# University of Essex Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (**DPIA**) is a process to help the University of Essex identify and minimise the data protection risks of a project. Staff **must** do a **DPIA** for processing that is likely to result in a high risk to the rights and freedoms of individuals. This includes some specified types of processing such as the processing of Special Category or Criminal Convictions data. The need to complete a DPIA may be identified by you and/or the Data Protection Officer during project planning, project initiative, procurement and/or following the completion of a ROPA (Record of Processing Activities), for example.

## Instructions for use

This DPIA should be completed by the person responsible for the project and/or processing of any personal data and any other key business owners to discuss the task, its importance and understand exactly what personal data is being processed, why, shared with whom, etc. Further guidance on filling in the DPIA can be found at the end of this document. Ideally you will start completing the DPIA yourselves, but if you require any further assistance, please contact the Data Protection Officer: [**dataprotectionofficer@essex.ac.uk**](mailto:dataprotectionofficer@essex.ac.uk)

### Section 1 – Project outline

|  |  |
| --- | --- |
| Project/Software title |  |
| **Project lead** |  |
| **Department/Section** |  |
| **Form completed by (if different from above)** |  |
| **Date completed** |  |

|  |
| --- |
| **Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA** |
|  |

#### Basis for assessment

|  |  |  |
| --- | --- | --- |
| Example (but please feel free to add any others that are relevant) | Yes | No |
| Use of new technologies |  |  |
| Processing personal data without providing a privacy notice directly to the individual |  |  |
| Processing personal data in a way which involves tracking individuals’ online or offline location or behaviour through use of third-party video conferencing solutions |  |  |
| Innovative technological or organisational solutions developed by these tools |  |  |
| This project involves the processing of personal data |  |  |

## Section 2 – Privacy considerations: fair and lawful processing

|  |  |
| --- | --- |
| 2.1 Data  Please specify the type of data to be used/shared and by whom |  |
| **2.2 Personal Data**  What data/information is/will/may be used/shared for this project? |  |
| **2.3 Special category data**  What sensitive data/information is/will be used/shared for this project? Is it:   * Data revealing racial or ethnic origin * physical or mental health or condition * sexual life / sexual orientation * religious / other beliefs * political opinions * trade union membership * biometric or genetic information used can identify an individual |  |
| **2.4 Criminal convictions data**  Personal data relating to criminal convictions and offences or related security measures, including criminal activity, allegations, investigations and proceedings. Can include restrictions or civil measures which can lead to a criminal penalty. |  |
| **2.5 Use of data** | For Sections A and B below, what lawful basis will the University of Essex rely on under GDPR?  **List all that apply in the next box**   * Data subject has given their **consent** * Data subject is party to a **contract** with the University of Essex * The University of Essex has a **legal obligation** to process the data * The data subject’s vital interests are at stake and they cannot give consent * The data processing is part of the University of Essex’s **public task** as an education provider * The data processing meets a **legitimate interest** for the University of Essex or another party   The processing of Special Category Data requires a legal basis under [Article 6 of the UK GDPR](https://www.legislation.gov.uk/eur/2016/679/article/9) and a separate condition for processing under Article 9 of UK GDPR. In some cases a substantial public interest condition from the Data Protection Act 2018 is also required.  The processing of Criminal Convictions data requires a substantial public interest condition from the Data Protection Act 2018. |
| **Section A – personal data** | List all which apply from the above list. |
| **Section B – special categories of personal data and criminal convictions data** |  |
| **2.6 Consent**  If consent is the lawful basis being used where will the consent be recorded once obtained? Will it be explicit?  NB – consent to process personal data is separate to consent to participate in research. |  |
| **2.7 Informing subjects**  Please outline what steps will be taken to inform individuals how the information about them will be used |  |

|  |  |  |
| --- | --- | --- |
| 2.8 Technologies | Yes | No |
| Does the project involve new or inherently privacy-invasive technologies? i.e. Radio frequency identification (RFID) tags, biometrics, phone location or GPC |  |  |

|  |
| --- |
| If yes, please outline measures that will be taken to reduce the impact on individual’s privacy |
|  |

## Section 3 – Stakeholder analysis

|  |  |
| --- | --- |
| **3.1 Stakeholders**  Please state the internal or external stakeholders on which this project has an impact and outline their involvement/contribution |  |
| **3.2 Consultation with data subjects**  Has any consultation with data subjects taken place? What was the outcome/feedback? |  |
| **3.3 Training**  What (if any) training and/or additional guidance will staff be required to undertake before the project starts? |  |

## Section 4 – Data quality and records management

|  |  |
| --- | --- |
| **4.1 Data Collection**  Will new information be collected? If so, please provide details  Note – ‘new data’ doesn’t necessarily mean a new type of data but could refer to new ways of processing existing data. |  |
| **4.2 Data Volume**  Will the project result in the handling of new data about a significant number of people, or a significant change in the population coverage? |  |
| **4.3 Linking systems**  Does the project involve the linking of personal data with data in other systems/locations within the University or externally? |  |
| **4.4 Accuracy**  How will the information be kept up to date and checked for accuracy and completeness? |  |
| **4.5 Retention**  What arrangements are in place to ensure the data is not kept longer than necessary? |  |
| **4.6 Security**  What arrangements are in place to keep the data secure? |  |
| **4.7 Retention guidance**  Does the University of Essex’s retention policy specify a retention period for this information?  If so, please outline: |  |
| **4.8 Destruction**  How will the information be securely destroyed when no longer required? |  |
| **4.9 Rights of Access**  What steps are in place to ensure information can be provided for a data subject access or access to records request? |  |

## Section 5 – Transfers/data mapping

|  |  |
| --- | --- |
| **5.1 Data location**  Where will the information be kept/stored/accessed? |  |
| **5.2 Transfer**  Will any information be sent/accessed off site? If so, where to? |  |
| **5.3 Transfer method**  Please state by which method the information will be transferred |  |
| **5.4 Transfer country**  Where will the information be transferred?   * Outside the UK * Inside the EEA (inc. the UK) * Outside the EEA |  |
| **5.5 Transfer protection**  If information is to be transferred outside the UK or EEA, what has been done to ensure an adequate level of protection for the data? |  |

## Section 6 – Third party access

|  |  |
| --- | --- |
| **6.1 Third parties**  Please give the name(s) of any third parties involved.  Note: If it is planned to use a company as a data processor (processing data on behalf of the University as the data controller) then you need to add their details to this section. |  |
| **6.2 Third parties**  System supplier contact details (including name and contact of the Data Protection Officer if possible) |  |
| **6.3 Information sharing agreements**  Has an information sharing agreement been developed and signed off by both parties?  Note: If we are sharing data with a partner (such as a local authority) an ISA should be in place. An ISA is not required for a data processor (see next section) |  |
| **6.4 Third parties contracts**  Do contracts contain Data Protection clauses and if so, are they fully compliant with the University of Essex’s data protection obligations (see contract checklist which can be provided by the DPO)? |  |
| **6.5 Third parties location**  Please provide information about the location of any third parties |  |
| **6.6 Data location**  Please provide information about the location of the data associated with third parties?  NB – this can be different from the location of the third party itself. |  |
| **6.7 Third party physical security**  Please provide any information about third party security measures. |  |

## Section 7 – Privacy risk assessment

| Risks  *(please add any others that might be relevant)* | Potential impact  E: Catastrophic  D: Severe  C: Medium  B: Minor  A: None | Likelihood  E: Almost certain  D: High  C: Medium  B: Small  A: Negligible | Risk Rating  Impact x Likelihood = Rating | Control Measures so Risk is   * Eliminated * Reduced * Accepted | Residual Risk Rating |
| --- | --- | --- | --- | --- | --- |
| Example: Unauthorised access | E: Catastrophic = A University dataset is publicly accessible e.g., on the internet | E: Almost certain = The data is being stored on an unencrypted website | E x E = 25 | After a review with the supplier information will not be stored on a external website, it will instead be accessed in a password protected box file. See updated risk assessment:  B: Minor = A member of staff at the University has been sent a record of limited personal data  B: Small = The data is being stored in a password protected Box file  Risk is reduced to B x B = 5 | Reduced |
| Example: *Misuse of service and authorisation* | E: Catastrophic = An individual may access personal data and use it for a non-university purpose | D: High = The information was going to be shared with a third party without a contract | E x D = 24 | All those involved in the project have contracts and data protection training. A contract has been implemented to ensure data can only be used for purposes defined by the University. | Reduced |
| Unauthorised access |  |  |  |  |  |
| Unauthorised sharing of personal data |  |  |  |  |  |
| Off campus access is misused |  |  |  |  |  |
| Unauthorised file transfer |  |  |  |  |  |
| Unauthorised personal recording, copying, taking screen shots of data |  |  |  |  |  |
| Misuse of service and authorisation |  |  |  |  |  |
| Sharing the University’s security log on details |  |  |  |  |  |
| External cyber threat compromises the [insert name of third party]’s service |  |  |  |  |  |
| Reputational risk for non-compliant activity |  |  |  |  |  |

## **University Risk Matrix**

### Scoring system

The scoring system looks at the Impact of an incident versus the Likelihood of it occurring.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Impacts | Likelihood  A Negligible | Likelihood  B Small | Likelihood  C Medium | Likelihood  D High | Likelihood  E Almost certain |
| E Catastrophic | 15 | 19 | 22 | 24 | 25 |
| D Severe | 10 | 14 | 18 | 21 | 23 |
| C Medium | 6 | 9 | 13 | 17 | 20 |
| B Minor | 3 | 5 | 8 | 12 | 16 |
| A None | 1 | 2 | 4 | 7 | 11 |

## Sign off and record outcomes

|  |  |
| --- | --- |
| Record outcomes | Sign off |
| Measures approved by |  |
| Assessment reviewed by |  |
| Residual risks approved by |  |
| Date |  |
| DPO advice |  |
| Comment |  |
| First review date (6 months post approval) *see guidance below* |  |
| This DPIA will be reviewed following any changes associated with the DPIA project. Last reviewed |  |
| Summary of key changes at review stage |  |

## **Guidance on filling out the template**

### Section 1 - Project outline

Describe what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

The basis for assessment help classify the type of data processing into broad categories and helps the Data Protection Officer highlight specific questions in the assessment. The bases provided on the form are examples but if there are any other relevant bases, please feel free to add a line to the table providing further details.

### Section 2 - Privacy Considerations: Fair and Lawful processing

2.1-4 This section defines the type of data you are processing in the project and how this relates to the legal framework around data protection.

2.5 The University needs to have identify at least one of the six available legal bases for processing the personal data. Identifying if any Special Category or Criminal Convictions data is involved is crucial, as these types of data require additional legal bases from the GDPR and the Data Protection Act 2018.

The Data Protection Officer will assist you on these sections. The key for the project is to include all types of data collected.

2.6 Consent is one of the legal bases available and, if used, we need to ensure that the consent is recorded. If consent is not the legal basis this section can be left blank.

2.7 Informing data subjects may be as simple as directing them to a privacy notice at the point the data is collected, but the University needs to ensure that this step is fully considered.

2.8 This section is to highlight any new technologies that might be involved in the project. Biometric data (face or fingerprint recognition) and functionality such as location tracking are common examples but there may be others which can be added if necessary.

### Section 3 - Stakeholder analysis

Please state the internal or external stakeholders on which this project has an impact and outline their involvement /contribution.

Consultation with data subjects is not always possible but it can be a really valuable exercise both in informing the University's project and building trust with data subjects. An example would be a survey with questions such as - 'Would you be happy with your cafeteria orders to be delivered by an app on your phone?' or 'Do you support the use of CCTV in the University's communal areas?' The feedback could be vital in assessing the privacy risks of the project.

### Section 4 - Data Quality & Records Management

Managing data and records effectively is vital for the University for both compliance and efficiency reasons. Whilst the immediate pressures of getting a project off the ground are considerable, this section is really looking at the long-term picture for how the data processed as part of the project will be managed in a year or five years’ time.

Refer to the [University’s Retention Schedules](https://www.essex.ac.uk/staff/freedom-of-information/policies-and-procedures#retention). Further information can be accessed from the [JISC Records Management webpages](https://beta.jisc.ac.uk/guides/records-retention-management).

### Section 5 - Data transfers

5.1-3 If we are transferring personal data between parties we need to ensure that this data is transferred securely. We should be considering measures such as encrypted emails and attachments, the use of ZendTo, the University’s secure file-sharing service, SharePoint sites and other approaches to ensure data is not subjected to unauthorised access or loss.

5.4-5 Increasingly information is no longer held 'onsite' in hard copy or University servers and is often stored in 'the cloud' by third party providers. The benefits in resilience, backup and security are clear but there are important compliance considerations and these need to be identified in this section, particularly if the data is stored outside the UK or EEA, when additional safeguards may need to be in place.

### Section 6 - Third party access

If we are using or planning to use a data processor to process data on our behalf, we should provide information about this arrangement in this section. If we are processing the data with a partner (such as a local authority) then we should ensure that an information sharing agreement is in place.

### Section 7 - Risk assessment

This is a simple matrix for quantifying risks in your project. Some may not apply. These risks can also be added to your wider project risk register if you have one. Please remove the two examples provided on the template when completing the risk matrix.

### Section 8 - Sign off and Record Outcomes

This section allows the business lead on the project to record approval and acknowledge any points raised by the Data Protection Officer in regard to compliance.

Having a review date is vital. A DPIA is a 'living document'; it may need to be updated at particular staging points of a project, such as procurement completed or contractor replaced.

The first review should be undertaken six months or at an appropriate time following approval and then as and when a project changes. In relation to software it is also a good idea to revisit the DPIA when software comes up for renewal as this allows any new risks to be identified, assessed and mitigated where necessary.

## Further information

Our Information Assurance webpage on [Data Protection Impact Assessments](https://www.essex.ac.uk/staff/working-with-information-and-data/data-protection-impact-assessments) and the [Information Commissioner’s Office website](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-impact-assessments/), are also a useful resource in completing DPIA’s.

For further information, please contact the Data Protection Officer at [dataprotectionofficer@essex.ac.uk](mailto:dataprotectionofficer@essex.ac.uk)