How to conduct a Data Protection Impact Assessment (DPIA)

This guidance is for any member of University staff tasked with completing a DPIA. It accompanies the University's online assessment tool and explains how to complete the DPIA using the tool.
You will need to use this guidance:

- When intending to start a new project involving personal data
- When using personal data already collected for a new purpose incompatible with the purpose for which they were collected.

Definitions

- Personal data
- Special categories of personal data
- Data subject
- Processing
- Data processor
- Data controller

Completing the DPIA

The DPIA provides you with a mechanism to accompany the entire life cycle of the project from the original concept to the actual implementation and first use. Thus, the DPIA does not constitute a one-off exercise but rather will be relevant throughout the implementation of your project.

1. What is a DPIA?

A DPIA is:

- A tool/process to assist organisations in ensuring that all activities involving personal data are proportionate and necessary
- A tool/process to help with identifying and minimising the privacy risks of new projects, systems or policies
- A type of impact assessment conducted by an organisation, auditing its own processes to see how these processes affect or might compromise the privacy of the individuals whose data it holds, collects, or processes

A DPIA is designed to accomplish four goals:

- Ensure conformance with applicable legal, regulatory, and policy requirements for privacy;
- Determine any potential risks the project might have to individuals' privacy;
- Evaluate protections and alternative processes to mitigate or eliminate these potential privacy risks; and
- Provide the necessary evidence in the case of any data subject complaints about the project.

2. When do I need to carry out a DPIA?

When you plan to:

- embark on a new project involving the collection of personal data;
- introduce new IT systems for storing, accessing or otherwise using personal information;
- participate in a new data-sharing initiative with other organisations;
- create new policies that affect individuals;
- initiate actions based on a policy of identifying particular demographics;
- use existing data for a “new and unexpected or more intrusive purpose”

Examples:

- Sensors under assigned staff desks to monitor frequency of use.
- Body-worn cameras for security staff.
- Deciding whether you have sufficiently anonymised an HR dataset to retain it for statistical use
- Automatic video and audio recording of lectures.
- Amalgamation of HR and Payroll computer systems and digitisation of HR records.
- Sharing student data with new third parties.
- Installing a CCTV system in the University Library reading room.
- Buying a CRM system.
- Writing a new HR policy

Using a DPIA to review or audit an existing system or activity

If an existing activity or system that processes personal data might have intrinsic risks and no DPIA has been done at the design stage, then it might be good to do a DPIA. The following criteria give you a rough guide as to when you should consider conducting a retrospective DPIA:

- Processing of special category personal data
- Processing of financial data
- Using external software
- Using a surveillance system
- Processing data that, if disclosed, could lead to discrimination or other harm
- Processing data that, if disclosed, could lead to loss of reputation for data subjects or University
- Review an existing system or activity if there are any concerns about privacy intrusion or security vulnerabilities

3. What are the risks of not carrying out a DPIA?

- The need to redesign all or major parts of the system/project.
- Collapse of the project due to adverse publicity.
- Loss of trust or reputation.
- Breach of data protection legislation and significant fines.

- Subsequent regulatory action by the Information Commissioner's Office (ICO) as a result of complaints received from data subjects.
- Individuals subjected to fraud, identity theft and distress.
- Legal action taken by individuals to sue the University.

4. How to carry out a DPIA

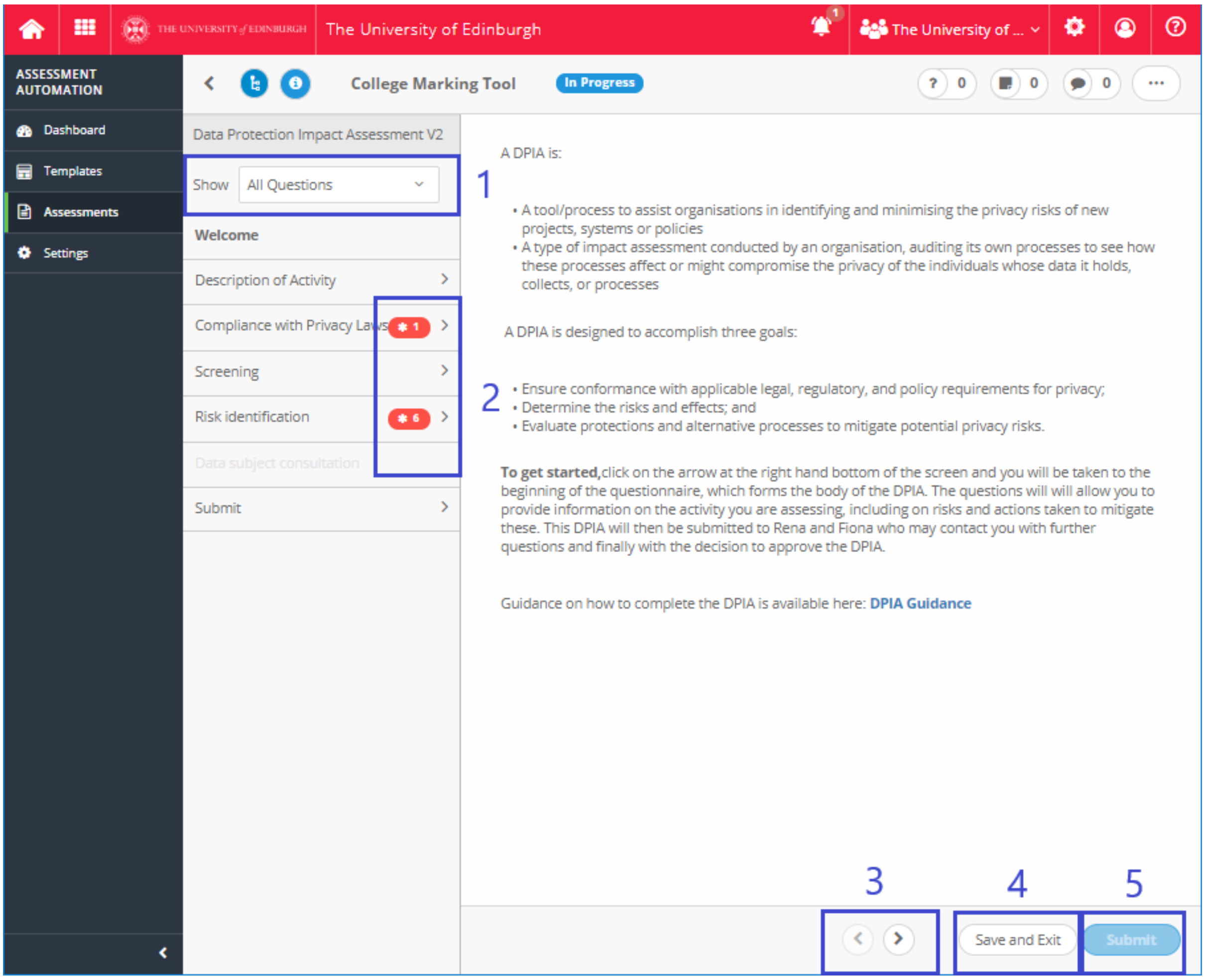
In the remainder of the guidance below, yellow boxes contain instructions on the use of the online tool, while regular text provides legal guidance.

The online tool will provide four distinct sections that require to be completed, namely;

- Description of Activity
- Compliance with Privacy Laws
- Screening
- Risk Identification

The purpose of the first three stages is to work out whether a full DPIA is necessary and, if that is the case, how it should be scaled. This process should ensure that the time and effort you put into carrying out a DPIA is proportionate to the risks.

The following offers a guide in the navigation of the online tool:



A DPIA is:

- A tool/process to assist organisations in identifying and minimising the privacy risks of new projects, systems or policies
- A type of impact assessment conducted by an organisation, auditing its own processes to see how these processes affect or might compromise the privacy of the individuals whose data it holds, collects, or processes

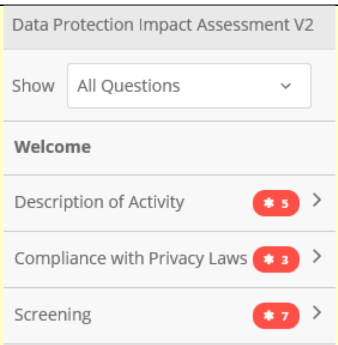
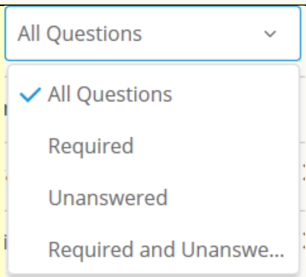
A DPIA is designed to accomplish three goals:

- Ensure conformance with applicable legal, regulatory, and policy requirements for privacy;
- Determine the risks and effects; and
- Evaluate protections and alternative processes to mitigate potential privacy risks.

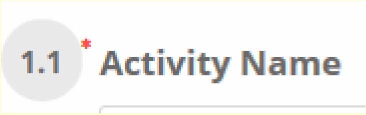
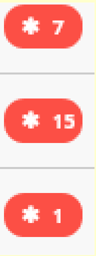
To get started,click on the arrow at the right hand bottom of the screen and you will be taken to the beginning of the questionnaire, which forms the body of the DPIA. The questions will will allow you to provide information on the activity you are assessing, including on risks and actions taken to mitigate these. This DPIA will then be submitted to Rena and Fiona who may contact you with further questions and finally with the decision to approve the DPIA.

Guidance on how to complete the DPIA is available here: **DPIA Guidance**

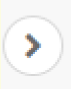
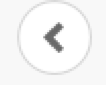
1

Selecting a section to complete To select a specific section, click on one of the appropriate section descriptions within the column titled ‘Data Protection Impact assessment’. However, it is recommended that each section is completed in the order they are defined. Please note that not all questions are visible in all sections at the beginning of an assessment. A further filter is available to ease the identification of questions to be answered. By selecting the drop down associated with the Show option	 Data Protection Impact Assessment V2 Show All Questions Welcome Description of Activity ✱ 5 Compliance with Privacy Laws ✱ 3 Screening ✱ 7
	 All Questions ✓ All Questions Required Unanswered Required and Unanswe...

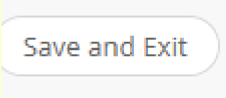
2

Mandatory Questions Please note that any of the numbered questions containing a red asterisk, indicates that this is a mandatory question. All mandatory questions must be answered before it will be possible to submit the DPIA for review. For information, the asterisk **will remain in place** even after the question has been completed.	 1.1 * Activity Name
Progress of DPIA The number displayed within the orange box indicates the number of mandatory questions still to be answered in each section. This number may change based on the answers given, and more questions may then become available.	 ✱ 7 ✱ 15 ✱ 1

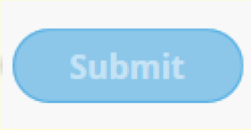
3

To continue through the DPIA Once you have finished the section, click on the next button, indicated by the little **arrow at the bottom of the screen,** next to the 'Save and Exit' button. This will take you to the next section	
To return to the previous section Click on the previous button, indicated by the little **arrow at the bottom of the screen.** This will take you to the previous stage	

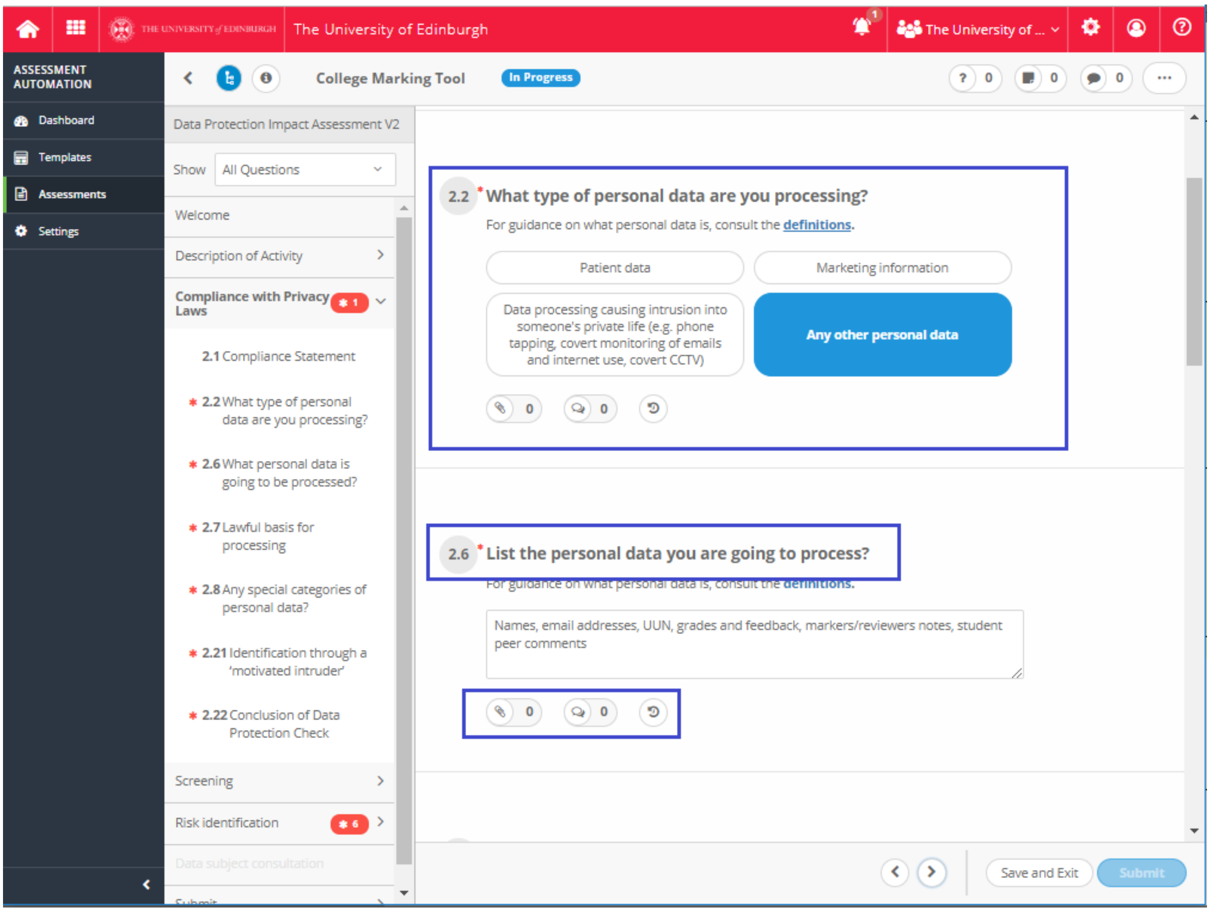
4

To exit You can, at any time, click on '**Save and Exit'**. When you want to continue work on the DPIA, just click on the link in the email again.	

5

Submitting your DPIA Click the 'Submit' button at the bottom right corner of the screen. Confirm that you indeed have finished your DPIA and wish to submit it.	

The following offers a guide to the questions and to the comments functions:



The University of Edinburgh

The University of ...

ASSESSMENT AUTOMATION

Dashboard

Templates

Assessments

Settings

College Marking Tool

In Progress

Data Protection Impact Assessment V2

Show: All Questions

Welcome

Description of Activity

Compliance with Privacy Laws (1)

2.1 Compliance Statement

* 2.2 What type of personal data are you processing?

* 2.6 What personal data is going to be processed?

* 2.7 Lawful basis for processing

* 2.8 Any special categories of personal data?

* 2.21 Identification through a 'motivated intruder'

* 2.22 Conclusion of Data Protection Check

Screening

Risk identification (6)

Data subject consultation

Submit

2.2 * What type of personal data are you processing?

For guidance on what personal data is, consult the definitions.

Patient data | Marketing information

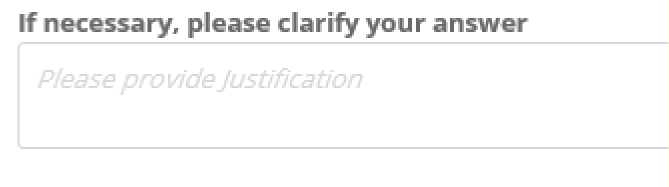
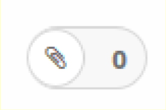
Data processing causing intrusion into someone's private life (e.g. phone tapping, covert monitoring of emails and internet use, covert CCTV) | Any other personal data

2.6 * List the personal data you are going to process?

For guidance on what personal data is, consult the definitions.

Names, email addresses, UUN, grades and feedback, markers/reviewers notes, student peer comments

Save and Exit | Submit

Textboxes - 'If necessary clarify your answer' These textboxes are not mandatory – if no clarification is required, then leave the textbox empty.	 If necessary, please clarify your answer Please provide Justification
Attaching documents If you want to attach documents, click on the **left icon under the textbox** depicting a paperclip. The number next to the icon, indicates the number of attachments	

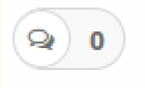
Comments

To add comments for the approver's attention
Click on the middle button under the textbox, the '**Comments'** icon button. The **Comments** pane appears.

Enter the text you want to send to the approver, then click the '**Send'** button.

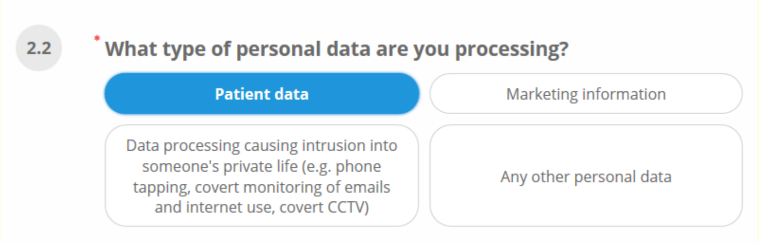
The number next to the icon, indicates the number of comments added

Note: If a DPIA is released under FOI, this will include any comments you make.

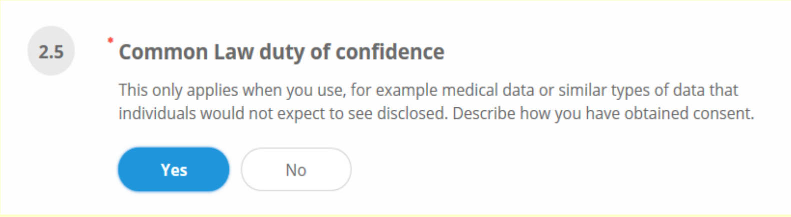


Multiple Choice Questions

On occasions, a number of options will be presented. On selecting the appropriate option, the selected item will be highlighted in blue.
In certain circumstances, the selected answer will dictate the following questions to be answered


2.2 * What type of personal data are you processing?

- Patient data
- Marketing information
- Data processing causing intrusion into someone's private life (e.g. phone tapping, covert monitoring of emails and internet use, covert CCTV)
- Any other personal data

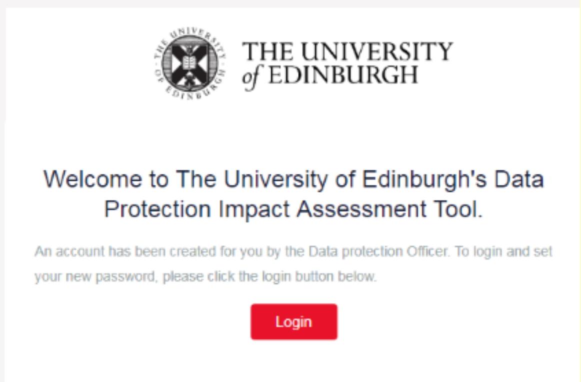

2.5 * Common Law duty of confidence

This only applies when you use, for example medical data or similar types of data that individuals would not expect to see disclosed. Describe how you have obtained consent.

The following provides a step-by-step guidance through the DPIA:

Complete user account set up

Click the red **'Login' button** on the link you have been emailed to launch the DPIA tool. You will be taken to the login screen to enable you to confirm your system account by creating your own system password

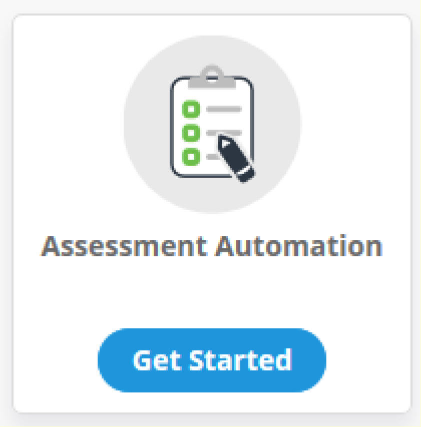

THE UNIVERSITY of EDINBURGH

Welcome to The University of Edinburgh's Data Protection Impact Assessment Tool.

An account has been created for you by the Data protection Officer. To login and set your new password, please click the login button below.

Accessing the DPIA tool

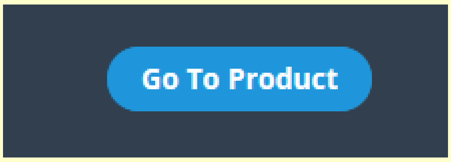
Click the blue **‘Get Started’ button** to launch the DPIA tool.



Launching the DPIA tool

Click the blue **‘Go To Product’ button** to launch the DPIA tool.

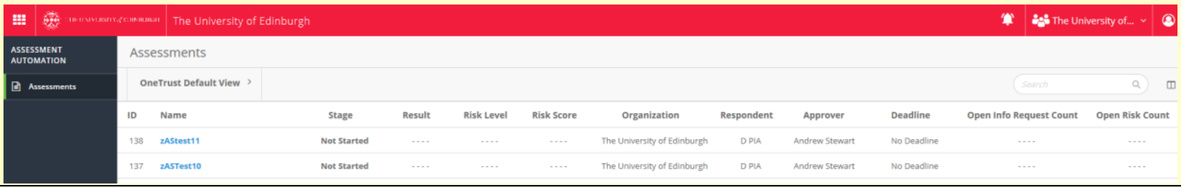
Note. A very high level overview of the product can be viewed by opening the video link on the screen



Viewing assigned Assessment(s)

Having accessed the product, this screen displays all DPIA’s assigned to you as an individual

Click on the Name field to launch the actual assessment



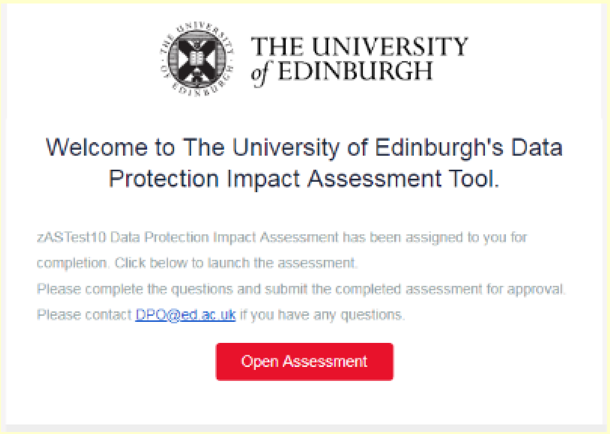
Assessments

OneTrust Default View ›

ID	Name	Stage	Result	Risk Level	Risk Score	Organization	Respondent	Approver	Deadline	Open Info Request Count	Open Risk Count
138	zAStest11	Not Started	----	----	----	The University of Edinburgh	D PIA	Andrew Stewart	No Deadline	----	----
137	zASTest10	Not Started	----	----	----	The University of Edinburgh	D PIA	Andrew Stewart	No Deadline	----	----

Starting the Assessment

Click the red **‘Open Assessment’ button** on the link you have been emailed to launch the DPIA tool. You will be taken to the start page of your assessment, which also includes a link to this guidance.



Welcome to The University of Edinburgh's Data Protection Impact Assessment Tool.

zASTest10 Data Protection Impact Assessment has been assigned to you for completion. Click below to launch the assessment.

Please complete the questions and submit the completed assessment for approval.

Please contact DPO@ed.ac.uk if you have any questions.

Stage 1: Description of Activity

Describing the project

In the left panel, click on ‘**Description of activity**’. Complete all fields as they are all currently deemed as mandatory.

Begin by outlining the project and listing the purpose and objectives and benefits to the University or the staff/students/etc. affected by the project. As well as providing a clear and well-argued case for the project as a whole, it should also highlight those features that may have the potential for the biggest impact upon privacy.
Next, make a preliminary assessment for data usage by mapping data flows:

- How is the information collected, stored, used and deleted?
- What information is used?
- What it is used for?
- Who will have access to it?

This gives you an understanding how the information is going to be used. The mapping can be done in the form of a flow chart, an information register, or a project design brief.
Then, begin to identify activity stakeholders (for example project team and software provider) and the data subjects (the groups affected by the project, such as students, staff or visitors) - note that project stakeholders do NOT include the DPO. Rather, they can be:

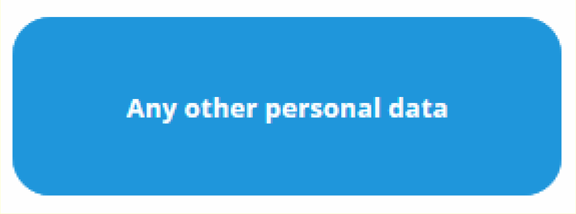
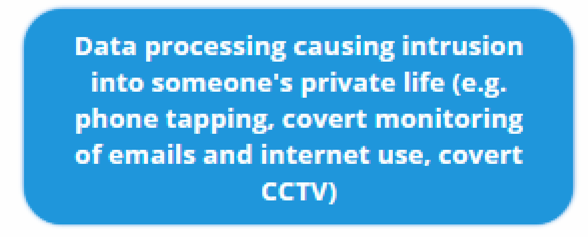
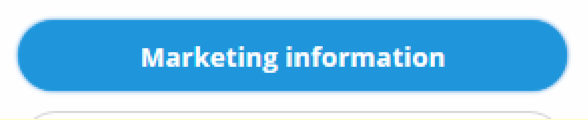
- school/College/Department using the project;
- project officers;
- IS, if involved, or:
- external organisations.

Next, conduct a so-called environmental scan to find external examples. Look around - both within and outside the University – to gather information from previous activities of a similar nature (particularly where the same or similar technology has been used) to see whether there are any lessons you can draw upon or whether a DPIA has already been conducted by somebody else for your activity.

Stage 2: Compliance with Privacy Laws

Every project must be compliant with privacy laws. Even if after stage 3, where you will be asked screening questions, you reach the conclusion that no full DPIA is required, your project must go through a data protection check.

This second stage allows you to examine the project as a whole to ensure that you comply with all six data protection principles, that you have, for example, a legal basis and that what you want to do is covered in a privacy notice. By checking the legislation, you ensure that your project is compliant with all the relevant privacy and data protection legislation that apply. Also, if applicable, state which privacy notice covers your activity – though there is no need to add a link to the privacy notice.

Type of personal data In question 2.2, you will be asked what type of personal data you are processing.	
If you only process ordinary personal data – no patient data, no data that may intrude into somebody's private life and no data for marketing purposes – then you will be directed to question 2.6.	 Any other personal data
If you use data that could be considered an intrusion into somebody's private life, you will be directed to question 2.3, where you will be asked to consider the Human Rights Act.	 Data processing causing intrusion into someone's private life (e.g. phone tapping, covert monitoring of emails and internet use, covert CCTV)
If you use personal data for marketing, you will be directed to question 2.4 and asked about PECR compliance.	 Marketing information
If you use patient data, you will be directed to question 2.5 where you will be asked to consider the common law duty of confidentiality.	Patient data

If your planned processing activities are likely to cause an intrusion into somebody's private, life, Article 8 of the Human Rights Act (HRA) comes into play. Article 8 protects the right to a private and family life. This can include reading the private emails an employee sends from their work email account, phone tapping, or insisting that every employee be contactable during their annual leave.

The common law duty of confidentiality is a law that sits beside the GDPR and needs to be considered separately. Essentially it means that someone shares personal information in confidence and expects that it be kept 'secret'. This usually applies only when patient data obtained through or from the NHS are used. The general position is that, if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the data subject's consent.

International transfer

In question 2.16, you will be asked whether you are sending personal data outside the EEA. If you click 'no', you will be directed to question 2.21.

If you click 'yes', you will be directed to question 2.18, which asks whether you send the data to one of the 'adequate', 'safe' countries. If you click on one of these countries, you will be directed to question 2.21.

If you click 'none of the above', you will be directed to question 2.19, where you will be asked which countries you send the data to. Then, in question 2.20, you will be asked for the safeguards in place for sending the data to that country/these countries.

Please also see Stage 4: Risk Identification

The 'motivated intruder test'

One of the most frequently used methods of protecting datasets is by attempting to anonymise the data. The 'motivated intruder' test allows you to check if what you have done is sufficient or whether there is a real risk of individuals still being identified. The test is also applied for photography, for example, where you might take photos at an event to put onto the internet. Key question is the motivation: whether anyone would have the motivation to carry out re-identification.

The 'motivated intruder' is going to be a person who starts without any prior knowledge but who wishes to identify the individual whose personal data you have anonymised. This test is meant to assess whether there would actually be a 'motivated intruder' and whether the 'motivated intruder' would be successful. The basis is that this 'motivated intruder' has access to resources such as libraries and the internet, but does not have computer hacking skills and criminal intention such as burglary.

Thus, your deliberations will be:

- Is the data likely to attract a 'motivated intruder? This attraction could be
  - finding out personal data about someone else, for nefarious personal reasons or financial gain;
  - the possibility of causing mischief by embarrassing others – the more sensitive the data is (e.g. health information), the more likely it is to attract a motivated intruder
  - revealing newsworthy information about public figures;
  - political or activist purposes, e.g. as part of a campaign against a particular organisation or person; or
  - curiosity, e.g. a local person's desire to find out who has been involved in an incident shown on a crime map.
- What is the risk of jigsaw attack, i.e. piecing different bits of information together to create a more complete picture of someone? Does the information have the characteristics needed to facilitate data linkage – e.g. is the same code number used to refer to the same individual in different datasets?
- What other 'linkable' information is available publicly or easily?

- What technical measures might be used to achieve re-identification?

Data subjects' rights

Next, you need to consider whether you will or need to be able to comply with subject rights. This means that you will need to explain whether you can provide personal data in response to a subject access request (SAR) or whether you won't have to as the so-called 'Golden Copy' of the data is held elsewhere and you are only using a copy of the data – the Data Steward of that area will respond to the request. Guidance on handling SARs can be found here.

You will also need to choose whether you can comply with a request for erasure or restriction of processing, or whether you can apply an exemption. All possible exemptions are listed for you to choose from. For help with deciding whether an exemption applies, consult chapter 11 of the Data Protection Handbook, which can be found here.

Finally, you must state how you will deal with a data protection breach, should the situation ever arise. Guidance on how to respond to a breach can be found here.

If you have any doubt, obtain advice from your local data protection champion or the Data Protection Officer.

Data Protection Champions

Data Protection Officer contact details

Finally, decide whether the answers you have provided show that the activity is data protection compliant by answering question 2.22.

Stage 3: Screening

Answer all questions with 'yes' or 'no'. Should you need to provide more detailed information to explain the project, do so.

If you have answered one or more of the questions with 'yes', you will need to carry out a full DPIA. Looking at the answers you've given, you should already get an understanding of where the privacy risks are. Always keep in mind: the purpose of the DPIA is to minimise privacy risk to the highest possible extent!

If all questions are answered with 'no' and you don't need to do a DPIA, remember that the privacy law compliance check will need to be a living document until the project is implemented and a final check will need to be conducted at implementation stage.

If you have concluded that a DPIA is warranted, the next stage is to make the preparations for the all-important consultation and risk analysis stages. These stages are at the core of any DPIA and are what distinguishes it from a straightforward legal compliance check.

Assessment

Answer question 3.17 by clicking '**Yes'** if you have answered any screening questions with yes, otherwise click '**No'**. If you have clicked '**Yes'**, you will be taken to Stage 4. If you have clicked '**No'**, you will be able to submit the DPIA for approval.

Stage 4: Risk Identification

Risk Identification

In the '**Risk identification'** section, you find a list of possible risks. If the risk does not apply to your activity, click '**No'**.

If the risk applies, click on '**Yes'**. Then answer the following three questions, what '**Mitigation'** measures you can implement, '**Likelihood'** of the risk manifesting after mitigation and '**Impact'** on data subjects and the University if the risk manifests even after mitigation.

One of the first actions to complete now is to work with the activity stakeholders you have identified in stage 1. Section 4 provides you with a list of possible risks – decide which ones apply to your activity. This identification of risks should be treated very much as a work in progress – if at a later stage, a risk that you discarded does manifest, you can reopen the DPIA and amend it.

Once you have identified a risk, the next question asks for any mitigation measures you can take to either reduce or completely eliminate the risk.

There are two types of solutions to privacy risks – avoidance measures and mitigation measures:

An avoidance measure is a means of dissipating a risk. It refers to the exclusion of technologies, processes, data or decision criteria, in order to avoid particular privacy issues arising. Examples are:

- Minimisation of personal data collection.
- Non-collection of contentious data items.
- Active measures to preclude the use of particular data items in the making of particular decisions.
- Active measures to preclude the disclosure of particular data items.

A mitigation measure is a feature that compensates for privacy intrusive aspects of a design. A mitigation measure may compensate partially or wholly for a negative impact. Examples are:

- Minimisation of personal data retention by not recording it, or by destroying it as soon as the transaction for which it is needed is completed.
- Destruction schedules for personal information which are audited and enforced.
- Limits on the use of information for a very specific purpose, which strong legal, organisational and technical safeguards preventing its application to any other purpose design, implementation and resourcing of a responsive complaints-handling system, backed by serious sanctions and enforcement powers.

Under some circumstances it may be appropriate to recognise and accept the privacy risk without mitigation where the likelihood of it being realised or the impact would be low.

However, this must be carefully considered, and must not be done simply as an alternative to taking action.

In the ‘Likelihood’ and ‘Impact’ questions, assess whether the residual risk after the mitigation measures have been implemented is likely to manifest and what impact it would have on the data subjects and the University.

A new possible risk has been added which will be approved by the respective Head of College or Director of Support Area. In July 2020 the European Court of Justice issued a decision that invalidated the Privacy Shield which had worked as a safeguard for transferring personal data to the United States of America. The reason for this was that that the Privacy Shield cannot appropriately safeguard personal data if a government agency (e.g. Police, CIA, NSA in the US relying on the Patriot Act), wishes to access the data. Essentially any transfer using the Privacy Shield is now unlawful, which means that all international data transfers outwith the EEA require appropriate contracts using the Standard Contractual Clauses (SCCs). There are, however, situations where SCCs are not possible, or where the supplier will refuse to sign them. In these situations, it is even more important for you to argue why the data are unlikely to be of any interest to government agencies in the recipient country. The new question 4.44 – 4.46 asks for a risk assessment of transferring personal data outwith the EEA using the SSCs.

Once you have answered all questions listing possible risks, conduct a ‘brainstorming’ consultation with the stakeholders to identify any other potential risks to the data subjects and record them in the final questions. Conduct the same assessment – mitigation measures, likelihood of residual risk manifesting and impact on data subjects and University as you have done for the listed risks.

Additional risks

If you have identified risks that are not listed in the question, add them in the questions following the list of possible risks

Now consider all the risks that you have identified: If there are multiple high risks that are not hacking-related, you will need to continue to Section 5 and conduct a data subject consultation. Should it become obvious at this stage that the risks are likely to be only low to medium, a data subject consultation will not be required.

Assessment

Answer the final question in this section by clicking ‘**Yes’** if you have identified multiple high risks, otherwise click ‘**No’**. If you have clicked ‘**Yes’**, you will be taken to Stage 5. If you have clicked ‘**No’**, you will be able to submit the DPIA for approval.

Stage 5: Data Subject consultation

Identify and list all data subjects, e.g. the people affected by the project, for example, these could be:

- students,
- staff,
- research participants,

- library subscribers,
- …

IMPORTANT: You will save time by involving the right *project* stakeholders in your meetings with the data subjects. For example, what a data subject might think is a good solution might not be so if your IT people tell you it is not technically feasible. Remember, your aim all the way through is to find ways to enhance privacy.

Ensure that the time and effort spent consulting each group of people is proportionate to the seriousness of the risks they are helping you address - as with the management of all risks proportionality should be the watchword.

From the work you have completed so far, you should have an initial view of the privacy risks which you can use to guide you in drawing up a consultation plan.

Next, you will need to decide who shall conduct the consultation. Then decide whether you can carry out the consultation with representatives of, or advocates for, some data subject groups and agree what the perspective, or interests, of all the people are. Then make a decision how best to consult with them:

- face to face meetings,
- phone calls,
- correspondence,
- focus groups,
- workshops,
- online consultation.

Keep in mind that an effective consultation depends on all data subjects being sufficiently well-informed about the project, having the opportunity to convey their perspectives and their concerns, and developing confidence that their perspectives are being reflected in the design.
Describe the project to the data subjects, explain the data flows and the benefits to them. Then hand the discussion over to them and ask them for their view:

- Where do they see privacy risks?
- Where do they see possibilities for improvement?
- Do they have any suggestions for improvement?

Some useful ways of ensuring effective consultation include:

- priming of discussions by providing some initial information about the project such as a powerpoint presentation;
- facilitated interactions among the participants;
- making sure that there is sufficient diversity among those groups or individuals being consulted, to ensure that all relevant perspectives are represented, and all relevant information is gathered;
- making sure that each group has the opportunity to provide information and comment, even including multiple rounds of consultation where necessary;
- making sure that the method of consultation suits the consultation group, for example using workshops or focus groups as an alternative to, or even as well as, formal written consultation;

- making sure that the information provided by all parties to the consultation is fed into the subsequent rounds of design and implementation activities; and
- ensuring that the perspectives, concerns and issues raised during the consultation process are seen to be reflected in the outcomes of the DPIA process.

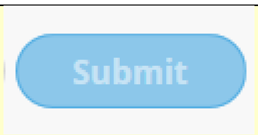
Stage 6: Scheduling a review

As you close the DPIA you should consider when it will be reviewed and how the review will be carried out.

The purpose of a review is to ensure that the measures introduced as part of the DPIA are working effectively. It is expected that such a review, particularly in the case of major DPIAs, will be carried out as part of the wider review into the effectiveness of the project or programme deliverables. For smaller DPIAs, the review may be carried out as a standalone process. Either way, upon completion of the DPIA you should record how this review will be carried out, by whom, and when.

Stage 7: Submission

Once you have finished inputting all answers and information, the DPIA will be ready for approval by the DPO. You can ‘Save and Exit’ the DPIA if you wish to revisit any sections before submitting – only submit when you feel that you have answered all questions to the best of your knowledge.

Submitting your DPIA Click the ‘Submit’ button at the bottom right corner of the screen. Confirm that you indeed have finished your DPIA and wish to submit it.	

The DPO will be notified and will assess the DPIA. If the DPO has any further questions, these will be entered into the system and you will receive an email informing you that you need to provide more details.

Stage 8: Readiness for service

Once the project has been formally approved by the relevant budget holder, you should be ready to implement the agreed solution. This stage may involve procurement of an IT system and the subsequent detailed design and build stages. It is important to ensure throughout these stages that the mitigating and/or avoiding measures that were worked up during the DPIA are carried through into implementation.

It is important that you ensure that any necessary updates regarding new personal data processing activities or systems are made to the relevant privacy notice. Contact the local Data Protection Champion to request changes to a privacy notice.

List of Data Champions

Finally, before going live, you should double-check that these measures are working in the way intended, and that the final system or process does still comply with privacy laws. If not, you may need to go back a stage to see whether the approved solution has been implemented correctly.

Although the privacy law compliance process will have to be initiated and performed as far as possible at this stage, it cannot be finalised until late in the project life-cycle when the design is complete. This is why you will need to revisit the compliance section immediately before implementation.

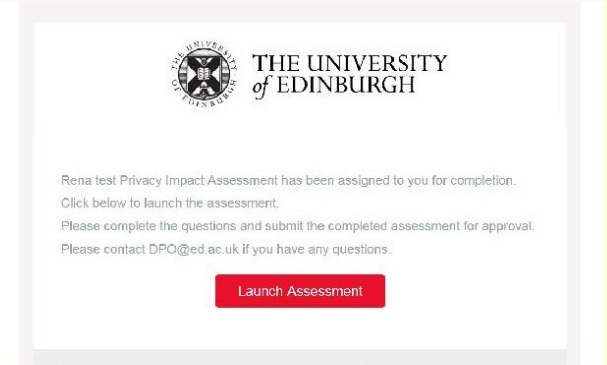
Ad hoc reviews

Additionally, whenever you realise that there are changes to the activity that may affect the risks, you will need to amend the DPIA.

To open a completed DPIA for your review or amendment, email the DPO and ask for the DPIA to be opened. You will receive the same email as when you started the DPIA.

Re-starting the Assessment

Click the red **'Launch Assessment' button** on the link you have been emailed to launch the DPIA tool. You will be taken to the start page of your assessment.



Rena test Privacy Impact Assessment has been assigned to you for completion.

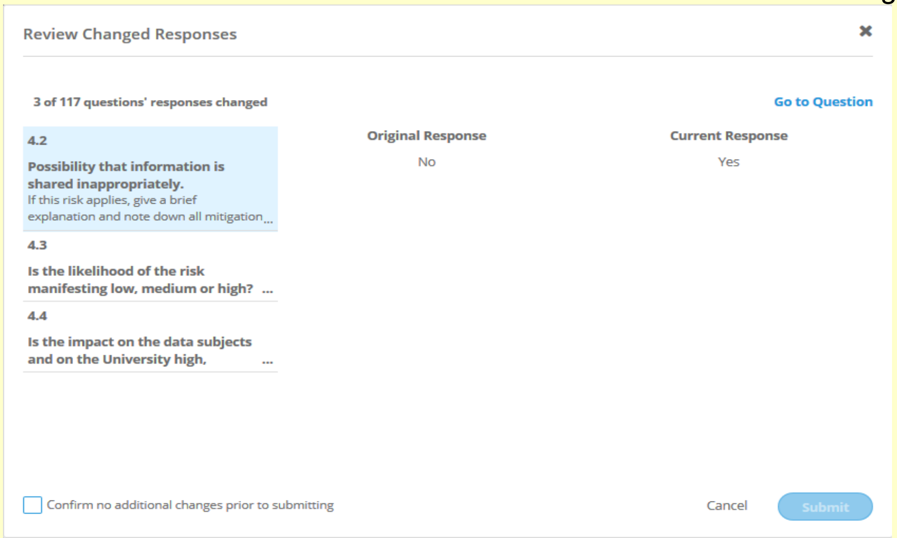
Click below to launch the assessment.

Please complete the questions and submit the completed assessment for approval.

Please contact DPO@ed.ac.uk if you have any questions.

Make the changes you need and re-submit the DPIA.

You will then see a window that displays the changes and asks for confirmation by ticking the box in the left bottom corner. Then click the blue '**Submit'** button in the bottom right corner.



Review Changed Responses

3 of 117 questions' responses changed

	Original Response	Current Response
4.2 Possibility that information is shared inappropriately. If this risk applies, give a brief explanation and note down all mitigation...	No	Yes
4.3 Is the likelihood of the risk manifesting low, medium or high? ...		
4.4 Is the impact on the data subjects and on the University high, ...		

□ Confirm no additional changes prior to submitting

If you require the guidance in an alternative format, please contact the Data Protection Officer: DPO@ed.ac.uk or 0131 651 4114