Data Protection Impact Assessment (DPIA) Policy
IGP-08

Summary			
The General Data Protection Regulation (GDPR) requires organisations to undertake Data Protection Impact Assessments (DPIAs) to assess and address risks to individuals whose personal data they process. This Policy sets out the university's approach to identifying the need for, undertaking and implementing DPIAs.			
Scope			
This Policy applies to all of the University's faculties, schools and divisions. All the University's activities involving personal data are subject to the Policy and the potential requirement to conduct a DPIA.			
Document Control			
Document type	Data Protection Impact Assessment Policy – IGP-08		
Document owner	Information Governance Manager		
Division	University Secretary's Office		
Lead contact	Information Governance Manager		
Document status	Draft		
Version	d.0.5		
Approved by	Information Governance and Security Advisory Board (IGSAB)	Date	June 2019
Date of publication	June 2019	Next review date	June 2021
Date of original publication	June 2019	Revision frequency	2 years
Superseded documents	Previous Privacy Impact Assessment template		
Related documents	See Information Governance section of SECO website		

Contents

1. Introduction

1.1. The General Data Protection Regulation (**GDPR**) and Data Protection Act 2018 (DPA) require the University as a data controller to consider and apply appropriate measures designed to implement their key principles effectively. Necessary safeguards must be incorporated into all activities involving the processing of personal data in order to ensure that the rights and freedoms of individuals are protected. This is known as "Data Protection by Design".

1.2. A key element of the GDPR's focus on accountability and Data Protection by Design is the requirement to undertake a Data Protection Impact Assessment (**DPIA**) (often referred to as a Privacy Impact Assessment) where any processing of personal data is "*likely to result in a high risk*" to the rights and freedoms of individuals.

1.3. A DPIA therefore serves as a tool to help the University to identify, evaluate and mitigate risks to individuals arising as a result of the processing of their personal data. At the same time, a DPIA should ensure compliance with data protection law and other legal and regulatory requirements (for example, the Equality Act 2010).

1.4. A failure to undertake a DPIA when required under the GDPR may result in a fine of up to €10 million or 20% of total global annual turnover, whichever is higher.

2. About this Policy

2.1. This Policy sets out the University's approach towards identifying the need for, undertaking and implementing DPIAs.

2.2. A glossary of the terms used throughout this Policy can be found in Appendix 1.

3. Scope of this Policy

This Policy applies to all the University's schools, faculties and professional divisions. It is relevant to both corporate functions and research activities.

4. Roles and responsibilities

4.1. All members of staff involved in the development of projects, initiatives, studies, processes and systems (collectively referred to in this Policy as **Initiatives**) are responsible for ensuring that they are aware of this Policy and understand the circumstances in which a DPIA should be undertaken.

4.2. The University's Data Protection Officer and Information Governance Manager is responsible for overseeing and reviewing the implementation of this Policy and must be consulted in relation to any DPIAs undertaken in accordance with its requirements.

4.3. In practice, it is the responsibility of the staff member or team leading an Initiative to undertake the screening questions and produce the first draft of a DPIA if necessary, i.e. the project manager, system owner, principal investigator etc. This can then be further worked up in collaboration with the Data Protection Officer and Information Governance Manager, and other relevant stakeholders.

4.4. **Draft DPIAs should be sent to the Information Governance Team at data-protection@bristol.ac.uk**

DPIAs produced as part of the IT Services new service assessment procedure, or with an IT element, should also be send to the Information Security Team at cert@bristol.ac.uk

5. Identifying the need for a DPIA

5.1. A DPIA must be undertaken *before* the processing of any personal data which is "*likely to result in a high risk to the rights and freedoms*" of individuals. As such, it is necessary to identify whether there are any factors that warrant the need for a DPIA to be undertaken.

5.2. In the case of any Initiatives involving the processing of personal data that were commenced before 25th May 2018 (when the GDPR came into force) and which are ongoing, such Initiatives should be reviewed and the need to undertake a DPIA considered.

5.3. The GDPR requires a DPIA to be undertaken where any Initiative will involve:

a. the systematic and extensive evaluation of personal data by automated means, including profiling, resulting in decisions that would have significant effects for those individuals;

b. the processing of special categories of personal data (see glossary in Appendix 1 for definition) or personal data relating to criminal convictions and offences on a large scale; or
c. the systematic monitoring of a publicly accessible area on a large scale.

5.4. Where any new Initiative will involve the processing of personal data, the DPIA Screening Questionnaire in Appendix 2 should be completed. It is expected that the questionnaire will be completed by those leading the development of the Initiative.

5.5. Before completing the questionnaire, it is important to:

a. identify the key stakeholders in the Initiative so that they can provide their input into the questionnaire; and
b. have a clear understanding of the scope and objectives of the Initiative so that the questionnaire can be completed as fully and accurately as possible.

5.6. If there is any uncertainty regarding completion of the questionnaire or the outcome, the University's Data Protection Officer should be consulted.

5.7. Where the outcome of the questionnaire suggests that the processing is unlikely to result in a high risk to individuals, there may be circumstances where it is advisable to undertake a DPIA anyway due to:

a. the nature, scope, context and purposes of processing personal data;
b. the groups of individuals affected by the processing (e.g. children or vulnerable adults);
c. the level of investment in the Initiative in terms of time, financial and other resources; or
d. the visibility of the Initiative internally and externally.

5.8. Where it has been concluded that a DPIA is unnecessary and will not be undertaken, the reasons for this should be clearly documented. The Screening Questionnaire should be retained to evidence the decision made and may need to be revisited and reviewed at a later date.

6. Undertaking a DPIA

6.1. Having concluded that a DPIA is necessary or desirable for a particular Initiative, the DPIA Template in Appendix 3 should be completed. The DPIA Template explains the objectives and requirements of each section. Where any section is not completed because it is not applicable or not considered necessary, this should be explained.

6.2. Part of the DPIA may involve consultation with relevant internal and external stakeholders. In the case of consultation with third party data processors, the contract with such third parties should include an obligation on them to provide assistance with undertaking DPIAs. However, this may have cost implications which should be considered and discussed with the third parties beforehand. In the case of consultation with professional advisers and other experts, the scope and cost of their

involvement will need to be considered and approved by the University's Data Protection Officer and Information Governance Manager.

7. Consultation with the ICO

7.1. Where the outcome of a DPIA is that the processing of personal data in the context of an Initiative *would* result in a high risk and it is not possible to take any measures to eliminate or mitigate that risk, the GDPR requires that the processing cannot commence before the Information Commissioner's Office (**ICO**) has been consulted.

7.2. The ICO should not be consulted without the approval of the University's Data Protection Officer, who will usually initiate contact with the ICO. Consultation with the ICO should only be necessary in very exceptional instances as it is expected that the University will be able to apply measures to appropriately mitigate or eliminate risk on most occasions.

7.3. The Data Protection Officer will contact the ICO, sending a copy of the DPIA together with a cover letter to dpiaconsultation@ico.org.uk. The ICO intends to respond to requests for consultation within eight weeks, though it can extend such period by a further six weeks in complex cases.

7.4. The ICO will provide a written response confirming whether the risks identified are acceptable or whether further action is required. In some cases, the ICO may recommend that the processing is not undertaken.

8. Review of DPIAs

8.1. A DPIA should be undertaken at the earliest opportunity in the development of an Initiative and re-assessed prior to commencement of the relevant processing activities to identify whether any changes to the Initiative impact upon the outcomes of the DPIA and whether the controls and measures identified in the DPIA have been integrated into the Initiative.

8.2. Once the processing of personal data has commenced in respect of an Initiative, the DPIA should be reviewed regularly having regard to the nature and risks associated with the processing, taking into account any changes to the processing activities or scope of the Initiative. A review should be undertaken at least annually by the staff member or team leading or owning the Initiative.

9. Disclosure and publication of DPIAs

9.1. There is no legal requirement to proactively disclose or publish a DPIA, although it could be subject to a request made under the Freedom of Information Act 2000 so may need to be released, subject to any exemptions contained in the legislation. However, it may be necessary to disclose a DPIA to another institution to provide assurance that due and proper consideration has been given to the data protection implications of an Initiative.

9.2. A decision may also be taken to publish a DPIA in order to foster trust and confidence in the processing of personal data in relation to an Initiative and to demonstrate accountability and transparency. However, such decision may only be taken in consultation with the University's Data Protection Officer and Information Governance Manager, and any DPIA that is being published should be redacted to remove any confidential or commercially sensitive information.

10. Policy review

This Policy will be reviewed as required and at least every 2 years by the University's Information Governance and Security Advisory Board IGSAB.

Document history

Version	Date	Summary of change	Reviewer	Approved by	Approved date
d0.1 draft	May 2018	Initial draft	External legal resource		
d0.2 draft	October 2018	Amends to initial draft	Information Governance Manager & Data Protection Officer		
d0.3 draft	May 2019	Additions and amends	IT Services Head of Governance, Information Governance Manager & Data Protection Officer		
d0.4 draft	June 2019	Minor amends	IGSAB		
d0.5	June 2019	Amendment to screening questions	Head of Research Governance		

Appendix 1 – Glossary of terms

data controller	the person or organisation that determines the purposes and means of processing personal data
criminal convictions and offences	personal data relating to criminal convictions, the commission or alleged commission of an offence, proceedings for the commission or alleged commission of an offence and sentencing
data subject	an individual to whom personal data relates and who can be identified or is identifiable from personal data
GDPR	the General Data Protection Regulation (Regulation (EU) 2016/679)
DPA	Data Protection Act 2018
personal data	any information identifying or relating to a data subject that can be identified (directly or indirectly) from that data alone, or in combination with other identifiers possessed or that can be reasonably accessed. Personal data includes criminal convictions and offences data, special categories of personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently, irreversibly removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour
process, processes, processing	any activity or set of activities which involves personal data including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or making available, alignment or combination, restriction, erasure or destruction
pseudonymised, pseudonymisation	replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms (e.g. a numerical code or key) so that the data subject cannot be identified without combining the identifier or pseudonym with other information which has been kept separately and securely. Personal data that has been pseudonymised is still treated as personal data (unlike personal data which has been anonymised)
special categories of personal data	previously known as “sensitive personal data” under the Data Protection Act 1998, this means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and, for the purposes of this policy, personal data relating to criminal offences and convictions.

Appendix 2 – Data Protection Impact Assessment Screening Questionnaire

Data Protection Impact Assessment (DPIA)
Screening Questionnaire

Date		
Assessor's Name		
Title of Initiative / project / process / study / system		
Summary of Initiative		
Outcome	☐	At least two questions answered 'yes' – DPIA required
	☐	One question answered 'yes' – DPIA not required, but recommended
	☐	No questions answered 'yes', and the Initiative will have a minimal impact on privacy – DPIA not required

Questions	Yes	No	Comments
1. Will the Initiative concern vulnerable individuals (for example children or vulnerable adults)?	☐	☐	
2. Will the Initiative involve special categories of personal data and/or personal data relating to criminal convictions or offences about themselves? (see DPIA Policy glossary for definitions)	☐	☐	
3. Will the Initiative involve the use of biometric data or genetic data?	☐	☐	
4. Will the Initiative involve the processing of personal data on a large scale, having regard to: • **the number of individuals concerned (i.e. over 100)** • **the volume of personal data** • **the range of personal data, and** • **the duration/permanence of the processing activity (i.e. over 1 year)?**	☐	☐	
5. Will the Initiative involve the evaluation or scoring of personal data, including profiling and predicting (for example competence for a role or genetic testing)?	☐	☐	
6. Will the Initiative involve systematic monitoring of individuals, including in a publicly accessible area?	☐	☐	

7. Will personal data about individuals be disclosed to people or organisations that have not previously had access to the personal data (including external collaborators, service or system providers, and cloud hosting services)?	☐	☐	
8. Will personal data be used for a purpose it is not currently used for or in a way that it is not currently used?	☐	☐	
9. Does the Initiative involve the use of new or unusual technology that is, or might be, perceived by individuals as privacy intrusive?	☐	☐	
10. Will the Initiative result in making decisions about, or taking actions against, individuals by automated means which might produce legal effects concerning them, or similarly significantly affect them through decisions made?	☐	☐	
11. Would the processing of personal data contemplated by the Initiative be outside of the reasonable expectations of the individuals?	☐	☐	
12. Will the Initiative involve contacting or interacting with individuals in ways that they might find intrusive?	☐	☐	
13. Will the Initiative involve the processing of personal data by third parties with whom the organisation has no experience of working?	☐	☐	
14. Will the Initiative involve the transfer of personal data outside the European Economic Area (the EU plus Norway, Lichtenstein and Iceland)?	☐	☐	

Appendix 3 – Data Protection Impact Assessment Template

Data Protection Impact Assessment (DPIA) relating to:
[Title of Initiative/project/process/study/system etc]

DPIAs should be sent to the Information Governance Team at **data-protection@bristol.ac.uk**
DPIAs produced as part of the IT Services new service assessment procedure, or with an IT element, should also be send to the Information Security Team at **cert@bristol.ac.uk**

Document control

Version	Date	Author	Summary of changes	Approver	Approval date

Part A: Summary of the Initiative	
Describe the scope of the Initiative (to include its aims and objectives; business/research/other case; level of investment in terms of time, financial and other resources; duration and geographic reach; visibility within and outside the organisation)	
Status of the Initiative (describe the current phase of development or implementation of the Initiative or, if the Initiative has already commenced, when it commenced and the extent to which the processing activities relating to the Initiative are still ongoing)	
Part B: Description of the processing	
Nature of the processing	
Method(s) of collection (e.g. online or paper-based forms completed by data subjects or feeds from other systems)	

Source(s) of the personal data being processed (if personal data originates from third party sources, describe them)	
Matching or combination of datasets (to what extent does the processing involve multiple datasets collected for separate purposes)	
Processing activities relating to the personal data (how will personal data be processed after collection)	
Scope of data sharing with third parties (you may want to refer to a data flow diagram or other materials explaining data flows)	
Extent of automated decision-making (describe extent to which decisions are made about data subjects without human intervention/review, e.g. through the use of automated algorithms)	
Scope of the processing	
Categories of personal data (identify each category of personal data processed, including any special category data and information relating to criminal convictions and offences)	

Categories of data subject (e.g. staff, students, research participants, website visitors, device users, children, vulnerable adults)	
Format of the personal data (e.g. paper records, electronic documents, spreadsheets, databases, system records or other files)	
Storage location (e.g. locked filing cabinets, document repositories, on-premise servers or storage devices, cloud-hosted services in UK, EU or international)	
Duration and frequency of processing (by reference to the relationship with the data subject or the nature of the Initiative)	
Volume of data subjects and records (or an approximation where it is not possible to confirm precise numbers at present)	
Context of the processing	

Relationship with data subjects (describe the proximity between the University and the data subjects and how the relationship is established)	
Data subjects' expectations (describe the extent to which the data subjects are aware of and expect their personal data to be used in connection with the proposed processing activities)	
Use of new technology or novel approach (describe the extent to which the processing activities involve the use of any technology or other approaches that may be considered state of the art, novel or unexpected)	
Relevant matters of public concern (describe any matters of public concern relating to the scope of the processing or the use of any particular technology or approach, if applicable)	
Purposes of the processing	

Benefits to the data subject (describe how the processing benefits the data subjects/individuals either directly or indirectly)	
Benefits to the organisation (describe how the processing benefits the organisation either directly or indirectly)	
Benefits to third parties (describe how the processing benefits any third parties either directly or indirectly)	
Part C: Consultation process	
Input of internal stakeholders, experts and other professionals (advice from parties including senior staff, specialists, IT experts, lawyers, security consultants, ethics advisers etc, where applicable)	
Advice from Data Protection Officer (where applicable, obtaining the advice of the DPO is a mandatory requirement – this may be set out in a separate appendix/document)	

Input from data subjects (or their representatives) (where relevant describe the views sought, consultation methodology or justification for not seeking input)	
Part D: Assessment of necessity and proportionality	
Lawful basis for processing (identify the most appropriate ground(s) for lawful processing, explaining the rationale - see Appendix 3 for permissible grounds. For legitimate interests a separate legitimate interest assessment is needed.)	
Fairness and transparency (describe the means by which data subjects will be informed about the intended processing, e.g. fair processing notices, technical notifications, consent forms, participant information sheets)	
Data minimisation (describe the steps that will be taken to ensure that the amount of personal data is minimised and limited to what is strictly necessary both initially and on an ongoing basis)	

Necessity of processing (explain the extent to which the processing is necessary in relation to the purposes of the initiative)	
Accuracy (describe the steps taken to ensure data quality in terms of accuracy and freedom from bias, both initially and on an ongoing basis, e.g. verification techniques and how individuals can update their data)	
Storage limitation (describe the steps taken to ensure that personal data are not retained longer than necessary in connection with the intended purposes of the processing)	
Security, integrity and confidentiality (describe the steps taken to ensure the security of the personal data, including protection against personal data breaches)	
Data subject rights (describe the steps taken to ensure that data subjects are able to exercise their rights fully and effectively. Individuals have the right to be informed, and rights of access, rectification, erasure, objection and to stop automated decision making)	

Third party processors (where relevant, describe the steps taken to ensure the reliability of third parties processing the data on the University's behalf, and their compliance with data protection law)	
International transfers (identify any international transfers of personal data, whether or not to a third party processor, and the safeguards implemented in relation to such transfers)	

Part E: Identification and assessment of risks (see Appendix 1 and Appendix 2 for example risks and assessment process)

Ref No	**Source of risk and potential impact on data subjects** (including associated compliance and organisations risks)	**Likelihood of harm** (see Appendix 2)	**Impact of harm** (see Appendix 2)	**Overall risk** (low, medium, high)
1.				
2.				
3.				
4.				
5.				

Part F: Identification of controls and measures to eliminate or mitigate risk (of medium or high risks items in Part E)			
Ref No	**Controls or measures to eliminate or mitigate risk** (changes to design or additional safeguards and measures)	**Effect on risk** (extent to which risk is eliminated or mitigated by the controls or measures)	**Residual risk** (any risk remaining after controls or measures have been implemented)
1.			
2.			
3.			
4.			
5.			

Part G: Implementation and integration of controls and measures				
Action	**Approved by**	**Person(s) responsible**	**Target completion date**	**Completed**
				☐
				☐
				☐

				☐
				☐

Part H: Outcomes and sign-off		
Residual risks that cannot be eliminated or mitigated (if any)		
Consultation with ICO (where there are any residual high risks that cannot be eliminated or mitigated)	**Date submitted**	
	Submitted by	
	Outcome	
Consideration of Data Protection Officer's advice (confirm whether advice accepted and implemented or rejected, and if rejected the reasons why)		
Sign-off	**Name and role**	
	Date	
Frequency of review (usually at least annually)		

Next review date	

Schedule 1 – Example types of risk associated with the processing

Risks to data subjects

- Risk of processing being unlawful and/or regarded as unfair due to more personal data being collected than is necessary for the intended purposes of the processing
- Risk of personal data being inaccurate due to collection or processing methods or the nature of the personal data being processed
- Risk of personal data being retained longer than necessary or not properly managed so that duplicate records are created
- Risk of personal data being inadvertently manipulated due to human error or otherwise
- Risk of personal data being disclosed or accessed inappropriately due to inadequate access and disclosure controls
- Collection of personal data may be regarded as unnecessary and/or overly intrusive having regard to the objectives of the Initiative
- Risk of processing being unlawful and/or regarded as unfair due to scope and purposes of processing being extended inadvertently
- Use of new technologies, approaches or methods may constitute an unjustified intrusion on the data subjects' right to privacy
- Risk of processing being regarded as unfair due to complexity of processing activities/involvement of algorithmic analysis
- Risk of processing being regarded as unfair due to the combination of matching of multiple datasets
- Identifiers may be collected and linked which prevent data subjects from accessing or using a service anonymously
- Collection of personal data and linking identifiers may result in anonymisation being compromised
- Vulnerable data subjects may be particularly concerned about risks of identification or disclosure of personal data
- Processing of personal data may produce legal effects or similarly significantly affect the rights and interests of the data subject
- Processing of personal data may result in inappropriate inferences being made or discrimination being suffered by the data subject
- Disclosure of personal data may result in discrimination, victimisation and/or harassment

Compliance risks

- Non-compliance with data protection laws, including the GDPR, Data Protection Act 2018, Privacy and Electronic Communications Regulations and other secondary legislation
- Non-compliance with common law duty of confidentiality
- Non-compliance with the Equality Act 2010 and other equality and human rights legislation
- Non-compliance with sector-specific legislation or standards

Associated organisational risks

- Risk of regulatory sanctions and fines
- Risk of reputational damage
- Risk of considerable financial expenditure to mitigate any risk that has materialised
- Risk of erosion of trust and confidence in processing activities resulting in loss of business
- Risk of investment returns being reduced or eliminated
- Risk of inaccurate, incomplete or outdated personal data having reduced value
- Risk of research or statistical objectives being compromised, skewed or false
- Risk of claims from individuals for compensation

Schedule 2 – Risk assessment methodology

Evaluation of likelihood of harm

Likelihood score	1	2	3	4	5
Description	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost certain**
Frequency	Will probably never happen	Not anticipated to happen, but possible	Might happen or recur occasionally	Will probably happen or recur, but not persistently	Almost certain to happen or recur, possibly frequently

Evaluation of impact of harm

Likelihood score	1	2	3	4	5
Description	**Very Low**	**Low**	**Medium**	**High**	**Very High**
Impact	Unlikely to have any impact	May have an impact	Likely to have an impact	Highly probably it will have a significant impact	Will have a major impact

Overall evaluation of risk

Impact						
	Very High (5)					
	High (4)					
	Medium (3)					
	Low (2)					
	Very Low (1)					
		Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost certain (5)
		Likelihood				

Schedule 3 – Lawful basis for processing personal data

Personal data

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. The University's public tasks revolve around teaching and research. All research can come under this lawful basis.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. This cannot apply if the University is processing data to perform its public tasks. A legitimate interests assessment may be required.

Special category data

If you are processing special category data (information about an individual's race, ethnic origin, political opinion, physical or mental health, religion, trade union membership, genetics, biometrics, sexuality or sex life) then you also need a further lawful basis set out in Article 9 of GDPR. At least one must apply whenever you process special category data. The main Article 9 lawful bases are outlined here, though others also exist. Please seek further advice from the Data Protection Officer if required:

(a) Explicit consent: the individual has given their explicit consent to the processing of their personal data for the specific purpose.

(b) Employment law: the processing is necessary for pursing obligations set out in employment law.

(c) Vital interests: the processing is necessary to protect someone’s life where they are incapable of giving consent.

(d) Substantial public interest: the processing is necessary for reasons in the substantial public interest where it will safeguard the rights and interests of the individual.

(e) Medical purposes: the processing is necessary for the purposes of preventive or occupational medicine, or the provision of health care.

(c) Research purposes: the processing is necessary for purposes of scientific or historical research in the public interest. This lawful basis will apply to all research conducted by the University involving special category data.