How to conduct a Data Protection Impact Assessment (DPIA)

This guidance is for all University researchers carrying out a project involving personal data. 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 category 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 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;
- use existing data for a new purpose

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.
- Legal action taken by individuals to sue the University.

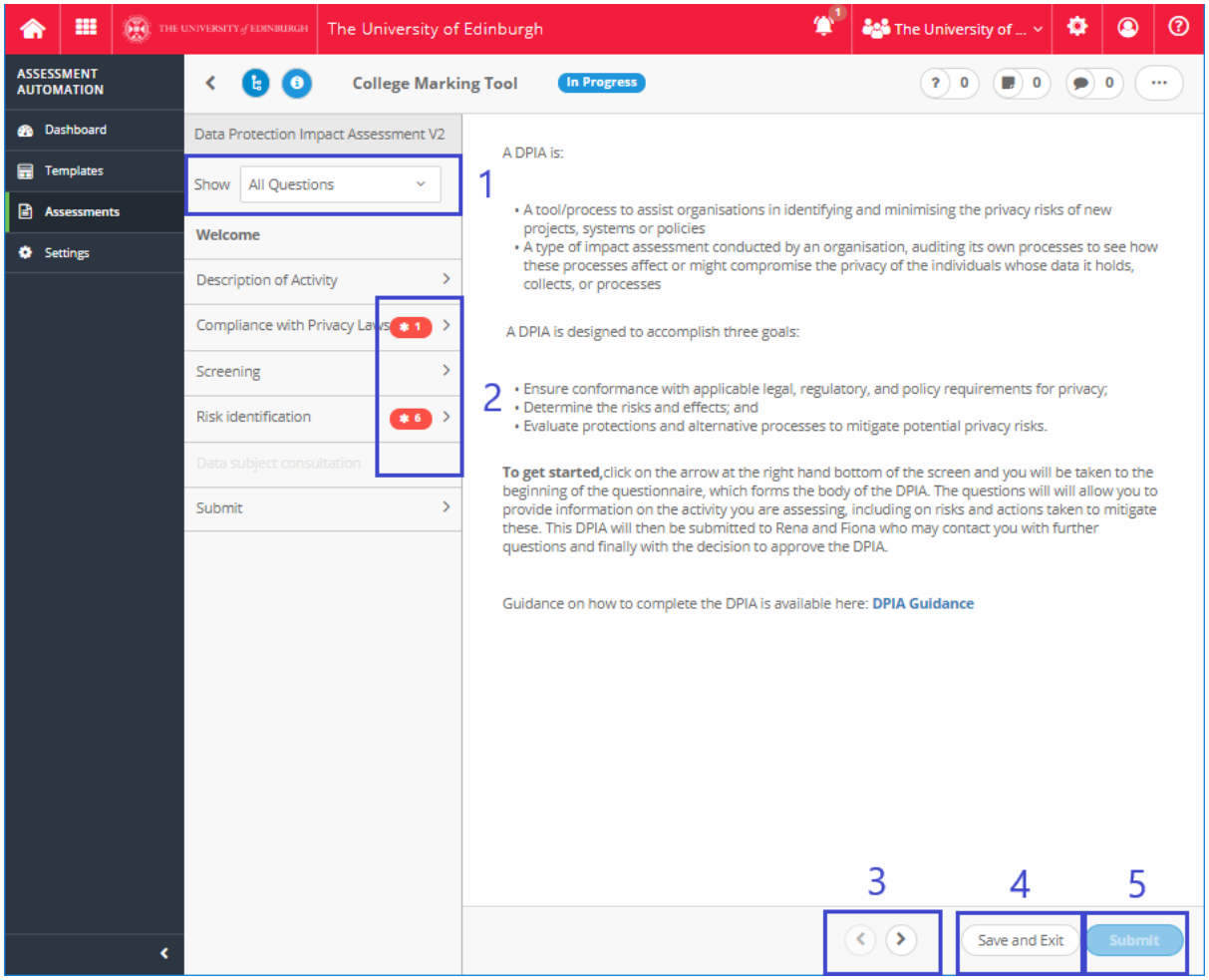
4. How to carry out a DPIA

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;

- Overview of research project
- Compliance with Privacy Laws
- Screening
- Risk Identification

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



1

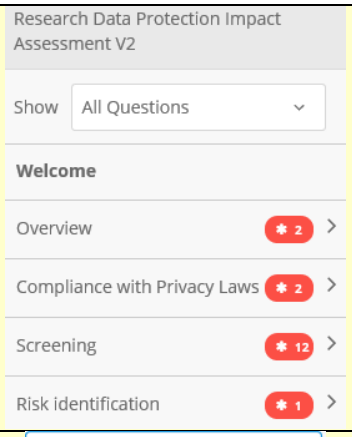
Selecting a section to complete

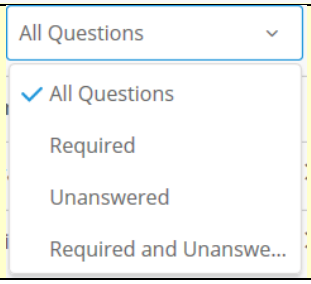
To select a specific section, click on one of the appropriate section descriptions within the column titled ‘Data Protection Impact assessment’.

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





2

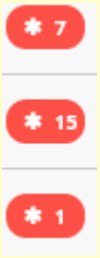
Mandatory Questions

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.

Progress of DPIA

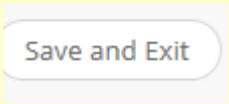
The number displayed within the orange box indicates the number of mandatory questions still to be answered in each section. This number may change based on the answers given, and more questions may then become available.



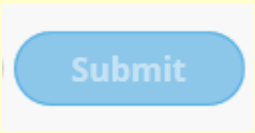
3

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	

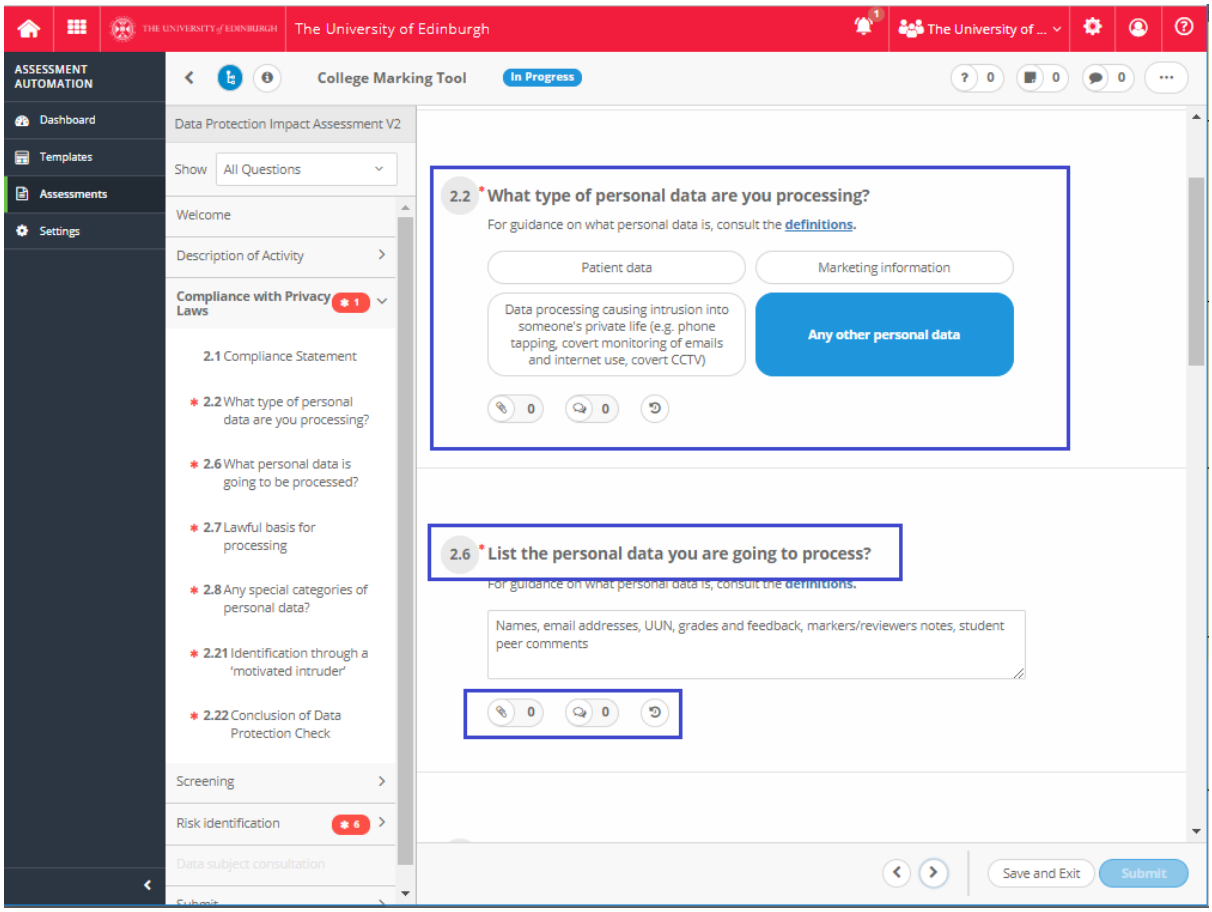
4

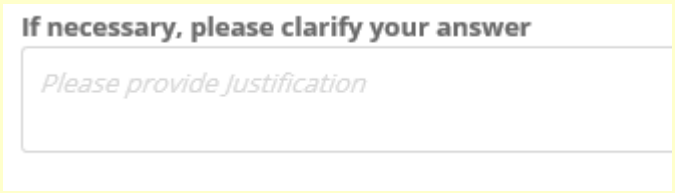
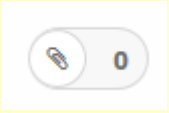
To exit You can, at any time, click on '**Save and Exit'**. When you want to continue work on the DPIA, just click on the link in the email again.	

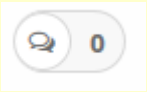
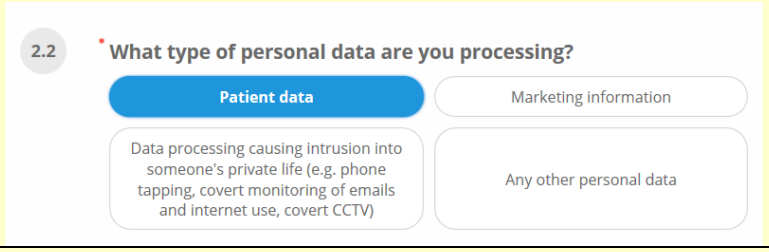
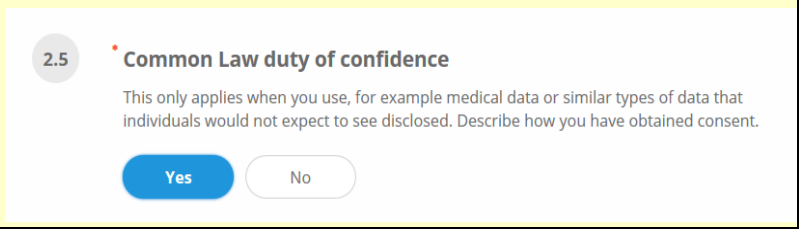
5

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.	

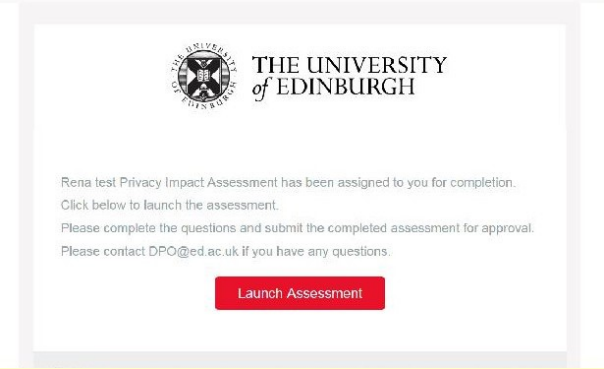
The following offers a guide to the questions and to the comments functions:



Textboxes - 'If necessary clarify your answer' These textboxes are not mandatory – if no clarification is required, then leave the textbox empty.	
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 resultant answer will dictate the following questions to be answered	 

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

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, which also includes a link to this guidance.	

Stage 1: Description of research project

Describing the project

In the left panel, click on '**Overview'**. Complete all fields as they are all mandatory.

Begin by outlining your research project. You can also upload documents describing your research and referring to the attachments.

Next, make a preliminary assessment for data usage by mapping data flows:

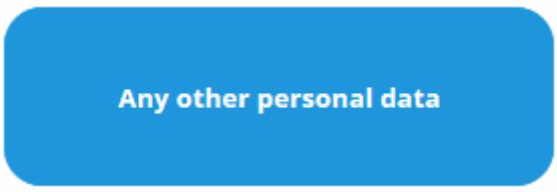
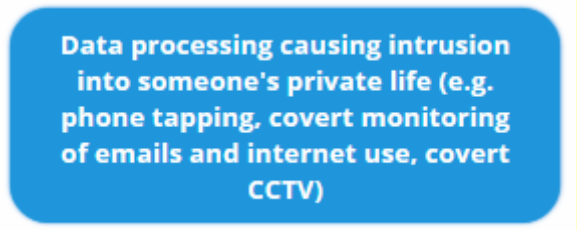
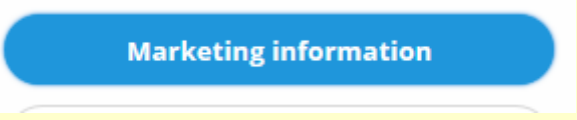
- How is the information collected, stored, used and deleted?
- What information is used?
- What it is used for?
- Who will have access to it?

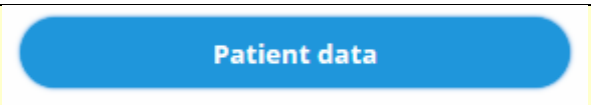
The mapping can be done in the form of a flow chart, an information register, or a research brief.

Stage 2: Compliance with Privacy Laws

Every research project using personal data must be compliant with privacy laws.

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.	
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.	
If you use personal data for marketing, you will be directed to question 2.4 and asked about PECR compliance.	

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.	

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 2.15, you will be asked whether you are sending personal data outside the EEA. If you click 'no', you will be directed to question 2.19.

If you click 'yes', you will be directed to question 2.16, 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 2.19.

If you click 'none of the above', you will be directed to question 2.17, where you will be asked which countries you send the data to. Then, in question 2.18, 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?

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.

The screening questions are there to guide you towards the more in-depth and all-important risk analysis stage. This stage is at the core of any DPIA and is what distinguishes it from a straightforward legal compliance check.

Question 3.13 then asks you to consider how best to approach the risk assessment stage and who to consult. This could be other members of your research team, a representative of the sponsor, members of the Research Support Office, external collaborators, a supervisor or principal investigator. These people are called 'stakeholders'.

Stage 4: Risk identification and mitigation

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 is to work with the stakeholders you have identified at the end of stage 3. You now need to consider in more detail what the interest of these various stakeholders are and the level of involvement they will have in the DPIA. You need to conduct an initial consultation, a brainstorming session, to identify any potential risks to the data subjects and record these risks in the table below according to the categories:

- Risks to individuals: risks affecting people directly, e.g. new surveillance methods, disclosure of sensitive personal data.
- Corporate risks: sanctions, fines, loss of reputation.
- Compliance risks: non-compliance with specific legislation.

From this, you should start to form a clear picture about how significant the risks are, and whether there are previously unseen risks.

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

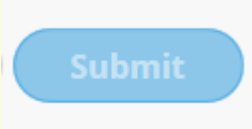
Stage 5: Review

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 6: 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.

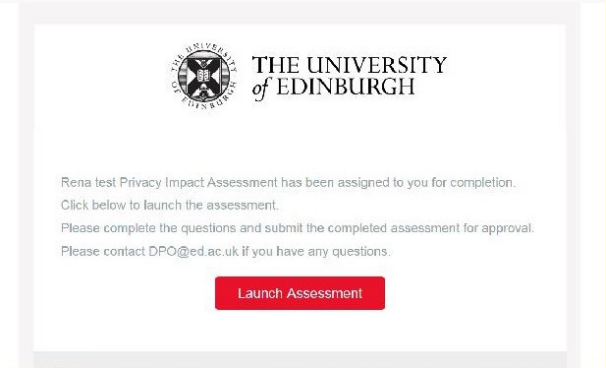
Submitting your DPIA Click the 'Submit' button at the bottom right corner of the screen. Confirm that you indeed have finished your DPIA and wish to submit it.	

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.

Ad hoc reviews

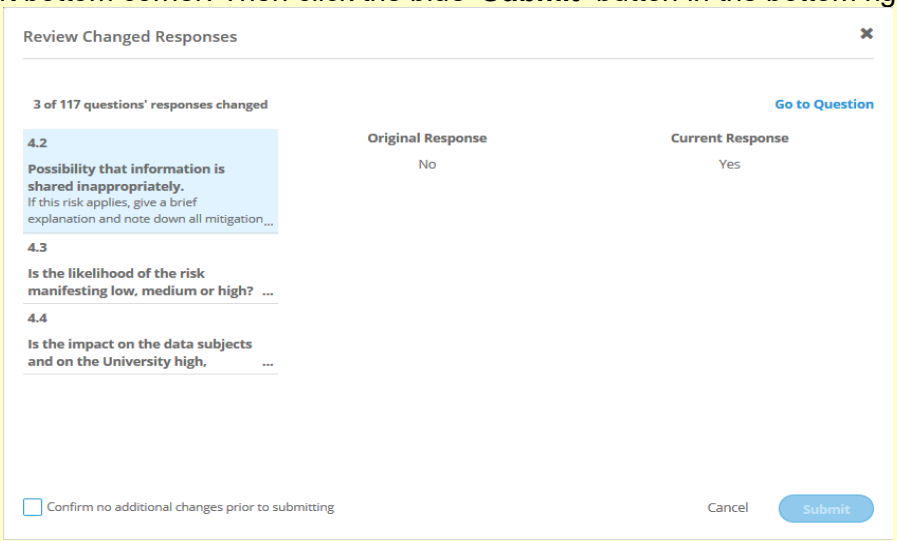
Additionally, whenever you realise that there are changes to the activity that may affect the risks, you will need to amend the DPIA.

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.	

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.



About this guidance

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