EDINBURGH BUSINESS SCHOOL
HERIOT-WATT UNIVERSITY

HERIOT WATT UNIVERSITY

PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA) TOOLKIT

INTRODUCTION

This methodology takes a proportionate and consistent approach to managing privacy and information security risks. This toolkit is to be used for all projects and initiatives involving collection or use of personal data and other confidential information. It has been designed to enable the University Group to meet two of its obligations under the EU General Data Protection Regulation:

1. To implement appropriate technical and organisational measures to apply the data protection principles and integrate these safeguards into processing activities so that we embed privacy by design and default into all of our management of personal data.
2. To carry out a Data Protection Impact Assessment, (DPIA) following the 5 steps in this toolkit for all processing that is likely to result in a high risk to the privacy of individual data subjects (e.g. students or staff). This DPIA process will help users to identify and minimise privacy risks presented by the development of new or modified procedures and services.

What are the objectives of this methodology?

By following this process we will:

- Ensure compliance with applicable legal, regulatory, and policy requirements for privacy.
- Determine the risks, including to individuals, in terms of damage and distress caused when personal data is mishandled, and organisational risks, such as financial and reputational damage resulting from data breaches.
- Evaluate protections and alternative processes to mitigate potential privacy risks.
- Identify actions to be taken to reduce privacy and information security risks.
- Embed privacy by design and other appropriate information security measures into the specification, design and build of systems and procedures.

The outcome of a properly conducted data protection and information risk assessment should be reduction in privacy, security and reputation risk, improved compliance with data protection legislation, improved systems and greater trust among data subjects, funders, sponsors and other stakeholders.

The University Group can rely on a DPIA to provide evidence in demonstrating compliance in two key areas:

- Were all material risks identified? An organisation can only comply with data protection requirements if it has identified and addressed the risks that arise in connection with its processing activities.
- What appropriate steps were taken to address those risks? The DPIA provides a record of the steps that were taken to resolve or mitigate any danger to the rights and freedoms of data subjects.

When does this toolkit need to be used?

This is to be applied to all new procedures and service changes involving the processing of personal data. The toolkit should be considered to be a living document that is **created at the first stage** of any project or initiative involving collecting or using personal data or confidential information **and updated and referred to at all subsequent stages**. This will enable privacy and information security risks to be considered at the early stages where there is greatest opportunity to address risks and to influence project design and implementation. DPIAs will always be required in the case of:

- Using data for new purposes.
- Developing marketing strategies that have privacy implications.
- Building new IT systems for storing or accessing personal data.
- Embarking on a data sharing initiative.
- A project using new technologies.
- Processing that is likely to result in a high risk to the freedoms of individuals.

Who completes the toolkit and conducts the DPIA?

The person responsible for the project will be responsible for completing the toolkit and, where necessary, the DPIA. The Data Protection Officer or the Edinburgh Business School Compliance Manager, as appropriate, can provide advice and guidance to the person completing the toolkit, review the completed toolkit, endorse the recommended actions and gain assurance that these have been completed. We can also provide this document in Word format.

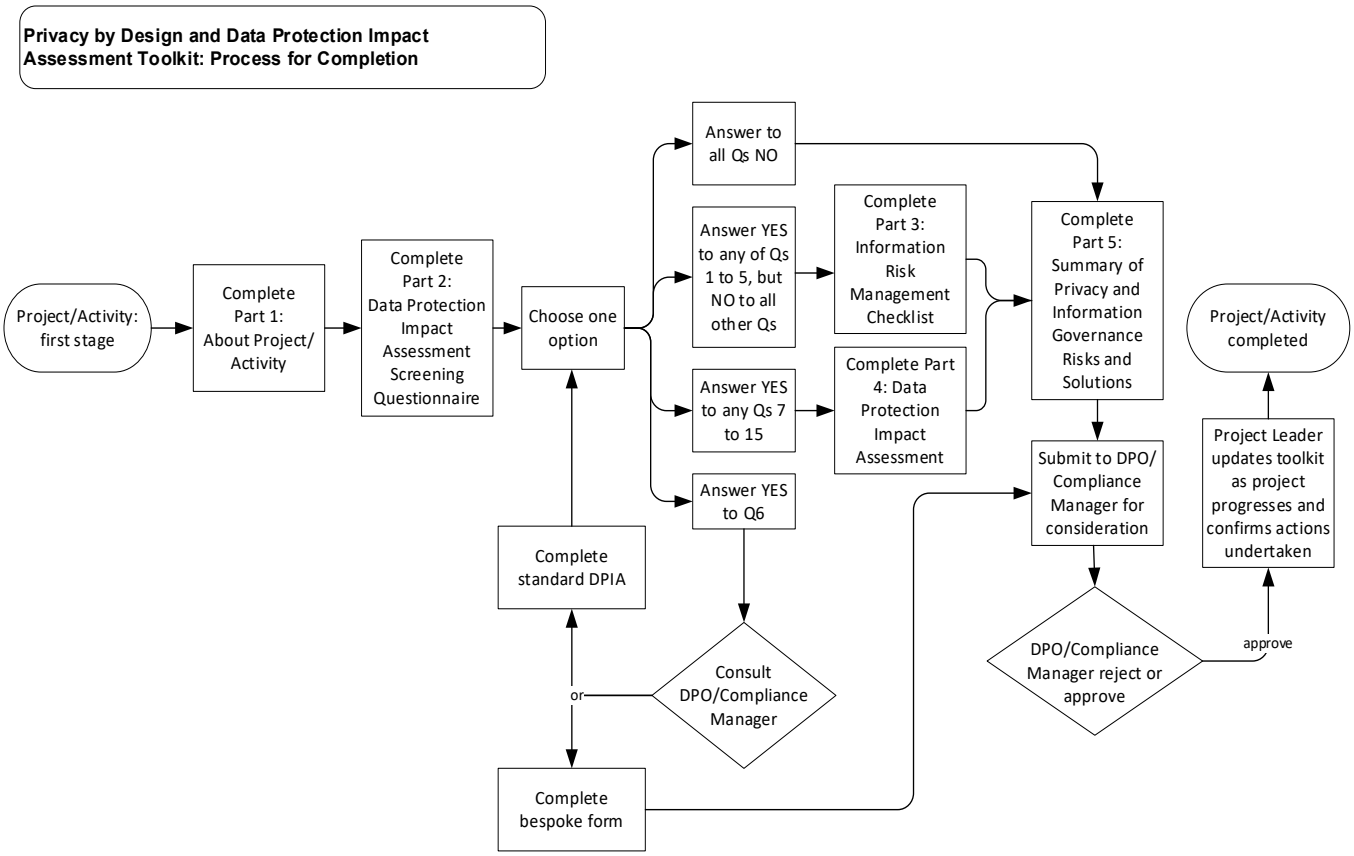
The Data Protection Officer will maintain a register of Assessments undertaken, with the relevant project documentation.

What needs to be completed to undertake a DPIA?

The following parts of the DPIA should be completed:

Part 1	About the Project/Activity: this includes information on the project/activity, implementation data, purpose of the project/activity, its aims and benefits.
Part 2	DPIA Screening Questionnaire: this should be completed to determine whether Part 3 or 4 need to be completed. • If the answer to all the questions is NO, the full DPIA is not required and Parts 3 and 4 need not be completed. • If you answer YES to any of the questions 1-5 but 'No' to all of the other questions, please complete the Information Risk Management checklist in Part 3. Part 4 need not be completed. • If you answer YES to any of the questions 7-15 a DPIA is required. Please complete • Part 4 – DPIA. Part 3 need not be completed. • If you answer YES to Question 6, please contact the DPO/Compliance Manager. **Contact the DPO/Compliance Manager after completing Part 1 and Part 2.**
Part 3	Information Risk Management checklist
Part 4	DPIA

Part 5	Summary of Privacy and Information Governance Risks and Solutions
Annexes	The following Annexes provide information to assist in the completion of the DPIA: • Annex 1: Legal basis for processing personal data under GDPR • Annex 2: Risk assessment matrix • Annex 3: Examples of privacy related risks



In this toolkit, all references to:

- University include all members of the University Group
- Project includes other activities and initiatives that present privacy or information security risks.

MORE HELP AND ADVICE

We're here to help. I f you have a question about any aspect of this methodology please contact

Data Protection Officer, Heriot-Watt University, Edinburgh EH14 4AS, UK Phone:+ 44 (0)131 451 3218/3219/3274 Email: HIG@hw.ac.uk https://www.hw.ac.uk/about/policies/data-protection.htm	Compliance Manager, Edinburgh Business School, Heriot-Watt University, Edinburgh, EH14 4AS, UK Phone +44 (0)131 451 4764 Email: stewart.Smith@ebs.hw.ac.uk https://www.ebsglobal.net/

PART 1
ABOUT THE PROJECT/ACTIVITY

Proposed Project/Activity	
Purpose of Proposed Project/Activity	
Describe the Aims and Benefits of the Project/Activity Explain what the project/activity aims to achieve, and what the benefits will be to the organisation, to individuals, and to other parties	
Proposed Implementation Date	
Completed By	
Name	
School/Directorate	
Role	
Phone	
Email	
Name of Project Leader (if different from person above)	
Name of Person Responsible for this Processing Activity After Project Ends (if different from person above)	
Date of Initial Completion of DPIA Toolkit	
Version Control (this toolkit should be updated at each stage of the project)	

PART 2
DATA PROTECTION IMPACT ASSESSMENT (DPIA)
SCREENING QUESTIONNAIRE

Q1	Will the project involve the processing of personal information?	Y		N	
Personal information is information about people who can be identified from that information or in combination with other information. If YES please give details (i.e. whose and what categories of personal data (e.g. students, dates of birth, programme etc.)). Processing includes storing data as well as collecting, accessing, updating, sharing, destroying etc. If not sure please give details of your query here.					

Q2	Will the project involve processing confidential information that is not personal data? Examples include, but are not confined to:	Y		N	
Unpublished research data that has been received or created under conditions of confidentiality or would if lost or disclosed significantly impact on the success of a research project, research income. REF outputs or knowledge transfer *Information received in confidence .e.g. legal advice from solicitors, trade secrets and other proprietary information received from contractors, suppliers and partners e.g. under a non-disclosure agreement* *Information that would substantially prejudice the University or another party's intellectual property rights, commercial interests or competitive edge if it were disclosed* *Information relating to high profile/high impact strategy or policy development before the outcomes have been decided and announced* *Information that would compromise public safety or the security of buildings, equipment or assets if disclosed* If YES please give details. If not sure please give details of your query here.					

Q3	Will the project involve the use of an external contractor or supplier (i.e. not a member of the Heriot-Watt University Group) to process personal data or other confidential information? This includes hosting or maintaining IT systems and applications.	Y		N	
If YES and you have already identified a potential supplier or suppliers please give details and confirmation that the following safeguard is in place: The organisation processing the data has agreed to sign the University data processor or data controller/data controller data sharing agreement or one that has been endorsed by the DPO/Compliance Manager as having equivalent assurance for the rights of data subjects. If not sure please give details of your query here.					

Q4	Will the project involve transfers of personal data outside of the UK, to organisations that are not members of the Heriot-Watt University Group?	Y		N	
If YES please indicate which country and seek advice from the DPO/Compliance Manager.					

Q5	Will the project involve processing special categories of personal data?	Y		N	
Special categories of data means personal data about one of the following: racial or ethnic origin; political opinions; religious of philosophical beliefs; trade union membership; physical or mental health; sex life or sexual orientation; proven or alleged offences. If YES please give details. If not sure please give details of your query here.					

Q6	Does this activity fall into one of the following categories?	Y		N	

- Approved Learning Partner (ALP)
- Exam Centres
- External examiners and supervisors
- Approved teachers, tutors and markers
- Recruitment agents
- Independent counselling services
- Undergraduate or PGT research involving interviews or surveys
- Direct marketing

If YES, please contact the DPO/Compliance Manager to ask if a generic DPIA or risk management checklist is available as appropriate for the relevant activity and apply the mandated actions. If you think that any other standard processing activity could usefully be added to this list, please contact the DPO/Compliance Manager.

Q7	Will the project involve processing other high risk personal data	Y		N	

High risk personal data includes the following:

- *Information that could be used to commit identity fraud such as payment card, personal bank account and other financial information and national identifiers, such as national insurance numbers and copies of passports and visas*
- *Personal information relating to vulnerable adults and children*
- *Detailed profiles of individuals; including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed*
- *Spread sheets of marks or grades obtained by students, information about individual cases of student discipline*
- *Sensitive negotiations which could adversely affect individuals*

• *Security information that would compromise the safety of individuals if disclosed* • *Any other personal information that would cause damage or distress to individuals if disclosed without their consent*
If YES please give details. If not sure please give details of your query here.

Q8	Will the project involve the collection of any new categories of personal information about individuals that we don't already collect about them?	Y		N	
If YES please give details. If not sure please give details of your query here.					

Q9	Will the project compel individuals to provide personal information about themselves (e.g. to receive a service or if participation is not voluntary)?	Y		N	
If YES please give details. If not sure please give details of your query here.					

Q10	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Y		N	
If YES please give details. If not sure please give details of your query here.					

Q11	Are you using information about individuals for a purpose it is not currently used for, or in a way not currently used?	Y		N	
If YES please give details. If not sure please give details of your query here.					

Q12	Does the project involve you using technology which might be perceived as being privacy intrusive (e.g. the use of biometrics or facial recognition)?	Y		N	
If YES please give details. If not sure please give details of your query here.					

Q13	Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them (e.g. a decision on a student that could affect the outcome of their studies)?	Y		N	
If YES please give details. If not sure please give details of your query here.					

Q14	Will the project require you to contact individuals in ways that they may find intrusive (e.g. contacting a student where there are concerns about their wellbeing)?	Y		N	
If YES please give details. If not sure please give details of your query here.					

Q15	Does the project involve a *high risk* to individuals which would make a DPIA mandatory under GDPR?	Y		N	

Please tick YES if any of the following may apply (these examples are taken from ICO guide to DPIAs):

- Using systematic and extensive profiling or monitoring with significant effects and/or on a large scale;
- Processing special category or criminal offence data on a large scale;
- Systematically monitoring publicly accessible places on a large scale;
- Contacting individuals in ways they may find intrusive;
- Using new of innovative technologies or technology that might be perceived as privacy intrusive;
- Using profiling or special category data to decide on access to services;
- Processing biometric data;
- Processing genetic data;
- Matching data or combine datasets from different sources;
- Collecting personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- Participation in a project is mandatory and participants are compelled to provide personal information about themselves;
- Tracking individuals' location or behaviour;
- Profiling children or targeting marketing or online services at them; or
- Processing data that might endanger the individual's physical health or safety in the event of a security breach;
- Processing that is large scale;
- Processing that decides on access to services or opportunities;
- Processing that involves sensitive data;
- Processing may cause discomfort or distress to individuals;
- Processing that involves vulnerable individuals;
- Processing will result in others making decisions or taking action against individuals in ways which can have a significant impact on them.

If YES, explain why you have reached that conclusion.

Conclusion

1	Are there any other relevant factors to consider in addition to the screening questions?	Yes		No	
If YES, provide further information.					

2	Does this project require a DPIA?	Yes		No	

If you answered YES for any of the Questions 1 to 5 only, it will not be necessary to conduct a DPIA. Instead, you will need to complete the Information Risk Management Checklist in Part 3.
If you answered YES to Question 6, ask the DPO/Compliance Manager for the generic completed DPIA and apply the relevant actions.
If you answered YES for any of the Questions from 7 to 15, a DPIA will be needed. Please complete Part 3

Please note that you should not proceed to the completion of Part 3 or Part 4 until Part 1 and Part 2 have been reviewed by the DPO/Compliance Manager.

Name	
☐	I confirm that the information I have provided is to the best of my knowledge correct.
Date	

Please send this completed screening questionnaire to the DPO/Compliance Manager, as appropriate, at the email address on Page 3.

Reviewed by Data Protection Officer					
Name					
Date					
I agree with the screening assessment		Yes		No	
Give reasons for decision					
At this stage to DPO/Compliance Manager will advise on any DPIAs already completed for similar activities and provide these as a point of reference					

PART 3
INFORMATION RISK MANAGEMENT CHECKLIST

Please note: only Part 3 or Part 4 should be completed, not both.

Step 1: Confirm the legal basis for processing any personal data necessary for the project In order to process personal data lawfully, you need to meet: a) at least one of the conditions in Annex 1 *and* b) in the case of special categories of personal data, at least one of the conditions in Annex 2	
Personal data	
Special categories of personal data (if applicable)	

Step 2: Describe the information flows and security controls
Describe the following *A flow diagram may also be included to explain the data flows.*
Why will the information be collected/used?
What information will be processed? This means types of data (e.g. name, date of birth, telephone number), specifying any special categories of personal data (see Annex 2 for examples), and any other high risk personal data including financial or location data.
What number of individuals will have their data processed (approximately)?
How will the information be obtained (e.g. provided by individual, collected in behalf of the Heriot-Watt Group)?
If the data is to be processed by a contractor, partner or other third party on behalf of the University please provide copies of the following: • Signed HWU data processor/data sharing agreement or one conforming to equivalent GDPR standards; • Details of relevant security certifications held by the contract (e.g. PCI-DSS, ISO 27001 or BS 10012:2017 if applicable); • Contactor's information security and privacy policies.
Describe how the information will be collected (e.g. electronically, on paper or both)?

Describe the security controls to be applied to the process of collection (e.g. secure document upload, secure portal).
How will information be secured in transit?
How will the information be stored (e.g. IT system used, database, filing cabinet)? In the answer include a description of the security controls to be applied to control access on a business need to see basis.
How will the information be destroyed (e.g. secure erasure, cross cut shredder, confidential waste disposal)?
Who will need to have access to the information (e.g. list individuals and staff groups)? In the answer include a description of the security controls to be applied to control access on a business need to see basis.
With whom will the data be shared (e.g. individuals, third parties)? In the answer include a description the security controls to be applied to control access on a business need to see basis.
Will any information be sent outside the Heriot-Watt Group and its computer networks? If YES please give details of security controls in place.
What records retention policy will be applied to the data and who is accountable for implementing the policy (e.g. student, HRD)? (Information on retention schedules is available here: https://www.hw.ac.uk/services/heritage-information-governance/manage/what-to-keep.htm).

Step 3. Explain how you will comply with the rights of data subjects
The Right to be Informed: a data subject has the right to be given information about how their data is being processed and why.
How will you inform data subjects what you are doing with their data when you obtain it from them (e.g. using a privacy notice)?
How will you inform data subjects what you are doing with their data when you obtain it from someone else (e.g. from a public website)?

The Right to Access: a data controller must provide a data subject with confirmation as to whether or not personal data concerning him/her are being processed, and where this is the case, access to the data free of charge within one month of the request.					
How will you identify and retrieve all information in a system that relates to a data subject?					
Can you provide self-service access for data subjects to obtain their records?	Y		N		
If YES, explain how?					
The Right to Rectification: a data controller is entitled to have their personal data rectified if inaccurate or incomplete					
If a data subject asks for inaccurate data about them to be corrected, how would you achieve this?					
The Right to Erasure: applies where it is no longer necessary to process the personal data or the data subject withdraws their consent where no overriding lawful grounds apply.					
If a data subject asks for their data to be erased, how would you achieve this?					
If a data subject asks you to restrict further processing of their data (e.g. until a complaint or request to correct inaccurate data has been resolved, or to prevent scheduled deletion until they have obtained a copy of the data) how will you comply with this?					
The Right to Data Portability: applies only where processing is based on consent or contract and allows a data subject to obtain and reuse their personal data across different services for their own purposes.					
How can a data subject be provided with a machine readable copy of the personal data he or she has provided (e.g. CSV file or other format that can be exported from one system to another)?					
Consent: applies only where processing is based on consent.					
If a data subject withdraws their consent for their data to be processed for specific purposes, what would you have to do to comply with this?					
The Right to Object: applies to all processing for marketing purposes. Also processing based on public interests/legitimate interests where no overriding public interest applies.					
If a data subject asks you to stop processing their data what would you have to do to comply with this?					
Automated Individual Decision-making, Including Profiling: a data subject has the right to obtain human intervention, express his or her point of view and to contest the decision.					
Does the system make automated decisions about data subjects that may have a significant impact on them?	Y		N		
Is YES, please give details.					

If YES, explain how you will you comply with a data subject's right to obtain human intervention, express his or her point of view and to contest the decision?

Step 4. International Transfers
Depending upon the advice received for Part 2, Question 4, and the advice you received from the Data Protection Officer/Compliance Manager, you will need to confirm the safeguard that you have in place for any international transfers of personal data. Examples of safeguards include: • The European Commission (EU) has designated the country as providing an adequate level of protection for privacy; • The organisation processing the data will sign an agreement with the University including the EU standard contractual clauses for international data transfers; • The organisation processing the data will sign the University data processor or data controller/data controller data sharing agreement and provide evidence of its certification under the EU –US Privacy Shield

PART 4
DATA PROTECTION IMPACT ASSESSMENT (DPIA)

This assessment should only be completed after the DPIA Screening Questionnaire has been completed, and the need for a DPIA has been identified.

Please note: only Part 3 or Part 4 should be completed, not both.

Referring to the Annexes before you complete the DPIA will assist you in responding to the questions below.

Step 1: Describe the information flows
Describe the following *A flow diagram may also be included to explain the data flows.*
Why will the information be collected/used?
What information will be processed? This means types of data (e.g. name, date of birth, telephone number), specifying any special categories of personal data (see Annex 2 for examples), and any other high risk personal data including financial or location data.
What number of individuals will have their data processed (approximately)?
How will the information be obtained (e.g. provided by individual, collected in behalf ok the Heriot-Watt Group)?
If the data is to be processed by a contractor, partner or other third party on behalf of the University please provide copies of the following: • Signed HWU data processor/data sharing agreement or one conforming to equivalent GDPR standards; • Details of relevant security certifications held by the contract (e.g. PCI-DSS, ISO 27001 or BS 10012:2017 if applicable); • Contactor's information security and privacy policies.
Describe how the information will be collected (e.g. electronically, on paper or both)?
Describe the security controls to be applied to the process of collection (e.g. secure document upload, secure portal).

How will information be secured in transit?
How will the information be stored (e.g. IT system used, database, filing cabinet)? In the answer include a description of the security controls to be applied to control access on a business need to see basis.
How will the information be destroyed (e.g. secure erasure, cross cut shredder, confidential waste disposal)?
Who will need to have access to the information (e.g. list individuals and staff groups)? In the answer include a description of the security controls to be applied to control access on a business need to see basis.
With whom will the data be shared (e.g. individuals, third parties)? In the answer include a description the security controls to be applied to control access on a business need to see basis.
Will any information be sent outside the Heriot-Watt Group and its computer networks? If so please give details of security controls in place.
What records retention policy will be applied to the data and who is accountable for implementing the policy (e.g. student, HRD)? Information on retention schedules is available here: https://www.hw.ac.uk/services/heritage-information-governance/manage/what-to-keep.htm

Step 2: Describe Stakeholders and Consultations

Identify internal and external stakeholders and how and when you will consult with them. The consultation needs to take place at appropriate stages in order to take into consideration stakeholders' views and to make changes if necessary. Consider the information on consultation requirements before providing the information required below.

Information on consultation requirements
Include: • *Who will be consulted internally and externally (e.g. senior management, IT, student support, EBS partners, suppliers, data processors, students, employees, DPO)?* • *How will consultation be undertaken?* • *At what stage will you consult?* *You can use consultation at any stage of the DPIA process. However the results of the consultation need to be taken into account and be capable of influencing decisions about the processing.*

If it is not appropriate to consult individuals then please record this decision here with a clear explanation. For example, you might be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable. *If the DPIA covers the processing of personal data of existing contacts (for example, existing customers or employees), the consultation should seek the views of those particular individuals, or their representatives.* *If the DPIA covers a plan to collect the personal data of individuals you have not yet identified, you may need to carry out a more general public consultation process, or targeted research. This could take the form of carrying out market research with a certain demographic or contacting relevant campaign or consumer groups for their views.* *If your DPIA decision is at odds with the views of individuals, you need to document your reasons for disregarding their views.* *If you are not sure whether or not you need to consult, contact the DPO/Compliance Manager.*	
Internal stakeholders	Identify internal stakeholders: (e.g. senior management, Information Services, student support, DPO).
External stakeholders	Identify external stakeholders (e.g. partners, suppliers, data processors, or external contractors).
Data subjects	Identify data subjects (e.g. students, employees) and/or their representatives and how you will seek their views where appropriate.

Step 3: Assessing the Risks in Association with the Data Protection Principles and other requirements of the GDPR
Answering these questions will help to identify where there is a risk that the project will fail to comply with the GDPR or other relevant legislation. When completing this step, please consider the risks to individuals and to the University Group set out in Annex 3.
The Data Protection Principles are set out in Article 5 of the GDPR.

Principle 1
Personal data shall be processed lawfully, fairly and in a way that is transparent to the data subject ("lawfulness, fairness and transparency")
In order to process personal data lawfully, you need to meet at least one of the conditions in Annex 1 and in the case of special categories of personal data, at least one of the conditions in Annex 2.
Describe the following
How will you tell individuals about the purpose of the project, the use of their personal data and who to contact if they want to find out more?

Do individuals have a reasonable expectation that you will do this with their data? If not, this should be an element of your consultation with them.	Y		N	
Does your privacy notice explain to data subjects what information about them will be shared?	Y		N	
Does your privacy notice explain to data subjects with whom their information will be shared?	Y		N	
Does your privacy notice explain to data subjects why their information will be shared?	Y		N	
Do you need to amend your privacy notices?	Y		N	
Does your privacy notice contain a link to the relevant Heriot-Watt Group privacy notice? The Heriot-Watt Group's privacy notices are available here: https://www.hw.ac.uk/about/policies.htm	Y		N	
What legal bases for processing under the data protection legislation will apply? Please explain all that apply. *See answer to legal basis for processing data in Annex 2.*				
If you are relying on consent to process personal data: • How will this be collected? • What will you do if it is withheld or withdrawn?				
Are you relying on consent which has previously been given? If YES how and when was the consent obtained and is it still valid under GDPR?				
Under the UK Equality Act 2010 the University has a duty to ensure equality and diversity is embedded throughout its functions that impact on people. Where the need for a DPIA has been identified an equality impact assessment may also be required. If you are unsure please consult the Data Protection Officer. The Equality Impact Assessment form is published on the Human Resources forms page here and there is more information on the Equality and Diversity web pages. Where necessary, please record the outcome of the EIA here and include any recommended actions in the relevant sections below (step 6 and 7). As the University is subject to the UK Human Rights Act (HRA), the following factors also need to be considered: • Will your actions interfere with the right to privacy under Article 8 of the HRA? • Have you identified the social need and aims of the project? • Are your actions a proportionate response to the social need?				

Principle 2
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')

Does your project plan cover all of the purposes for processing personal data?	Y		N	
Have you identified potential new purposes as the scope of the project expands?	Y		N	
If YES, what are the benefits to the University and to individuals?				
What lawful condition of processing have you identified for these purposes?				
Do the data subjects have a reasonable expectation that you would use the data for these purposes?	Y		N	
Do the privacy notices need to be reviewed periodically during the course of the project to reflect these changes?	Y		N	

Principle 3				
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');				
Is the quality of the information good enough for the intended purposes?	Y		N	
How will you ensure that you have collected sufficient data to achieve the intended purpose?				
Is all of the information necessary for the purpose?	Y		N	
Which personal data could you not use, without compromising the needs of the project?				
Are any of the data processing activities particularly intrusive?	Y		N	
If YES, please provide details and confirm whether or not any of the data processing can be avoided without affecting the intended purposes?				
Is the processing proportionate to achieve its purpose?	Y		N	
Please explain your reasoning and give examples (e.g. the aims of the project can't be achieved without collecting and/or sharing this data).				
How will you prevent function creep (i.e. the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended)?				

Principle 4				
Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');				
If you are procuring new software does it allow you to amend data when necessary and retain any audit trail of changes?	Y		N	

How are you ensuring that personal data obtained either from other Heriot-Watt Group systems, from individuals or from other organisations is accurate?
How will the information be kept up to date and checked for accuracy?
How will you make it easy for individuals to update their data securely?

Principle 5
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
What records retention policy will be applied to the data and who is accountable for implementing the policy (e.g. student, HRD)? (Information on retention schedules is available here: https://www.hw.ac.uk/services/heritage-information-governance/manage/what-to-keep.htm).
Retention policies apply to activities as well as to personal data. A software system needs to be able to apply deletion policies to transactions that no longer need to be retained, without deleting the entire record of the person.
How will you delete information in line with your retention periods?
Confirm that this will form part of the specification of mandatory requirements for any system or procurement.
Can the data be anonymised if needed for statistical or research purposes, publication, or re-use? If data is truly anonymised it is no longer personal data.

Principle 6
Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')
What are the risks in relation to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the data in storage, in transit, and when in use?
How will the specification for any new systems provide protection against the security risks you have identified?

What controls and processes will you put in place to provide and rescind access to the data on a need to see basis?				
How is data protected in transit (e.g. when communicated by email) to ensure that only the intended recipient can access it?				
Do you intend to use any of the following?	Y		N	
• Encryption • Pseudonymisation • Anonymisation to share or publish statistical data while needing to retain the original data set containing personal data. If YES please give details.				
Resilience				
How often will the system data be backed up?				
Where will the backup data be stored?				
How quickly can access be restored following disruption of service?				
Outline training and instructions necessary to ensure that users: • Understand potential security risks; • Understand their responsibilities and how to apply these; • Understand what actions they need to take to protect the data.				
What process will be in place for testing the security of the system and how often will this take place?				
Will the system have security logs?	Y		N	
If YES, what will these record?				
How will the information be destroyed (e.g. secure erasure, cross cut shredder, confidential waste disposal)?				
Is there a need to lock down access to specific locations (e.g. one office, one secure laboratory)	Y		N	
Is there a need to provide remote access to the data?	Y		N	
If YES, how will this be secured?				

Has the external supplier agreed to enter into the University GDPR –compliant data processor or data sharing agreement?	Y		N		

Step 4. Explain how you will comply with the rights of data subjects					
The Right to be Informed: a data subject has the right to be given information about how their data is being processed and why.					
How will you inform data subjects what you are doing with their data when you obtain it from them (e.g. using a privacy notice)?					
How will you inform data subjects what you are doing with their data when you obtain it from someone else (e.g. from a public website)?					
The Right to Access: a data controller must provide a data subject with confirmation as to whether or not personal data concerning him/her are being processed, and where this is the case, access to the data free of charge within one month of the request.					
How will you identify and retrieve all information in a system that relates to a data subject?					
Can you provide self-service access for data subjects to obtain their records?	Y		N		
If YES, explain how?					
The Right to Rectification: a data controller is entitled to have their personal data rectified if inaccurate or incomplete					
If a data subject asks for inaccurate data about them to be corrected, how would you achieve this?					
The Right to Erasure: applies where it is no longer necessary to process the personal data or the data subject withdraws their consent where no overriding lawful grounds apply.					
If a data subject asks for their data to be erased, how would you achieve this?					
If a data subject asks you to restrict further processing of their data (e.g. until a complaint or request to correct inaccurate data has been resolved, or to prevent scheduled deletion until they have obtained a copy of the data) how will you comply with this?					
The Right to Data Portability: applies only where processing is based on consent or contract and allows a data subject to obtain and reuse their personal data across different services for their own purposes.					

How can a data subject be provided with a machine readable copy of the personal data he or she has provided (e.g. CSV file or other format that can be exported from one system to another)?					
Consent: applies only where processing is based on consent.					
If a data subject withdraws their consent for their data to be processed for specific purposes, what would you have to do to comply with this?					
The Right to Object: applies to all processing for marketing purposes. Also processing based on public interests/legitimate interests where no overriding public interest applies.					
If a data subject asks you to stop processing their data what would you have to do to comply with this?					
Automated Individual Decision-making, Including Profiling: a data subject has the right to obtain human intervention, express his or her point of view and to contest the decision.					
Does the system make automated decisions about data subjects that may have a significant impact on them?	Y		N		
Is YES, please give details.					
If YES, explain how you will you comply with a data subject's right to obtain human intervention, express his or her point of view and to contest the decision?					

Step 5. International Transfers

Depending upon the advice received for Part 2, Question 4, and the advice you received from the Data Protection Officer/Compliance Manager, you will need to confirm the safeguard that you have in place for any international transfers of personal data.

Examples of safeguards include:

- The European Commission (EU) has designated the country as providing an adequate level of protection for privacy;
- The organisation processing the data will sign an agreement with the University including the EU standard contractual clauses for international data transfers;
- The organisation processing the data will sign the University data processor or data controller/data controller data sharing agreement and provide evidence of its certification under the EU –US Privacy Shield

PART 5
SUMMARY OF PRIVACY AND INFORMATION GOVERNANCE RISKS AND SOLUTIONS

Step 1:Identify Privacy and Information Governance Risks and Solutions

Identify the key privacy risks:

- To individuals;
- For the University;
- To legal compliance.

To calculate the level of risk please refer to your answers in Part 3 or Part 4, examples of privacy related risks in Annex 3, and to the risk assessment matrix in Annex 4. Identify the key privacy risks and then consider the applicable measures to reduce the risks.

For projects that have a risk register, risks identified in this DPIA need to be added to that project risk register so that the Project Board can have proper oversight of their management . This methodology should also link to the University Project Management Methodology.

Indicate whether risks are low (L), medium (M) or high (H) and provide solutions to ensure the protection of personal data (i.e. details of measures to address risks, including safeguards and security measures).

Risk	**Gross governance risk level (L/M/H)** This is the risk before taking steps to reduce the risk See matrix in Annex 4 to determine risk level	**Measures to be taken to reduce risk** Confirm that the risk can be: • Terminated • Transferred (e.g. insurance/contract) • Treated (mitigation plan) • Tolerated (no additional mitigation required)	**Net risk (L/M/H)** This is the risk taking into consideration measures to reduce the risk See matrix in Annex 4 to determine risk level	**Confirmation that actions have been taken**
Risk to Individuals (e.g. breach of privacy)				
Risk to University Group (e.g. breach of compliance, financial or reputational risk)				

Risks added to the project risk register by (for projects that have a risk register)		
Name	Role	Date

Step 2: Sign Off and Record DPIA Outcomes		
Please use this section to confirm that the actions identified in Step 5 have been integrated into the project plan		
Approved by	**Name/Role**	**Date**

Step 3: Reviewed by Data Protection Officer/Compliance Manager	
Name	
Date:	
Please provide the following additional information:	
OR	
I endorse /disagree with the DPIA conclusions and approved solutions *Give reasons*	
Prior consultation *For any high risks remaining after solutions have been approved the DPO is required to consult the Information Commissioner's Office. The University must await a decision by the ICO before proceeding with the processing activity. The ICO will give written advice within 8 weeks, or 14 weeks in complex cases. In appropriate cases the ICO may issue a formal warning not to process the data, or ban the processing altogether.*	
Referred to ICO on date	
Outcome	
Outcome communicate on date	

Step 4: Confirmation of Actions Taken	
Name	
Role	
Date	
Provide confirmation of action taken and date of completion of actions	

ANNEX 1: LEGAL BASIS FOR PROCESSING PERSONAL DATA UNDER GDPR

In order to process personal data lawfully, the University must be able to demonstrate that it complies with one of the following conditions. Where we process personal data for more than one purpose, a lawful condition must be identified for each purpose. The lawful condition provides the legal basis for processing.

In order to process special categories of personal data the University must be able to comply with one of the following conditions AND at least one of the conditions set out in Annex 2 below.

1. Identify a condition for processing personal data (GDPR Article 6)

Consider if the reason for the processing is on the basis of one of the following categories.

(a) Freely given explicit consent for one or more specific purposes. Do not rely on consent if processing would still need to be carried out if a person said no or subsequently withdrew their consent, or if one of the other categories apply;
(b) Processing is necessary for performance of a contract or steps (at the request of an individual) before entering into a contract;
(c) Necessary for compliance with a legal obligation to which the Data Controller is subject;
(d) necessary in order to protect the vital interests of the data subject or of another natural person;
(e) Necessary for performance of a task in the public interest, or in the exercise of official authority vested in the controller; DPO can assist if this might fall within the public interest determined by the University's charter and statutes);
(f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

2. If the condition is legitimate interests

The GDPR states that public authorities cannot use legitimate interests as a legal basis for processing personal data in the performance of their "public tasks". As Heriot-Watt University and Edinburgh Business School are public authorities this means that we cannot rely on legitimate interests to process data for University purposes set out under the Charter and Statutes such student administration, learning, teaching and research.

In order to determine whether a member of the University Group can rely on legitimate interests it is necessary to apply a three part test called a Legitimate Interests Assessment (LIA). We use the following LIA developed by the Information Commissioner's Office (ICO) https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

You can seek advice at any stage from the DPO/Compliance Manager.

3. Legitimate Interests Assessment (LIA)

Part 1: Identify the legitimate interest(s)

Why do you want to process the data – what are you trying to achieve?				
Who benefits from the processing? In what way?				
Are there any wider public benefits to the processing?	Y		N	
How important are those benefits?				
How is data protected in transit to ensure that only the intended recipient can access it?				
What would the impact be if you couldn't go ahead?				
Would your use of the data be unethical or unlawful in any way?				

Part 2: The necessity test

Does this processing actually help to further that interest?	Y		N	
Is it a reasonable way to go about it?	Y		N	
Is there another less intrusive way to achieve the same result?	Y		N	

Part 3: The balancing test

Consider the impact of your processing and whether this overrides the interest you have identified.

You can consider legitimate interests for processing children's data, but you must take extra care to make sure their interests are protected.

What is the nature of your relationship with the individual?				
Is any of the data particularly sensitive or private?	Y		N	
Would people expect you to use their data in this way?	Y		N	
Are you happy to explain it to them?	Y		N	
Are some people likely to object or find it intrusive?	Y		N	
What is the possible impact on the individual?				
How big an impact might it have on them?				

Are you processing children's data?	Y		N	
Are any of the individuals vulnerable in any other way?	Y		N	
Can you adopt any safeguards to minimise the impact?	Y		N	
If so please describe them.				
Can you offer an opt-out?	Y		N	

You then need to make a decision about whether you still think legitimate interests is an appropriate basis. There's no foolproof formula for the outcome of the balancing test – but you must be confident that your legitimate interests are not overridden by the risks you have identified.

If you are not sure about the outcome of the balancing test, it may be safer to look for another lawful basis. Legitimate interests will not often be the most appropriate basis for processing which is unexpected or high risk.

Conclusion				
The processing meets the legitimate interests test	Yes		No	
Please answer YES only if *1. You have identified a legitimate interests* *2. The legitimate interest is NOT overridden by the risks to the privacy rights of individuals*				
Please send this completed LIA to the DPO/Compliance Manager at the email address on page 3				

Actions
Details of any safeguards to be taken to protect the rights of individuals
Text for privacy notice to be provided to the individuals

Reviewed by Data Protection Officer	
Name:	
Role	
Date:	
I agree/disagree with the LIA decision *Give reasons*	
The DPO/Compliance Manager will keep a record of your LIA and the outcome. Keep your LIA under review and refresh it if there is a significant change in the purpose, nature or context of the processing.	

ANNEX 2: CONDITIONS FOR PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA (GDPR ARTICLE 9)

What's different about special category data?

You must still have a lawful basis for your processing under Article 6, in exactly the same way as for any other personal data. The difference is that you will also need to satisfy a specific condition under Article 9.

This is because special category data is more sensitive, and so needs more protection. For example, information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

Under the GDPR processing of personal data relating to **criminal convictions and offences** is only allowed under limited circumstances, which may be further defined by UK law. Please ask the DPO/Compliance Manager for advice if your processing involves this special category of data.

What are the conditions for processing special category data?

The conditions are listed in Article 9(2) of the GDPR:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular

contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

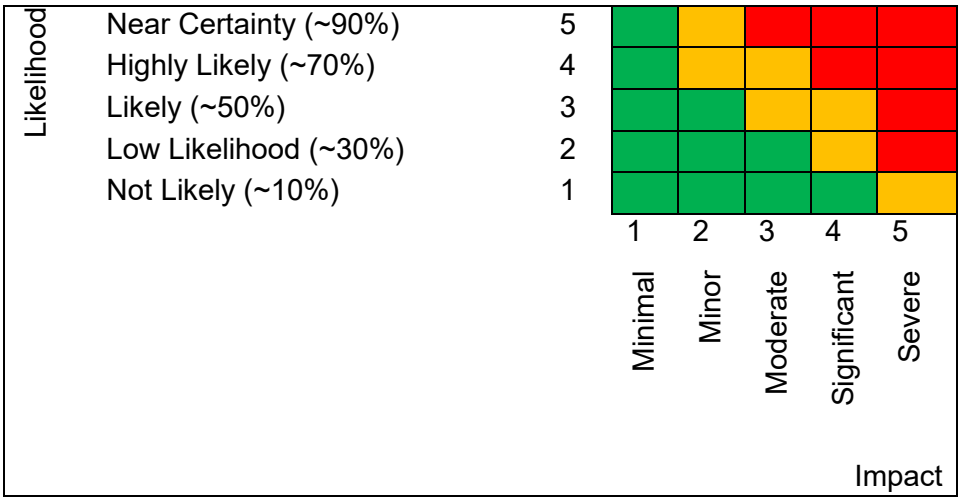
e) processing relates to personal data which are manifestly made public by the data subject;
f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 of Article 9 of the GDPR;
i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

ANNEX 3: EXAMPLES OF PRIVACY RELATED RISKS

Risk to Individuals
1. Inadequate disclosure controls or security measures, increasing the likelihood of information being shared inappropriately (e.g. via IT systems)
2. The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge or consent
3. Surveillance methods may be an unjustified intrusion on individuals' privacy
4. Failure to ensure that personal information is kept up to date
5. Collecting information and linking identifiers might mean that we no longer use information that is safely anonymised; or pseudonymised data is identified
6. Information may be collected and stored unnecessarily, or not properly managed so that duplicate records are created, presenting a greater security risk
7. If an appropriate retention period is not established this might mean information is retained or used for longer than necessary
8. Information may be collected and stored unnecessarily, or not properly managed so that duplicate records are created
9. Information may be subject to profiling or automated processing without the a data subject's consent
10. The data subject may suffer a breach of confidentiality
11. The processing may result in data subjects' inability to exercise rights (including but not limited to privacy rights), access services or opportunities, or be put an any other significant economic or social disadvantage
12. The processing may result in discrimination against individual data subjects
13. Data subjects may lose control over their personal data
14. Data subjects may suffer identity theft, fraud or financial loss due to unlawful data collection, processing or failures in security controls
15. Data subjects may be put at a risk of physical harm in the event of a security breach
Risks to the University Group or to Compliance
16. The sharing and merging of datasets means we collect a much wider set of information than people might expect
17. Public/customer distrust about how information is used may damage the University's reputation and lead to loss of business
18. Data losses which damage individuals could lead to claims for compensation or the imposition of a financial penalty
19. Non-compliance with Data Protection Act or other relevant legislation/ 20. regulations can lead to sanctions, fines and reputational damage
21. Non-compliance with the rules on marketing (Privacy and Electronic Communications Regulations (PECR)
22. Problems which are only identified after the project has launched are more likely to require expensive fixes
23. Difficulties associated with insufficient consents being obtained from data subjects
24. Information which is collected is stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business

ANNEX 4: RISK ASSESSMENT MATRIX

Use the risk assessment matrix to define the levels of risk for each risk identified.



Risk Level	
Low	
Medium	
High	