UNIVERSITY OF
LEADING
THE WAY
WESTMINSTER

# University of Westminster Data Protection Impact Assessment (DPIA) Policy

## For Compliance with the General Data Protection Regulation & UK Data Protection Law

### 1. Background

1.1 The General Data Protection Regulation (GDPR), enforceable from May 2018, has replaced the Data Protection Act 1998 as UK personal data protection law. This legislation is also supplemented by the Data Protection Act 2018.

1.2 Under the above legislation the University as a Data Controller has an obligation to incorporate necessary safeguards into all activities that involve the processing of personal data, 'data protection by design'.

1.3 A key element in data protection by design is the requirement to undertake a Data Protection Impact Assessment (DPIA), sometimes also referred to as a 'Privacy Impact Assessment (PIA), where any processing of personal data is 'likely to result in a high risk' to the rights and freedoms of individuals. See Appendix One DPIA Screening Questions below and ICO Guidance.

1.4 A DPIA serves as a tool to help the University identify, evaluate and mitigate risks to identifiable individuals arising out of the processing of their personal data. It is also an opportunity to review personal data processing in relation to other legislation, e.g. The Human Rights Act, Equality Act 2010, etc.

1.5 A failure to undertake a DPIA when required by law could result in sanctions or fines from the governing authority, which in the UK is the Information Commissioner's Office.

See GDPR

### 2. Scope

2.1 This policy applies to all the University's Colleges, Schools, Departments, research and professional services activities and functions.

### 3. Roles and Responsibilities

3.1 All colleagues involved in the development of projects, initiatives, studies, surveys, processes, and systems (known from this point as an 'Initiative') are responsible for ensuring that they are aware of this policy and understand the circumstances in which a DPIA should be undertaken.

3.2 The University's Data Protection Officer and the Information Governance Advisory Group are responsible for overseeing and reviewing the implementation of

this Policy and must be consulted in relation to any DPIA's undertaken in accordance with the policy's requirements.

3.3 In practice, it is the responsibility of the colleague or team leading an Initiative to undertake the screening questions and produce a first draft of a DPIA if necessary, i.e., the Business Relationship Manager, Business Analyst, Project Manager, System Owner, Principal Investigator, etc. This can then be further elaborated on and completed with the assistance of the Data Protection Officer and the Information Compliance Team and other relevant stakeholders, including third party suppliers.

3.4 Information about DPIA's and early draft DPIA's should be sent to the Information Compliance Team dpa@westminster.ac.uk

3.5 DPIA's that are initiated as part of IT procurement, IT development or with an IT element should also be involved and be sent to the IS&S Developments – Data Security by logging a call to the Service Desk or by email to cybersecurity@westminster.ac.uk.

## 4. Identifying the need for a DPIA

4.1 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. It is therefore necessary to identify whether there are any factors that require the need for a DPIA to be undertaken.

4.2 The GDPR requires a DPIA to be undertaken where any initiative will involve:

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

4.2.2 The processing of special categories of personal data or personal data relating to criminal convictions and offences on a large scale; or

4.2.3 The systematic monitoring of a publicly accessible area on a large scale.

4.3 Where any new Initiative will involve the processing of personal data, the DPIA screening questions in Appendix One should be completed. These questions should be completed by those leading and knowing most about the intentions of the Initiative.

4.4 Before completing the questionnaire, it is important to identify key stakeholders in the Initiative so they can provide their input to the questions and have a clear understanding of the scope and objectives of the Initiative so the questionnaire can be completed as accurately as possible.

4.5 If in any doubt about the applicability of any of the screening questions, consult with the Information Compliance Team and the Data Protection Officer, as necessary.

4.6 Where the outcome of the DPIA questionnaire suggests that the Initiative 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;

4.6.1 The nature, scope, context and purposes of processing personal data.

4.6.2 The individuals affected by the processing (e.g., vulnerable adults, children, etc.)

4.6.3 The strategic nature or level of investment in the Initiative in terms of time, finances, and other University resources.

4.6.4 The importance and visibility of the Initiative internally and externally.

4.7 Where it has been concluded that a DPIA is not necessary and will not be taken in relation to any Initiative, the questionnaire and any supporting reasons should be documented and retained to evidence the decision made. These should be submitted to the Information Compliance Team at dpa@westminster.ac.uk and may need to be revisited and reviewed later.

## 5. Undertaking a DPIA

5.1 Having completed the questionnaire and decided that a DPIA is necessary or desirable for a specific Initiative, the full DPIA template in Appendix One should be completed.

5.2 The sections of the DPIA form allow for the Initiative to be described in both diagram and text and the key privacy risks, risk controls and control owners to be captured and eventual implementation agreed and signed off.

5.3 Completing the DPIA runs alongside other Initiative tasks, but the DPIA should be completed *prior* to the processing of the personal data it describes starting.

5.4 Completing the DPIA successfully is likely to involve relevant internal and external stakeholders. In relation to involving any third-party data processors (service providers), the contract they have with the University should cover an obligation to assist the University in required DPIA's. However, this may have cost implications which may need to be discussed and agreed with third parties beforehand.

## 6. Review of DPIA's

6.1 A DPIA should be taken at the earliest opportunity in the development of an Initiative and subject to ongoing assessment and review prior to any eventual completion and an Initiative going live, to ensure the Initiative is accurately reflected in the DPIA and the controls and measures it covers are adequate for the risks identified and all these controls have been integrated into the Initiative.

6.2 For Initiatives that are part of IT procurement, IT development or with an IT element, these DPIA's should follow a process agreed with IS&S Business Relationship Managers and the Digital Transformation Team. See Appendix Two for details.

6.3 In normal circumstances it is expected the identification of privacy risks and their controls and mediation will reduce the overall privacy risk related to any Initiative to Low or at most Medium. The University Risk Appetite is low to medium, so subject to the approval of the Cyber Security Technical Lead and the Data Protection Officer, DPIA's of this level of risk may be approved without further authorization.

6.4 In circumstances where any Initiative DPIA privacy risks have been identified that still remain above medium to high, even following suggested controls and mediation, these DPIA's will be escalated to the Senior Information Risk Officer and key stakeholders for discussion. Any introduction of these risks into normal University business will be exceptional and will be subject to consultation with the Information Commissioner's Office.

6.5 Once the processing in any DPIA has commenced, the authorized DPIA should be logged as completed and made available to the key stakeholders. Any future changes to processing within the scope of an existing DPIA could trigger another DPIA and an updated set of documentation.

6.6 DPIA's should record the Article 30 Records of Processing information at the time of the Initiative implementation. Again, changes to this information over time should be updated and any DPIA implications considered.

## 7. Consultation with the Information Commissioner's Office

7.1 Where the outcome of a DPIA is that the processing of personal data in the context of the Initiative would result in a high risk and it is not possible to take any measures to eliminate or mitigate that risk, and the University SIRO and stakeholders wish to proceed with the Initiative, the GDPR requires that the University consults with the ICO **before any processing relating to the Initiative takes place.**

7.2 The Data Protection Officer will initiate this contact with the ICO, which is likely only to happen in very exceptional circumstances, on the instruction of the SIRO.

7.3 The Data Protection Officer will send a copy of the DPIA and a covering note with all relevant information to the ICO.

7.4 Further activity on the Initiative will only take place in consultation with the ICO, which may cover providing additional information. In some cases, the ICO will confirm that the risks and mitigations described are acceptable to them or in others they may recommend the processing is not undertaken.

## 8. Disclosure and publication of DPIA's

8.1 Records of DPIA's should be kept with any project or initiative that requires them. A reference copy and all signed copies should also be available from the Information Compliance Team. They should be considered completed when they are signed off by either the Data Protection Officer or Senior Information Risk Officer,

8.2 There is no legal requirement to disclose or publish DPIA's, although the University is a public authority subject to the Freedom of Information Act 2000 (FOIA), so information held about DPIA's may be disclosed in response to questions raised under the FOIA if no applicable exemption on disclosure can be applied. DPIA's may be a condition of collaboration or a contractual obligation in some Initiatives.

8.3 Any published, disclosed or shared DPIA should be redacted to remove any personal, confidential or commercially sensitive information as applicable.

## 9. Policy Review

9.1 This policy should be reviewed as required and at least every two years in collaboration with relevant stakeholders and the Information Governance Advisory Group.

## 10. Related policies

This policy forms part of the information security management system (ISMS) at the University of Westminster.

The DPIA Policy should be read in conjunction with all other University information management policies, which are reviewed and updated as necessary to maintain an effective Information Security Management System to meet the University's business needs and legal obligations.

## 11. Publishing policies

This policy is published on the University website at https://www.westminster.ac.uk/about-us/our-university/corporate-information/policies-and-documents-a-z.

**Authorised by: University Information Governance Advisory Group**

## Version Record

| Version | Date | Author | Description |
|---|---|---|---|
| 0.5 | December 2021 | M. Bacon - Information Compliance Manager | Draft for comment and approval – update of 2018 DPIA form and process. |
| 1.0 | April 2022 | M. Bacon and includes IGAG comments. | Version 1.0 |
| 1.0 | April 2022 | Approved by IGAG | Version 1.0 |
| | | | |

UNIVERSITY OF
LEADING
THE WAY
WESTMINSTER

**Appendix One – DPIA Questionnaire and Template Form**

| | |
|---|---|
| DPIA author: | |
| | |
| Initiative title / IS&S Project ID: | |
| | |
| Date completed: | |

**Context**

| |
|---|
| Provide a brief explanation of the initiative - What is the initiative for? When is it likely to happen? How will it provide a benefit to the University? How will it provide a benefit to others? |

**Step One - Identify the need for a DPIA**

| Screening question | Yes/No |
|---|---|
| Does your initiative involve evaluating or scoring individuals (including profiling and predicting)? | |
| Does your initiative involve automated decision-making that may have a significant effect on an individual? | |
| Does your initiative involve systematic monitoring? | |
| Does your initiative involve the processing of sensitive personal data? | |
| Does your initiative involve processing personal data on a large scale? | |
| Does your initiative involve datasets that have been matched or combined? | |
| Does your initiative involve the personal data of vulnerable people? | |
| Does your initiative involve the use or application of innovative technological or organisational solutions? | |
| Does your initiative involve the transfer of personal data outside of the European Union? | |
| Does your initiative prevent individuals from exercising a right or using a service or contract? | |

Based on the above information, it has been decided that a full DPIA [is/is not] required.

UNIVERSITY OF
LEADING
THE WAY
WESTMINSTER

**Step Two – Describe the information flows in Text and Diagrams**

| |
|---|
| |

**Step Three – Identify and assess the privacy risks**

Please tab to add more rows to the table if needed.

| Risk ID | Privacy risk | Impact | Likelihood |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

**Step Four - Identify and approve controls**

Please tab to add more rows to the table if needed.

| Risk ID | Control(s) identified | Expected result | Approved by |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

**Step Five – Assign responsibility for implementing controls**

Please tab to add more rows to the table if needed.

| Risk ID | Control(s) | Responsible officer | Deadline for implementation | Completion date |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

**Step Six – Reassess and accept the risks**

Please tab to add more rows to the table if needed.

| Risk ID | Privacy risk | Impact after control | Likelihood after control | Risk accepted by |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

**Consultation**

The conduct of this Data Protection Impact Assessment has involved the following consultations:

E.g.
Business Sponsor and Information Asset Owner or their Representative -
Project Manager -
Data Management and Security –
Data Protection Officer – Malcolm Bacon

Senior Information Risk Officer – If Required

UNIVERSITY OF
LEADING
THE WAY
WESTMINSTER

**Contact for raising additional privacy concerns**

| | | | |
|---|---|---|---|
| Name: | | | |
| | | | |
| Job title: | | | |
| | | | |
| Email address: | | Telephone: | |

UNIVERSITY OF
LEADING
THE WAY
WESTMINSTER

**Appendix 2 – Article 30 Records of Processing**

| | Business Change Name |
|---|---|
| Data Controller or Joint Controllers | Contact details |
| Purpose of processing | |
| Categories of data subjects and personal data | |
| Categories of recipients of the data | |
| International transfers and safeguards | |
| Data retention and deletion policies | |
| A general description of the technical and organisational security measures applied. | |
| Privacy Statement | Use URL link or attach copy |

UNIVERSITY OF
LEADING
THE WAY
WESTMINSTER

## Appendix TWO – IS&S DPIA Process