

Data Protection Impact Assessment

Guidance

Introduction to Data Protection Impact Assessments

What Is a Data Protection Impact Assessment (DPIA)?

A DPIA is a simple, risk-based mechanism to help identify the level of risk to personal data when implementing a new activity, project or system. It enables an organisation systematically to analyse how a project or system will affect the privacy of the individuals involved. DPIAs include an assessment of personal and sensitive personal data used by Data Controller and Data Processor in processing activities.

Why is a DPIA needed?

A DPIA will help to ensure that potential problems with a project or change are identified at an early stage, when addressing them is usually simpler and less costly. Conducting a DPIA is required as an integral part of privacy by design required to achieve compliance with the current Data Protection Regulations.

Definitions

| | |
|--|--|
| Privacy | Information privacy is the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. |
| Personal Data | Is data that relates to a living individual, who can be identified from that data, or from a combination of that data and other information held by, or likely to come into the possession of, the Data Controller or Data Processor. Examples include HR records or client data. |
| Special Category Data (Formerly known as Sensitive Personal Data) | Is data which relates to ethnic or racial origin, political opinion, religious or similar belief, sexual life, physical or mental condition and information related to criminal activity. The GDPR extends this definition to include genetic, biometric or health data where processed to uniquely identify a person. |
| Processing | Encompasses the following aspects of an operation, such as obtaining, recording, storage (including backup copies), retrieval, erasure, manipulation, organisation, combination (with other data), adaptation or alteration, consultation or use of the information or data. |
| Data Controller | Is the person or organisation who collects, processes and manages personal data, and has a legal basis for doing so. |
| Data Processor | Is any third party who processes personal data on behalf of National Church Institutions . |

When is a DPIA required?

At the point where any process, programme or project brief is being created, it must be risk assessed using a DPIA, usually prior to the project initiation phase. If the project will involve a system or service being procured, the needs of the project should be established before procurement takes

place. This ensures the risks, and costs of mitigating those risks are fully understood when assessing the viability of the project.

Examples of situations where a DPIA is suitable include:

- A new IT system for storing and accessing personal data
- A new database which consolidates information that has been held separately
- A data sharing initiative where **National Church Institutions** and third-party organisations seek to pool or link sets of personal data
- Using existing data for a new or more intrusive purpose.

DPIAs should be conducted for changes to existing processes even if a DPIA has been carried out before.

Completing the DPIA

Each section of the DPIA is to be completed as fully as possible. Guidance notes are provided. If a question or section is not relevant to your project, then it should be indicated as Not Applicable (N/A).

Prior to completing the template, you should familiarise yourself with **National Church Institutions'** Data Protection Policies and Procedures.

When completed the guidance notes can be removed from the document.

Support Questionnaire

In the appendix to this template is a simple questionnaire that will help you to think about the kinds of thing that you need to consider when doing a DPIA, especially if you have not had much experience in completing one before.

Process For completion

- The Project Manager/Lead Officer from the department completes the DPIA
 - ▶ Section 1 – This provides an initial assessment to identify if a DPIA is required
 - ▶ Section 2 – This section must be completed if any of the initial screening answers are YES
- Send the completed DPIA to the Data Protection Officer and other relevant individuals who been consulted for review and feedback.
- Once the review process is completed, the DPIA should be signed off as indicated in Section 4.
- The Project Manager/Lead Officer keeps a copy of the signed DPIA with their project documentation and provides a copy to the Data Protection Officer.

Information Commissioner Review

Under Data Protection Legislation where there is a significant risk to data subjects that cannot be mitigated and there is no option to terminate the processing then the DPIA must be submitted to the Information Commissioners Office (ICO) for review. The ICO will support the data controller to identify mitigations, or may instruct the data controller to terminate the processing.

Data Protection Impact Assessment Initial Screening

Section 1 - Assessment Details

| | | |
|-----|---------------------------------|---|
| 1.1 | Project/Programme/Process Title | Church of England National HR Information Sharing |
| 1.2 | Form Completion Date | 10/1/2022 |
| 1.3 | Your Name | Robert Hutton |
| 1.4 | Your Job Title | Senior Consultant Inform-Consult |

1.5 Project or change overview, and the personal data activities involved

| |
|--|
| Response Sharing people and human resources information for the purposes listed in Section 2 of the CoE Information Sharing Agreement between the Partner Organisations. |
|--|

1.6 Initial Screening Questions

| 3 | Question | Y | N |
|---|---|---|---|
| 1 | Will the project involve the collection of new information about individuals? | X | |
| 2 | Will the project compel individuals to provide information about themselves? | X | |
| 3 | Will information about individuals be shared with organisations or people who have not previously had routine access to the information? | X | |
| 4 | Will information already held about individuals be used for a purpose for which it is not currently used? | X | |
| 5 | Will the project involve using technology, which may be perceived as being privacy intrusive? E.g. fingerprint readers, facial recognition, voice recording. | | X |
| 6 | Will the project result in making decisions or acting against individuals in ways that can have a significant impact on them? E.g. change of social or medical wellbeing. | | X |
| 7 | Will the information processed be considered personal sensitive data, which is likely to raise privacy concerns? For example, health records. | X | |

If the answer to any of the above questions is **YES**, section 2 **MUST** be completed.

If all the answers are **NO**, you do not need to complete section 2, only sign below and save to the appropriate related project file.

| | |
|---------------------------------------|--------------------|
| Signature <i>Robert Hutton</i> | Date 10/01/2022 |
|---------------------------------------|--------------------|

Section 2 - Privacy Impact Assessment Checklist

Background

Has a DPIA been undertaken for this project (or one similar) before? If so, please give dates and brief details. This should also include the details of the relationship with and Third-Party processors (if applicable) and the relationship with Data Subject/s whose data will be processed.

Response:

No

Project Status

At what stage in the project lifecycle are you completing this DPIA and what is the target deadline for “go live”?

Response:

The DPIA is being undertaken prior to the finalisation of the Information Sharing Agreement (ISA). The aim is to have the key mechanisms in place by the mid-January 2022.

Legal Requirements

Is the project subject to any legal requirements or standards? e.g. Charities Act 2011

Response:

No

Data Involved

The project will use (process) the following data (add rows where required).

| Type of data | Data Source | Data Source Owner | Is the Data Sensitive Personal Data (Y/N) |
|--|-----------------------|-----------------------|---|
| Personal data relating to the Clergy, Lay persons and employees of the Partner Organisations as outlined in the HR information Sharing Agreement | Partner Organisations | Partner Organisations | Yes |

Data Collection

Will the data collection be fair and transparent? Is the data source clearly defined?

| Type of Data | How will the data be collected | How will the reason for data collection be communicated to the individual |
|--|--------------------------------|---|
| Personal data relating to the Clergy, Lay persons and employees of the Partner Organisations as outlined in the HR information Sharing Agreement | Through various processes, | This will be undertaken using a Privacy Notice supplied as required and made available online |

Data Relevancy

Is the data collection limited to what is adequate and relevant?

| Type of Data | Reasons why you need to collect the data, and how it will be used in the project | Is there lawful basis and/or condition for processing the data? | Is a Legitimate Interest Assessment required If so, has this been undertaken |
|---|---|---|--|
| Personal data relating to the Clergy, Lay persons and employees of the Partner Organisations as outlined in the HR information Sharing Agreement | To share people/human resources information between the Partners | Depending on the data and the reason for sharing the following lawful bases will be applied: Consent – (Art 6(1)(a)) Contract (Art 6(1)(b)) Contract – (Art 6(1) (b)) Contract – (Art 6(1) (b)) Public task – (Art 6(1)(e) - Legitimate Interest (Art 6(1)(f)) | Yes – in relation to the Isle of Man |
| Special category Personal data relating to the Clergy, Lay persons and employees of the Partner Organisations as outlined in the HR information Sharing Agreement | to facilitates the sharing of people/human resources information between the Partners | Depending on the data and the reason for sharing the following conditions will be applied: Employment law (Art 9(2)(b)) Legitimate activity Art 9(2)(d)) Legal claims (Art 9(2)(f)) Substantial Public Interest ((Art 9 (2)(g)): Data Protection Act 2018 s. 10(3) | N/A |

Data Source

Will the data be collected from sources other than the data subject?

| Type of Data | Have you sourced the data directly from the individual? (Answer N/A if information gathered from 3 rd party) | What external data source is the information being gathered from? (Answer N/A if sourced directly from individual) | If collecting from an external source – has the individual whose data, you are collecting been informed (either by yourself or the external source) |
|--------------|--|---|---|
| | | | |

| | | | |
|--|-----|--|--|
| Personal data relating to the Clergy, Lay persons and employees of the Partner Organisations as outlined in the HR information Sharing Agreement | Yes | Yes (See List in Appendix A of the HR ISA) | Yes a Privacy Notice will be provided. |
|--|-----|--|--|

Consent

How will consent be obtained, monitored, and managed? Can consent be withdrawn easily and a record of withdrawal maintained? (Add rows where required).

| Type of Data | How will consent be gathered | How and where will the consent be recorded | Is mechanism is in place to renew consent | What mechanism is in place for dealing with the withdrawal of consent? |
|---------------------|--|--|--|--|
| Medical/Health data | Partner Organisations will obtain consent from the data Subjects | Use of an appropriate consent form | Partner Organisations responsible for ensuring this. | Partner organisations are responsible for ensuring this process in accordance with their Privacy notice. |

Additional processes

Will the data be processed for a new purpose not originally specified at collection?

| Type of Data | Is there a lawful purpose for the additional processing? e.g. legal obligation | If personal data will be processed for a different purpose than originally required, will additional consent be required? | How will additional consent be gathered? | How will additional consent be stored and managed? |
|--------------|--|---|--|--|
| n/a | n/a | n/a | n/a | n/a |

Sharing Data

Who do you intend to share the data with? (Name all intended internal and external recipients)?

| Data Title | Who will be given access to the data | Reason for sharing | Is a data processor agreement required for 3 rd parties | If sharing with a 3 rd party processor, are they a GDPR compliant organisation? | Are data subjects aware of the 3 rd party data sharing? |
|------------|--------------------------------------|--------------------|--|--|--|
| | | | | | |

| | | | | | |
|--|--|---|--|-----|---|
| Personal data relating to the Clergy, Lay persons and employees of the Partner Organisations as outlined in the HR information Sharing Agreement | Partners of the ISA; external IT contractors/suppliers | Purposes as listed in Section 2 of the ISA. | Yes. A 3 rd party processing agreement is in place with IT contractors/suppliers. | Yes | Yes. It is included in the relevant Privacy Notice. |
|--|--|---|--|-----|---|

Processing Scale

Will the Data Processing involve the processing of high volumes of data?

| Type of Data | Are there a high number of individuals whose data is being processed within this project? | Does the processing involve a wide range of different data items? E.g. high number of data fields or data items per data subject. |
|---|---|---|
| Personal data relating to the Clergy and employees of the Partner Organisations as outlined in the HR information Sharing Agreement | Yes | Yes, it will include a variety of data items including name, role, contact details, financial information, medical information etc. See List in Appendix A of the HR ISA. |

Transferring data

When obtaining and/or sharing data, how will it be transferred? E.g. via secure webpage, encrypted email.

| Type of Data | Is there an intention to share the data internally with users who previously had no access to this data? | Is there an intention to share the data with 3rd parties external to the institutional Church of England? | Are arrangements in place for the secure electronic and physical transfers of the information being shared? | Will the data be shared outside the UK? | If the data will be shared outside the UK what measures have been taken to make sure the data is handled in compliance with GDPR? |
|--|--|---|---|---|---|
| Personal data relating to the Clergy, Lay persons and employees of the Partner Organisations as outlined in the HR information Sharing Agreement | Yes –internally across the institutional Church of England | No | Yes – there are secure methods of either sharing or uploading information into secure electronic environments | Yes. It will be shared with the Bishops Office in Brussels; the Isle of Man and the Channel Islands | Adequacy Arrangements |

Storage

How will the data be stored and for how long?

| Data Title | How will the data be stored? | How long will the data be retained? | How will the data be erased when redundant? | How will the destruction of copies be ensured? |
|--------------------------|--|---|---|--|
| Safeguarding information | On the dedicated National Safeguarding Case Management System, the national People System and local systems within Partner Organisations | Various in accordance with the relevant retention and disposal criteria | Manual Deletion | Manual checks |

Permissions

How will access to the data be controlled?

| Data Title | Are there sufficient controls over who can administer and use the system on which data will be held? | If the system can be accessed remotely, are adequate protection measures in place? |
|--|--|--|
| Personal data relating to the Clergy, lay persons and employees of the Partner Organisations as outlined in the HR information Sharing Agreement | Yes, the systems have appropriate access controls in place (passwords, 2FA). | All national systems are controlled by 2FA |

Security

Has a Security Risk Assessment been undertaken on the new system? Are robust technical and operational security measures in place? E.g. IT systems updated; staff trained. Do you plan to use live personal data in testing the new system?

Response:

The systems have been evaluated to ensure that the appropriate security measures are in place for maintaining the information.

CCTV

Does the project involve any video surveillance of individuals? If so, what guidance and legislation has been consulted?

Response:

N/A

Corporate/ Organisational Benefits

Does the data processing benefit your organisation or society as a whole? For example will data gathered be used for marketing and/or fundraising activities?

If so what guidance and legislation has been consulted?

Response:

The processing of the data will provide efficiency benefits and enable the Partner Organisations to support the work and mission of the Church of England through effective management of people; it will also enable the publication of the national clergy register.

Section 3 - Risk Assessment

What are the risks to the individuals whose data is being used in this project?

The purpose of this section is to score the risks to personal data used within this project.

| Risk | Current Mitigations | Impact (i) | Likelihood (l) | Risk rating (i x l x 2) | Required Mitigations | Residual likelihood (rl) | Residual risk (ixrlx2) |
|--|--|------------|----------------|-------------------------|---|--------------------------|------------------------|
| Information sharing agreements with Partner Organisations not in place | Information sharing agreement being developed | 2 | 2 | 8 | Finalisation of the ISA, and partner organisations signing up to it. | 1 | 4 |
| The individual Partner Organisations will not have the capability to ensure compliance with information sharing requirements | Partner organisations are required to put in place the organisational and technical measures to comply with data protection legislation. | 2 | 3 | 12 | Each Partner Organisation should ensure that they have the appropriate controls in place to share and receive shared information. | 2 | 8 |
| Loss of control over personal data when being stored. | Systems have appropriate security controls in place. | 3 | 1 | 6 | None | 1 | 6 |
| Data subjects not being provided with details of how their information is being processed therefore breaching the principles of the data protection act. | Privacy Notice being developed for the purpose of sharing information between partner organisations | 2 | 3 | 12 | Finalisation and distribution of the Privacy Notice | 1 | 4 |

| | | | | | | | |
|--|--|---|---|----|--|---|---|
| Loss of control over personal data when being transferred | Sharing is limited to within the partnership organisations. There are mechanisms for safely transferring data between partners, but not all partners currently have access to these methods, more specifically those with limited resources. | 3 | 2 | 12 | At the time data sharing is required, each partner organisation must look to use the safest method of sharing that they have access to, or ensure that they provide suitably secure methods using appropriate software or applications, and train their staff to use them. | 1 | 6 |
| Reputational damage to the Church because of poor information sharing practices | In the process of implementing controls to minimise the risks and therefore reduce the risk of any reputational damage occurring. | 3 | 2 | 12 | Each Partner Organisation should ensure that they have the appropriate controls in place to share information, and that the Partner Organisation that they are planning to share data with has equally appropriate controls in place for protecting the data being shared | 1 | 6 |
| Loss of control over data when being shared; data is shared with unauthorised people, or without a lawful basis | Authorised individuals have been listed in the ISA and all lawful bases have been provided. | 2 | 1 | 4 | Partners will receive additional training on data sharing, and core groups will be reminded about what data sharing controls apply. | 1 | 4 |
| Loss of control over personal data as a result of data being shared unlawfully due a change in legislation or process which is not updated in the ISA. | A period of review is stated in the ISA, and appropriate steps are in place for urgent or required changes to be made when necessary. The Lead Signatory will be advised if the law or processes change that affect information sharing. | 2 | 2 | 8 | All Partners to monitor changes in practice or process and inform the Lead Signatory. The NCIs DPO and the CoE DPO network will monitor changes in the law. Updates will be issued to all partners when necessary. | 1 | 6 |

| | | | | | | | |
|---|---|---|---|----|---|---|---|
| Data subject could be harmed or experience detriment if data is not be shared due to lack of awareness by a Partner organisation that they have entered into a sharing agreement. | The project has communicated with a number of individuals at various levels across all partner organisations. | 3 | 2 | 12 | All Partner organisation to ensure that the documents and agreements are shared with relevant individuals and that appropriate handover is done if senior officers leave the organisation; the NCIs will inform the HR, DSA, DPO and Communications networks. | 1 | 6 |
|---|---|---|---|----|---|---|---|

Section 4 – Review and Sign-Off

DPO comments

| |
|---|
| Comments: |
| Although there overall risk rating is medium, there are a number of mitigations required from all Partner organisation to achieve this risk level. Partner Organisations must take responsibility for ensuring that they are compliant with the requirements of Information Sharing as outlined in the ISA, and are required to undertake necessary actions to mitigate risks in their organisations. If there any risks that cannot be mitigated this must be brought to the attention of the lead organisation. |

Required Mitigations

| # | Required Mitigation to achieve residual risk |
|---|--|
| 1 | Finalisation of the ISA, and Partner Organisations signing up to it. |
| 2 | Finalisation and publication of the HR Information Sharing Privacy Notice. |
| 3 | Each Partner Organisation should ensure that they have the appropriate controls in place to share and receive shared information. |
| 4 | Partner organisations should train their staff on keeping data secure and ensure all storage repositories, including for paper storage, are secure and only accessed by authorised individuals |
| 5 | At the time data sharing is required, each partner organisation must look to use the safest method of sharing that they have access to, or ensure that they provide suitably secure methods using appropriate software or applications, and train their staff to use them. |
| 6 | Each Partner Organisation should ensure that they have the appropriate controls in place to share information, and that the Partner Organisation that they are planning to share data with has equally appropriate controls in place for protecting the data being shared |
| 7 | Partners will receive additional training on data sharing, core groups will be reminded about what data sharing controls apply. |
| 8 | All Partners to monitor changes in practice or process and inform the Lead Signatory. The NCIs DPO and the CoE DPO network will monitor changes in the law. Updates will be issued to all partners when necessary. |
| 9 | All Partner organisation to ensure that the documents and agreements are shared with relevant individuals and that appropriate handover is done if senior officers leave the organisation; the NCIs will inform the HR, DSA, DPO and Communications networks. |

Final Project Risk Rating (Mark relevant box)

Note: In the event of one or more the residual risks being identified as high, then this will automatically rate the whole project as a high risk and it may be submitted to the ICO for evaluation.

| Risk level | Action | Tick here |
|--------------------|---|-----------|
| Low Risk (2-6) | Project can proceed | |
| Medium Risk (8) | Minor actions are required before proceeding | x |
| High Risk (12 -16) | Significant actions required may need to be submitted to the ICO for evaluation | |

Review - Sign Off

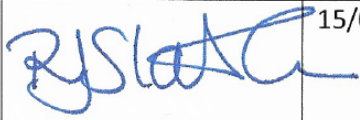
| Position | Name | Date |
|--------------------------------|-----------------|----------|
| NCIs Director of Data Services | Fraser McNish | 24/01/22 |
| NCIs Head of HR Operations | Simon Cook | 24/01/22 |
| NCIs Data Protection Officer | Madi McAllister | 19/01/22 |

Authorisation Levels

The DPIA must be signed off in Section 4 by the following roles according to the assigned risk level:

| | |
|---------------------|--|
| High Risk | Senior Information Risk Owner (SIRO) or in cases where Risks cannot be mitigated submitted to ICO for review or the project is terminated. |
| Low and Medium risk | Information Asset Owner(s)/ Project Manager |

DPIA – Approval and Final Sign Off

| Position | Name | Signature | Date |
|---|-------------------|--|----------|
| Chief Operating Officer, Church of England Central Services (Lead Signatory) | Rosie Slater-Carr |  | 15/03/22 |