type="checkbox"/>
Digital file, in cloud, individual user/pass	<input type="checkbox"/>
Database, unencrypted device	<input type="checkbox"/>
Database, encrypted device	<input checked="" type="checkbox"/>
Database, on server, no password	<input type="checkbox"/>
Database, on server, password	<input checked="" type="checkbox"/>
Database, in cloud, common user/pass	<input type="checkbox"/>
Database, in cloud, individual user/pass	<input checked="" type="checkbox"/>
Other, please give full details Modus is hosted at a secure data centre in the UK (for more information on the hosting provider including all ISO accreditation click here). All data transmitted to and from the site is encrypted with 256bit SSL. Access to Modus requires a username and strong password; Paloma staff are all DBS checked with nominated staff receiving enhanced Police vetting and all staff are required to sign confidentiality agreements.	<input type="checkbox"/>
How long will the data be retained?	Please Tick All that Apply
For a set period of time we have already determined	<input checked="" type="checkbox"/>
Please state retention period	<input type="checkbox"/> 7 years after the last MARAC meeting held.
Supplier of the information has opportunity to delete	<input type="checkbox"/>
Third party only allows us to keep for set time	<input type="checkbox"/>
Indefinitely	<input type="checkbox"/>
Other	<input type="checkbox"/>
How many staff process this data?	All core agencies attending MARAC are joint controllers as opposed to processors, the processors will be within individual organisations

**Data Protection Impact Assessment -
Template**

Information Governance & Compliance for data processing

What is the justification for the inclusion of identifiable data rather than using de-identified/anonymised data?

Safeguarding individual victims, children and families who are experiencing domestic abuse. This would not be possible to achieve if we were not able to use identifiable data

If we were unable to identify individual perpetrators who are carrying out the domestic abuse, we would not be able to implement a robust safety plan to protect the victims or put actions in place to deter the behaviour or prevent further crime.

This sharing is in order to increase the safety of all victims, including children, enable the protection of vulnerable people and reduce crime and disorder locally.

Case discussions will focus how best to support victims and deal with offenders. Disclosure of personal information and sensitive personal information must be decided on a case-by-case basis to ensure that the disclosure is necessary to support action under the Crime and Disorder Act 1998, is proportionate, and the public interest is of sufficient weight to override the presumption of confidentiality.

The public interest criteria will include:

- The prevention of crime and disorder
- The detection of crime
- The apprehension of offenders
- The protection of vulnerable members of the community
- Maintaining Public Safety
- The administration of Justice

Have there been any legislation changes that have requires the new/change in processing?

If yes, please state the legislation change?


DPA 2018

UK GDPR

Will the information be new information as opposed to using existing information in different ways?

The information will be new on each occasion that the case is heard at MARAC, but will also involve looking at historical information to determine future risks and patterns of behaviour

**Data Protection Impact Assessment -
Template**

<p>What governance measures are in place to oversee the confidentiality, security and appropriate use of the data and manage disclosures of data extracts to third parties to ensure identifiable data is not disclosed or is only disclosed with consent or another legal basis?</p>	<p>Information Sharing Agreement signed by all partners who attend MARAC the ISA covers:</p> <ol style="list-style-type: none"> 1. Purpose of the protocol, 2. Data, 3. Data Retention, 4. Process 5. Security and Data Management, 6. Complaints, 7. Data Breaches, 8. Review Arrangements, 9. Withdrawal from this Agreement, 10. Signatories  <p>BBC Marac Information Sharing A</p> <p>All MARAC documentation is regularly reviewed by the MARAC Steering Group to ensure it is up to date and fit for purpose.</p> <p>Confidentiality Agreement is sent to all representatives attending MARAC prior to each meeting and is a standing agenda item at the start of the MARAC meeting.</p> <p>Any concerns or issues with data protection on individual cases to be heard at the meeting can be outlined with the Chair of the relevant MARAC meeting. Any ongoing Data Protection issues will be shared by the Chair with the MARAC Steering Group to address.</p>
<p>If holding personal i.e. identifiable data, are procedures in place to provide access to records under the subject access provisions of the GDPR?</p> <p>Is there functionality to respect withdrawals of consent?</p>	<p>Local Authority procedures will be followed with the guidance of the Data Protection Officer</p> <p>All involved agencies are required to have their own policies in place</p> <p>It should <u>not</u> be assumed that informed consent is essential in order for agencies to share information in support of victims of domestic abuse.</p> <p>Obtaining consent remains a matter of professional good practice and, in circumstances where it is appropriate and possible, explicit consent should be sought from, and freely given by, the subject of the information.</p> <p>Consent may be withdrawn or refused, however if it is felt to be in the best interests of the victim, their children or the general public to share information to reduce risk, information will still be shared as MARAC meets the conditions of Schedule 1 Part 2 of the DPA 2018 (Substantial Public Interest) in particular (6, 10 & 18), and Schedule 8 Part 3 of the DPA 2018 in particular (1,2,3 & 4).</p>

Data Protection Impact Assessment - Template

<p>Is there functionality in place to respect the data subject's rights in respect of:</p> <ul style="list-style-type: none"> a) Rectification b) Erasure c) Restriction d) Data portability e) Objection 	<p>Local Authority procedures will be followed with the guidance of the Data Protection Officer.</p> <p>All involved agencies are required to have their own policies in place</p>
<p>Will processing involve any automated decision taking yes/no and if so, is functionality in place to respect the data subject's right to object?</p>	<p>No</p>
<p>Are there any plans to allow the information to be used elsewhere either in the Council or by any other third party? E.g. partners, suppliers etc.</p> <p>If so, a copy of the appropriate Data Sharing Agreement should be attached together with a copy of the appropriate contract</p>	<p>Not outside of the remit of MARAC</p>
<p><u>Data Quality</u></p> <p>What is the process to allow personal information to be checked for relevancy, accuracy and validity?</p>	<p>Each agency sharing the data is responsible for ensuring the information shared is checked. Any concerns over inaccuracy or validity will be challenged within the MARAC, actions set to verify the information and corrected or deleted on relevant documents</p>

Describe the information flows

The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows.

**Data Protection Impact Assessment -
Template**



<p>Does any data flow in identifiable form? If so, from where, and to where?</p>	<p>From the referrer to the MARAC co-ordinator and from MARAC Co-ordinator to the referrer.</p> <p>From the MARAC co-ordinator to the core agencies attending MARAC and core agencies to the MARAC Co-ordinator</p>
<p>Media used for data flow? (e.g. email, fax, post, courier, other – please specify all that will be used)</p>	<p>Secure e-mail</p>

Data Protection Impact Assessment -

Data Linkages	
Will the data be linked with any other data collections?	Not directly; it will not be stored on any other data bases
How will this linkage be achieved?	All core agencies are required to check their records prior to the MARAC meeting and complete research on the victim's, children and families and perpetrators. The research is added to the data base MODUS which is used solely for MARAC.
Is there a legal basis for these linkages?	<p>Yes - Schedule 1 Part 2 of the DPA 2018 (Substantial Public Interest) in particular (6, 10 & 18), Schedule 8 Part 3 of the DPA 2018 in particular (1,2,3 & 4)</p> <p>Agencies also have statutory duties under the following legislation:</p> <ul style="list-style-type: none"> General Data Protection Regulation 2018 (GDPR) Data Protection Act 2018 (DPA18) The Children Act (1989 & 2004) The Human Rights Act (2000) S.115 The Crime & Disorder Act 1998 Criminal Procedures and Investigations Act 1996 Common Law Duty of Confidence Freedom of Information Act 2000 Housing Act 1996 Mental Health Act 1983 Health & Social Care Act 2001 Education Act 1996 and 2002 NHS and Community Care Act 1990 Sex Offenders Act 1997 Care Act 2014 Anti-Social Behaviour Crime and Policing Act 2014 Mental Capacity Act 2005 Protection of Freedom Act 2012

Information Security	
Who will be able to access identifiable data and what security controls will be in place for access?	All representatives from the organisations signed up to the Information Sharing Agreement. Only those individuals identified as being a representative for their organisation at MARAC will be granted access. The data base is password protected and each user is allocated their own username and password. All users of the data

Data Protection Impact Assessment - Template



Information Security	
	<p>base are required to sign a MODUS user confidentiality agreement prior to being granted access to the database.</p> <p>On occasions at the MARAC meeting an individual who is working with the vulnerable person or family but is not part of the information sharing agreement will be invited to attend MARAC for their particular case to share relevant information to the meeting to ensure that the safety measures being put in place are informed by having all the information required to make safeguarding decisions. The MARAC confidentiality statement is read out at each meeting and when a non-core partner attends for their case to ensure that the bounds of confidentiality and information sharing within the meeting are maintained.</p>
<p>What security measures will be in place to protect the data in transit?</p>	<p>All e-mails must be sent securely by all partners using enforced TLS encryption. User accounts are MFA enabled. Laptop and Mobile devices have encrypted storage devices (e.g. hard drives). USB storage (if used) will also be encrypted as default.</p>
<p>What confidentiality and security measures will be in place to protect the data when it is stored?</p> <p>Please provide an answer for the Logical, physical and Procedural security measures that will be applied.</p>	<p>Each partner will be a controller and will need to confirm that they have sufficient security when signing the ISA. Answers to this question have been provided in the ISA and below:</p> <p>Logical: Access controlled by individual username and password, staff must sign user confidentiality agreement, Administrative access is restricted, all users are baseline security screened.</p> <p>Data transmission via secured email (using forced TLS encryption), data at rest encrypted using 256bit SSL on the server and FIPs 140-2 on mobile devices.</p> <p>Physical: Server in a secure location (data centre) with ISO27001 controls in place. Bedford Borough Council Laptop hard drives are Encrypted to FIPS 140-2 standards, controls in place for USB devices (forced encryption). Any printed material will be disposed of in confidential waste bins.</p> <p>Procedural: Bedford Borough Council Computer User Security Policy applies to all staff, acceptable use policies are covered as are Access Controls. Personnel Services Agile Working Policy in place. Confidentiality statement incorporated into each meeting agenda as item number 1.</p>

Data Protection Impact Assessment - Template



Information Security	
	<p>Bedford Borough Council's Technology department are also ISO27001 certified, have a current Cyber Essential Certificate and PSN code of connectivity certificate.</p>
<p>What procedures will be in place for reporting of Information Security incidents/data breaches such as; electronic or manual loss of data or equipment loss; unlawful disclosure, deletion, or destruction?</p>	<p>Local Authority procedures will be followed with the guidance of the Data Protection Officer.</p> <p>All involved agencies are required to have their own policies in place</p> <p>The chair of the MARAC will place a complaint with the organisation where it is believed the breach has come from for them to follow their procedures.</p>
<p>How will it be destroyed once it has passed its retention period?</p> <p>Please refer to ICO Guidance for destruction of electronic media</p>	<p>All client records will be archived 7 years after the last MARAC meeting. If a referral is received after a file has been archived the historical information will be made available again and re-archived 7 years from the date of the last MARAC meeting.</p>
<p><u>Business Continuity</u></p> <p>What will the process be to enable data retrieval to support business continuity in the event of emergencies or disasters</p>	<p>Modus is hosted at a secure data centre in the UK (for more information on the hosting provider including all ISO accreditation click here). All data transmitted to and from the site is encrypted with 256bit SSL. Access to Modus requires a username and strong password; Paloma staff are all DBS checked with nominated staff receiving enhanced Police vetting and all staff are required to sign confidentiality agreements. All activity in the system is logged within the database as an audit trail. The database is backed up four times a day and once at night; two weeks of backups are stored at any one time. A dedicated Firewall protects the server, KCOM perform regular checks on the environment to check for vulnerabilities but we also undertake regular penetration tests to ensure our web code is not vulnerable.</p>

Data Protection Impact Assessment - Template

Privacy Risks

List any identified risks to privacy and personal information of which the project is currently aware.

Risks should also be included on the project risk register.

Risk Description (to individuals, to the council or to wider compliance)	Current Impact	Current Likelihood	Risk Score (I x L)	Proposed Risk solution (Mitigation)	Is the risk reduced, transferred, or accepted? Please specify.	Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Individuals not being in a position to give informed consent to information sharing	L	U		<p>All agencies completing a referral form are required to fully inform the individual/s of what MARAC is, the purpose of MARAC, who information will be shared with, how it will be stored and for how long. This can be achieved via the privacy notice.</p> <p>All agencies to understand the legal basis for information sharing at MARAC and where informed consent is not given completing an information sharing without consent form</p>	Reduced	Yes
To individuals of the perpetrator becoming aware	VH	VU		All professionals who make referrals to MARAC are	Transferred	Yes

Data Protection Impact Assessment - Template

of the case being heard at MARAC and this causing an increase in risk of harm to the individual from the perpetrator				<p>made aware of the consequences of disclosure to a perpetrator for the victim</p> <p>At the point of referral all referrers to inform the client of the purpose of MARAC and that the perpetrator is not aware of the meeting and why and what the consequences could be of the perpetrator having an awareness</p>		
Personal data is shared inappropriately outside of the MARAC meeting	H	U		<p>All core agencies who attend MARAC are required to read the ISA and confirm their agreement at the start of each meeting to the confidentiality agreement</p> <p>Confidentiality statement is shared with individual agencies who are not part of the ISA, but have participated in the meeting for specific cases and are aware of the legal basis for sharing information</p>	Reduced	Yes
Data breach through sharing information on	VH	VU		All partners are aware via the ISA that information must only be	Transferred	Yes

Data Protection Impact Assessment - Template

insecure IT systems				shared through secure e-mail. Any data breaches are dealt with through the process identified in the ISA		
Requests for MARAC information to be shared with other partners and for court purposes/ FOI requests.	H	L		All requests are agreed in consultation with Data Protection Officer and agreed by the said MARAC chair. The data is redacted as necessary in line with GDPR/ Data Protection and CP/VA safeguarding legislation or anonymised where feasible so individuals cannot be identified.	Reduced	Yes

RISK CALCULATION

IMPACT	SCORE	LIKELIHOOD	SCORE
Very Low		Very unlikely	
Low		Unlikely	
High		Likely	
Very High		Very Likely	

Data Protection Impact Assessment - Template



Approval by Information Governance/Information Security

Risk Description	Approved solution	Approved by	Date of approval

Actions to be taken within the Project

Action to be taken	Date of Completion	Action Owner

Consultation requirements

Part of any project is consultation with stakeholders and other parties. In addition to those indicated “Key information, above”, please list other groups or individuals with whom consultation should take place in relation to the use of person identifiable information.

It is the project’s responsibility to ensure consultations take place, but Information Governance will advise and guide on any outcomes from such consultations.

DPO

Legal

IT Security & Governance

Further information

Please provide any further information that will help in determining privacy impact.

Data Protection Impact Assessment - Template



Data Protection Officer (DPO) comments:

Following review of this DPIA by the DPO, a determination will be made regarding the privacy impact and how the impact will be handled. This will fall into four categories:

1. No action is required by Information Governance excepting the logging of the Screening Questions for recording purposes.
2. The questionnaire shows use of personal information but in ways that do not need direct IG involvement – the DPO may ask to be kept updated at key project milestones.
3. The questionnaire shows significant use of personal information requiring DPO involvement via a report and/or involvement in the project to ensure compliance.
4. The DPIA needs referral to the Information Commissioner’s Office in respect of risks which cannot be mitigated and remain high – such as where individuals may encounter significant or even irreversible consequences, or when it is obvious that a risk may occur. The GDPR contain specific procedural directions for this and the SIRO should be consulted.

It is the intention that the Data Protection Officer will advise and guide those projects that require information governance’s (IG) compliance but at all times will endeavour to ensure that the project moves forward and that IG is not a barrier unless significant risks come to light which cannot be addressed as part of the project development and will need to be escalated to the Council’s Senior Information Risk Owner (SIRO), for approval.

Please email entire completed document to dpo@bedford.gov.uk.

Data Protection Impact Assessment - Template



Information Governance Approval (for low to medium risk processing)

IG staff name: Jashpal Mann

Signature: *Jashpal Mann*

Date: 27.01.2023

SIRO approval (for high risk processing)

SIRO name:

Signature:

Date:

Data Protection Impact Assessment - Template

Appendix 1- The conditions (the legal basis) for processing Personal Data under the General Data Protection Regulations (GDPR)

The conditions for processing Personal Data and Special Category (formerly Sensitive Data) Personal Data are set out in Article 6(1) and Article 9(1) and (2) of the GDPR as follows:

Definition of Personal Data and Special Categories (formerly Sensitive data) of Personal Data

Personal Data- means data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Special Categories of Personal Data- includes information relating to the data subject's -

- racial or ethnic origin,
- political opinions,
- religious belief or other philosophical beliefs
- trade union membership,
- data concerning physical or mental health or condition,
- sex life and sexual orientation
- genetic data
- biometric data where processed to uniquely identify an individual

The Data Protection Bill 2017 is awaited in respect of derogations regarding whether the processing of personal data in relation to criminal convictions and offences will be categorised as Special Category (formerly Sensitive) data.

Article 6(1) conditions for processing Personal Data

Unless a relevant exemption applies, at least one of the following conditions must be met whenever you process personal data:

- a) The data subject has given their consent to the processing: this consent is explicit. Further conditions are imposed in the case of children online.
- b) The processing is necessary for the performance of a contract with the data subject or to take steps preparatory to such a contract
- c) The processing is necessary for compliance with any legal obligation to which the data controller is subject.
- d) The processing is necessary in order to protect the vital interests of the data subject.
- e) The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

Data Protection Impact Assessment - Template



f) The processing is necessary for the

purposes of legitimate interests.

Nb under GDPR this ground can no longer be relied on by Public Authorities processing personal data in exercise of the functions

Article 9(1) and (2) Special Categories (formerly sensitive) of Personal Data

Article 9(2) sets out the circumstances in which the processing of Special Category (sensitive) personal data which is otherwise prohibited, may take place. The following categories of data are considered Special Category or sensitive as set out in Article 9(1):

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Data concerning health or sex life and sexual orientation;
- Genetic data (new)
- Biometric data where processed to uniquely identify a person (new)

At least one of the conditions listed on the previous page must be met whenever you process personal data (Article 6(1) conditions). However, if the information is Special Category (formerly sensitive personal data), at least one of several other conditions must also be met before the processing can comply with the first data protection principle: Lawfulness, fairness and transparency Article: 9(2). These other conditions are as follows:

- a) The individual whom the sensitive personal data is about has given explicit consent to the processing.
NB: measures must be in place in order that the individual can easily withdraw that consent at any time and please see guidance in respect of consent from children.
- b) The processing is necessary so that you can comply with employment or social security or social protection law, or a collective agreement.
- c) The processing is necessary to protect the vital interests of: the data subject who is physically or legally incapable of giving consent.
- d) The processing is carried out by a not-for-profit organisation with a political, philosophical, religious, or trade union aim provided the processing only relates to members or former members (or for those with regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- e) Data manifestly made public by the data subject.
- f) The processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity

Data Protection Impact Assessment - Template



- g) The processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguarding measures.
- h) The processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and service on the basis of Union or Member State law or a contract with a health professional
and,
- i) The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.

Both provisions 9(2)(h) and (i) expand the equivalent provision in the Data Protection Directive and address acknowledged gaps in that Directive, by providing a formal legal justification for regulatory uses of healthcare data in the health and pharmaceutical sectors, and by providing for the sharing of health data with providers of social care.

Both conditions require obligations of confidentiality to be in place by way of additional safeguards.