worcestershire county council

Date printed: 08/02/2022
Assessment not yet complete
Requester: Paul Kinsella

Data Protection Full Assessment
Impact Assessment Id: #279

1.0 Screening Information

Project Name
Implementation of new Domestic Abuse Duty under Part iv of the DA Act 2021

Name of Project Sponsor
Dr Kathryn Cobain

Name of Project Manager
Tony Mercer

Name of Project Lead
Paul Kinsella

Please give a brief description of the project
Implementation of the changes introduced by the new duties in part iv of the Domestic Abuse Act 2021

Data Protection screening result
Will require a full impact assessment

Equality and Public Health screening result
Will require a full impact assessment

Environmental Sustainability screening result
Does not need a full impact assessment

1.1 Background and Purpose

Background and Purpose of Project?
To support your answer to this question, you can upload a copy of the project's Business Case or similar document.
To oversee delivery of the additional duties under part iv of the Domestic Abuse Act 2021

Upload Business Case or Support documents
DA Strategy Spec 2021 07 01 Mature Draft.docx

Project Outputs
Briefly summarise the activities needed to achieve the project outcomes.
Accommodation and support to victims of Domestic Abuse

Project Outcomes
Briefly summarise what the project will achieve.
Improve the safety of victims of DA and children involved in DA
Enable victims of DA (and their children to maintain tenancies and recover from the effects of DA

Is the project a new function/service or does it relate to an existing Council function/service?
Existing

Was consultation carried out on this project?
No

1.2 Responsibility

Directorate/Organisation

People

Service Area

Public Health

1.4 Specifics

Project Reference (if known)

Not Recorded

Intended Project Close Date *

April 2024

1.5 Project Part of a Strategic Programme

Is this project part of a strategic programme?

No

2.0 Personal Data

Who are you processing data about?

Customers, clients or service users
Suppliers
Staff, persons contracted to provide a service
Professional advisers and consultants
Students and pupils
Landlords
Recipients of Benefits
Witnesses
Offenders and suspected offenders
Representatives of other organisations

What personal data will be collected? *

The second stage is to list all of the types of personal data that you believe the project/works/additional processing will utilise. Please select yes for as many examples of types of data that are relevant and include any others in the free text at the bottom of the page.

Basic Identifiers:

Name

Yes

Date of Birth

Yes

Age

Yes

Gender

Yes

Sex

Yes

Contact Details:

Address

Yes

Email Address

Yes

Home Phone Number

Yes

Mobile Phone Number

Yes

Postcode

Yes

ID Number:

National Insurance Number

Yes

Driving Licence/Number

No

NHS Number

Yes

Other General Identifier

Yes

Employment:

Work Related Training/Awards

No

Financial:

Income/Financial/Tax Situation

Yes

Appearance:

Photograph

No

Physical Description

No

Lifestyle:

Living Habits

Yes

Marital Status

Yes

Technology:

Login/Username

No

Device MAC Address (Wireless Network Interface)

No

Device Mobile Phone/Device IMEI No

No

Location Data (Travel/GDPS/GSM Data)

No

Online Identifier e.g. IP Address

No

Website Cookies

No

Other Data Types Collected

Not Recorded

2.1 Legal basis for Personal Data

What is your lawful basis for processing the personal data? *

Please choose one of the following

Data Subject's consent for the purpose
No

Necessary for a contract with the Data Subject
No

Necessary to comply with a legal obligation
Yes

Necessary to protect the vital interests of an individual(s)
Yes

Necessary for a task in the public interest or exercise of official authority of Controller
Yes

Necessary for legitimate interests of Controller unless interests are overridden by the interests or rights of the individual (only available in limited circumstances to public bodies)
No

2.2 Special Data

What special category personal data (if any) will be collected? *

This section will not apply to all projects and should only be completed if it applies to you.
It is important that you read this section carefully, as these data types require additional care and protection.
If you do pick anything from this list, you will be required to give more details in Section 4 of this form.
You can read more about Special Category Data through this link;
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

Race

Yes

Ethnic origin

Yes

Political opinions

No

Religion

Yes

Philosophical beliefs

No

Trade union membership

No

Genetic Data

No

Biometric Data

No

Sex life

No

Health or social care

Yes

2.3 Legal basis for Special Data

What is the relevant condition for processing the special category personal data? *

You must qualify under one of the below exemptions as well as having a legal basis from the previous question.

Explicit Consent

The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
Yes

Employment and Social Security

Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
No

Vital Interests

Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
No

Legitimate Interests of:

"a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim".

Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

Note – this is not often applicable to local authorities.

No

Publicly Available Data

Processing relates to personal data which are manifestly made public by the data subject;

No

Legal or Court Proceedings

Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

No

Public Interest - Statutory Necessity

Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

No

Medical, Health and Social Care Provision

Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

No

Public Health

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 quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

No

Archiving or Scientific, Historical or Statistical Research Purposes

Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

No

2.4 Information Involved

Understanding the information flows involved in a project is essential to a proper assessment of privacy risks.

How will the data be collected? *

This section should be filled in for every project, not just those collecting Special Category data.
The data collected is to enable vulnerable victims of domestic abuse to be placed in accommodation with appropriate support services.
This data is already collected for this purpose by the partners involved in the provision of accommodation and services to the survivors of Domestic Abuse , but the act requires an expansion of the scale on which it is collected as there is a need to meet a broader set of needs from a more diverse group of DA survivors

What will the data be used for? *

This section should be filled in for every project, not just those collecting Special Category data.
The data collected is to enable vulnerable victims of domestic abuse to be placed in accommodation with appropriate support services.

Has data already been collected?

No

Are the purposes for which you are collecting the data different? *

If the data you are hoping to use was not collected specifically for this project, please explain in the box below why it was collected. This will include data that you have collected from other teams within WCC.
The data needs to identify and enable engagement with individuals with protected characteristics and as identified under the Equalities Act

Explain why existing and/or less intrusive processes or measures would be inadequate *

In this section, you should explain why your new method/project is absolutely necessary and show that you have thought about all other options.
The data needs to identify and enable engagement with individuals with protected characteristics and as identified under the Equalities Act to meet the statutory duties under the Domestic Abuse Act 2021.

3.0 Other organisations

Are other organisations involved in processing the data?

Yes

Please provide details of each organisation that is involved in the processing of Data. Do this by adding to the below list. *

Organisation Name	WM Police
Data Controller or Data Processor	Data Controller
Organisation's Role	Controller and originator
Data Sharing Agreement or Contract	Yes
Contract Reference Number/DSA Name	DS006395 ISP037 Safer Communities
Organisation involved reason	It owns/originates the data
Disclosure and Security	Secure encrypted email

Organisation Name	Worcester Acute Trust
Data Controller or Data Processor	Data Controller
Organisation's Role	Originator and owner of data
Data Sharing Agreement or Contract	Yes
Contract Reference Number/DSA Name	DS006395 ISP037 Safer Communities
Organisation involved reason	It owns the data
Disclosure and Security	Secure encrypted email

Organisation Name	Herefordshire and Worcestershire Health and Care NHS Trust
Data Controller or Data Processor	Data Controller
Organisation's Role	Controller and originator of data
Data Sharing Agreement or Contract	Yes
Contract Reference Number/DSA Name	DS006395 ISP037 Safer Communities
Organisation involved reason	It is the originator of data and may provide services to the subjects
Disclosure and Security	Secure Encrypted email

Organisation Name	Probation Service
Data Controller or Data Processor	Data Controller
Organisation's Role	Information originator
Data Sharing Agreement or Contract	Yes
Contract Reference Number/DSA Name	DS006395 ISP037 Safer Communities
Organisation involved reason	It holds offender and victim data
Disclosure and Security	Encrypted email

4 records

3.1 Storage detail

How will the information be stored? *

Please include details of whether data will be stored outside of the European Economic Area (EEA).
Please remember that cloud storage and back up servers maybe outside the EEA.
On organisations servers

For how long will the data be retained? *

In accordance with Data retention directives and local policies

What is the deletion process? *

TBC

4 Consultation details

Consultation can be used at any stage of the DPIA process and is important to allow people to highlight privacy risks and solutions based on their own area of interest or expertise.
For further assitance and information please visit the consultation toolkit section on Ourspace.

Explain what practical steps you are going to take to ensure that you identify and address privacy risks *

Through consultation with the partners to the Domestic Abuse Partnership Board (DAPB)

Who should be consulted, internally and externally? Do you need to seek the views of members of the public? *

DAPB has internal and external members with experience in the DA arena and with a view of the issues. This means public consultation is not required

How will you carry out the consultation? *

(You should link this to the relevant stages of your project management process)
Through the DAPB in accordance with existing meeting structure and timescales

5 Risk register

At this stage you should identify the possible privacy risks together with their likelihood, severity and overall level, and for high risks the measures taken to reduce the risk.
Add any risk to the relevant sections below.

Fair and Lawful Processing

Data must be processed lawfully, fairly and in a transparent manner.
Please also consider

- Have you identified at least one lawful basis for the personal data processed as part of the project?
- Does at least one Controller involved have a lawful power to act?
- Do you need to create or amend a privacy notice?
- How is your processing going to be transparent?

Risk that processing is not transparent, and individuals are unaware that data is being collected or why it is processed

No Risk

Risk that information is being processed unlawfully

Unmitigated Risk
Likelihood - Unlikely
Severity - Minimal Impact
Score - Low
Mitigation/Solution

None at this stage

Mitigated Risk
Likelihood - Unlikely
Severity - Minimal Impact
Score - Low

Result
Accepted

Specific, explicit and legitimate purposes

The purpose for which you process personal data must be specified, explicit and legitimate. Personal data collected must not be processed in a manner that is incompatible with the purpose for which it was originally collected.
Please also consider

- Does your project plan cover all of the purposes for processing personal data? If not your plan needs amending accordingly.
- Are all elements of the processing compatible with the original reason and justification for the processing?
- What are these specific, explicit and legitimate purposes?

Risk of 'mission creep' and information is used for different, or incompatible purposes to that identified when originally collected

Unmitigated Risk
Likelihood - Reasonably Unlikely
Severity - Some Impact
Score - Medium

Mitigation/Solution
This a complex area; the ORIGINAL collection of information may be in connection with delivering each individual service's responsibilities and this exchange drops out of a secondary commitment to housing (and supporting) victims. It is unlikely that data retained for these purposes will then be used for other purposes

Mitigated Risk
Likelihood - Reasonably Unlikely
Severity - Some Impact
Score - Medium

Result
Accepted

Adequate, relevant and not excessive

Personal data processed must be adequate, relevant and not excessive in relation to the purpose for which it is processed.
Please also consider

- Is the quality of the information adequate for the purposes it is used?
- If not, how is this to be addressed?
- Are measures in place to ensure that data is limited to that which is needed to fulfill the aim of the processing?
- Which personal data elements do not need to be included without compromising the needs of the project?

Risk of loss of control over the use of personal data

No Risk

Risk that inadequate data quality means the information is not fit for the identified purpose(s) potentially leading to inaccurate decision making

Unmitigated Risk
Likelihood - Unlikely
Severity - Minimal Impact
Score - Low

Mitigation/Solution
None - the reason for collecting the data is to improve outcomes

Mitigated Risk
Likelihood - Unlikely
Severity - Minimal Impact
Score - Low

Result
Accepted

Risk that any new surveillance methods may be an unjustified intrusion on individuals' privacy

No Risk

Accurate and timely

Personal data processed must be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay.
Please also consider

- If you are procuring new software does it allow you to amend data when necessary?
- How are you ensuring that personal data obtained from individuals or other organisations is accurate?
- Do you have processes in place to keep data up to date?
- If any data sets are to be merged, what checks are carried out to ensure that the right data records are matched/merged together?

Any data matching or linking, including whole data sets may link wrong records together

Unmitigated Risk
Likelihood - Unlikely
Severity - Some Impact
Score - Low

Mitigation/Solution
This is a part of each organisations data processes and staff development

Mitigated Risk
Likelihood - Unlikely
Severity - Some Impact
Score - Low

Result
Accepted

Storage limitation

Personal data must be kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data.
Please also consider

- What are the risks associated with how long data is retained and how they might be mitigated?
- Has a review, retention and disposal (RRD) policy been established?
- How does the software enable you to easily act on retention criteria – does it enable bulk review/destruction; set review periods; extract for long-term preservation/retention of the corporate memory?

Risk information is retained for the wrong length of time (both too long and too short)

Unmitigated Risk
Likelihood - Unlikely
Severity - Minimal Impact
Score - Low

Mitigation/Solution
Each Data Controller is compliant with national requirements and its own policy and has Data governance structures in place

Mitigated Risk
Likelihood - Unlikely
Severity - Minimal Impact
Score - Low

Result
Accepted

Risk information is not securely destroyed when its retention period has been reached

Unmitigated Risk
Likelihood - Reasonably Unlikely
Severity - Minimal Impact
Score - Low

Mitigation/Solution
Each Data Controller is compliant with national requirements and its own policy and has Data governance structures in place. The impact in NOT destroying data is compliance, not in terms of delivering service

Mitigated Risk

Likelihood - Unlikely
Severity - Minimal Impact
Score - Low

Result
Accepted

Security

Personal data must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, “appropriate security” includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).
Please also consider

- What technical and organisational measures are in place to ensure that the data is protected to an adequate level?
- What training on data protection and/or information sharing has been undertaken by relevant staff?
- What access controls are in place to enforce the ‘need to know’ principle?
- What assurance frameworks are utilised to assess adequacy of security measures in place e.g. NHS DSPT; Cyber Essentials Plus; PSN Certification?

Risk of loss of confidentiality

Unmitigated Risk
Likelihood - Unlikely
Severity - Serious Impact
Score - Medium

Mitigation/Solution
This applies to personal data across all the relevant organisations in all their areas of business. Each Data Controller is compliant with national requirements and its own policy and has Data governance structures and oversight in place

Mitigated Risk
Likelihood - Unlikely
Severity - Serious Impact
Score - Medium

Result
Accepted

Risk of inadequate security controls in place to protect and secure personal data, including inappropriate access

Unmitigated Risk
Likelihood - Unlikely
Severity - Serious Impact
Score - Medium

Mitigation/Solution
This applies to personal data across all the relevant organisations in all their areas of business. Each Data Controller is compliant with national requirements and its own policy and has Data governance structures and oversight in place. Data security forms part of all training for staff (eg WCC Mandatory training). There is nothing specific to this risk/issue that justifies additional training to staff

Mitigated Risk
Likelihood - Unlikely
Severity - Serious Impact
Score - Medium

Result
Accepted

Risk that workers processing the data are not aware of their data responsibilities

No Risk

Risk that information is distributed using inappropriate methods

Unmitigated Risk
Likelihood - Unlikely
Severity - Minimal Impact
Score - Low

Mitigation/Solution
This applies to personal data across all the relevant organisations in all their areas of business. Each Data Controller is compliant

with national requirements and its own policy and has Data governance structures and oversight in place. Data security forms part of all training for staff (eg WCC Mandatory training). There is nothing specific to this risk/issue that justifies additional training to staff

Mitigated Risk
Likelihood - Unlikely
Severity - Minimal Impact
Score - Low

Result
Accepted

Risk of re-identification of pseudonymized or anonymised data (e.g. collecting matching and linking identifiers and information may result in information that is no longer safely anonymised)

No Risk

Risk that information is transferred to a 'third country' without adequate safeguards

No Risk

Financial and reputational

Risk of identity theft or fraud

Unmitigated Risk
Likelihood - Unlikely
Severity - Serious Impact
Score - Medium

Mitigation/Solution
This applies to personal data across all the relevant organisations in all their areas of business. Each Data Controller is compliant with national requirements and its own policy and has Data governance structures and oversight in place. Data security forms part of all training for staff (eg WCC Mandatory training). There is nothing specific to this risk/issue that justifies additional training to staff.

Mitigated Risk
Likelihood - Unlikely
Severity - Serious Impact
Score - Medium

Result
Accepted

Risk of financial loss for individuals or other third parties

Unmitigated Risk
Likelihood - Unlikely
Severity - Serious Impact
Score - Medium

Mitigation/Solution
This applies to personal data across all the relevant organisations in all their areas of business. Each Data Controller is compliant with national requirements and its own policy and has Data governance structures and oversight in place. Data security forms part of all training for staff (eg WCC Mandatory training). There is nothing specific to this risk/issue that justifies additional training to staff

Mitigated Risk
Likelihood - Unlikely
Severity - Serious Impact
Score - Medium

Result
Accepted

Risk of financial loss for the Council (including ICO fines)

Unmitigated Risk
Likelihood - Unlikely
Severity - Serious Impact
Score - Medium

Mitigation/Solution
Measures are in place already: This applies to personal data across all the relevant organisations in all their areas of business. Each Data Controller is compliant with national requirements and its own policy and has Data governance structures and oversight

in place. Data security forms part of all training for staff (eg WCC Mandatory training). There is nothing specific to this risk/issue that justifies additional training to staff

Mitigated Risk
Likelihood - Unlikely
Severity - Serious Impact
Score - Medium

Result
Accepted

Risk of reputational damage to the Council, partners, and processors

Unmitigated Risk
Likelihood - Unlikely
Severity - Serious Impact
Score - Medium

Mitigation/Solution
This applies to personal data across all the relevant organisations in all their areas of business. Each Data Controller is compliant with national requirements and its own policy and has Data governance structures and oversight in place. Data security forms part of all training for staff (eg WCC Mandatory training). There is nothing specific to this risk/issue that justifies additional training to staff

Mitigated Risk
Likelihood - Unlikely
Severity - Serious Impact
Score - Medium

Result
Accepted

Health, safety and wellbeing

Risk of physical harm to individuals

Unmitigated Risk
Likelihood - Unlikely
Severity - Serious Impact
Score - Medium

Mitigation/Solution
Data breach could expose vulnerable DA Survivors to risk of harm (This is true throughout the DA environment). Each organisation has measures in place and its staff are aware of these risks. No additional measures are required

Mitigated Risk
Likelihood - Unlikely
Severity - Serious Impact
Score - Medium

Result
Accepted

Risk of physical harm to staff and workers

Unmitigated Risk
Likelihood - Unlikely
Severity - Serious Impact
Score - Medium

Mitigation/Solution
As above. Staff are aware of the risk to themselves when working within the DA environment. This is not a new or additional risk so existing measures are appropriate

Mitigated Risk
Likelihood - Unlikely
Severity - Serious Impact
Score - Medium

Result
Accepted

Risk of discrimination

Unmitigated Risk
Likelihood - Unlikely

Severity - Serious Impact
Score - Medium

Mitigation/Solution
The part iv duty is designed to address protected characteristics and equalities act issues Staff are/will be tasked to identify and overcome discrimination.

Mitigated Risk
Likelihood - Unlikely
Severity - Some Impact
Score - Low

Result
Accepted

Risk of other significant economic or social disadvantage

Unmitigated Risk
Likelihood - Unlikely
Severity - Minimal Impact
Score - Low

Mitigation/Solution
Accept

Mitigated Risk
Likelihood - Unlikely
Severity - Minimal Impact
Score - Low

Result
Accepted

Individuals Rights

Data protection legislation gives data subjects' various rights (listed below). Limiting or restricting any of these rights is likely to be a significant impact so the justification for any restriction, as well as mitigations, must be fully outlined.

Inability to meet individuals' right to be informed

No Risk

Inability to meet individuals' right of access

No Risk

Inability to meet individuals' right to rectify inaccurate data

No Risk

Inability to meet individuals' right to erase data

No Risk

Inability to meet individuals' right to restrict processing

No Risk

Inability to meet individuals' right to object

No Risk

Inability to meet individuals' rights relating to automated decision making and profiling

No Risk

Additional project specific risks

No additional risks recorded

6 Declaration

I confirm to the best of my knowledge that the information I have provided is true, complete and accurate *
Selected

I confirm that I will make sure that data protection has been and continues to be considered throughout the project life cycle and should circumstances change in the project to include any processing of personal data a further Data Protection Impact Assessment Screening will be carried out *
Selected