University of Warwick - Data Protection Policy

Version 2 - 2019

This policy provides an overview of the following data protection topics and links to sources of further information:

University of Warwick’s Data Protection Statement

Legislation

Principles

Lawful basis for processing

Data subject rights

Accountability and Governance obligations

Privacy notices

Security

International Data Transfers

Personal Data Breaches

Changes to this policy

University of Warwick Data Protection Statement

The University of Warwick is committed to protecting the privacy rights of individuals who entrust the University with their personal data. This Data Protection Policy outlines the University’s commitment to transparency and accountability and promoting good information governance.

Legislation

Data Protection Legislation (GDPR and DPA 2018) governs how organisations (‘Data Controllers’) can use (‘Process’) information (‘Personal Data’) from which a living individual (‘Data Subjects’) can be identified. The Law applies to all organisations that process personal data but does not apply to ‘Anonymised’ data or data about a deceased individual. Data Protection Legislation is based around the concepts of principles, rights and accountability.

The General Data Protection Regulation (‘GDPR’) has direct effect in the UK from and including 25th May 2018, coupled with the new Data Protection Act 2018 (‘DPA 2018’). The DPA 2018 serves to assist with and supplement the adoption of the GDPR into UK law and once the UK leaves the EU, the DPA 2018 helps to ensure that the standards of the GDPR are enshrined in UK law.

Data Protection is regulated by the Information Commissioner’s Office (ICO) who are the supervisory authority for the UK and can be contacted at https://ico.org.uk/concerns/. The University’s
registration number is Z5856740 and further details of the Data Protection register entry can be found on the Information Commissioner’s public register.

Data Protection Act 2018
The DPA 2018 is the UK’s third generation of data protection law which was passed by Parliament on 21st May 2018, given Royal Assent on the 23rd May 2018 and came into effect on 25th May 2018. It seeks to empower individuals to take control of their personal data and to support organisations with their lawful processing of personal data. It addresses areas within the GDPR which are left to the discretion of the UK as well as areas outside the scope of the GDPR.

The General Data Protection Regulation
In 2016, the EU adopted the General Data Protection Regulation (GDPR) which replaced the 1995 Data Protection Directive. GDPR seeks to better protect individuals’ rights around privacy and personal data, in view of the rapid changes in technology that have occurred. GDPR has direct effect in the UK from and including 25th May 2018.

Principles
Under the GDPR there are six data protection principles. A data controller must comply with all six general principles when processing personal data:

1. **Lawfulness, fairness and transparency** - Personal data must be processed lawfully, fairly and in a transparent manner.

2. **Purpose limitation** - Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (with exceptions for public interest, scientific, historical or statistical purposes).

3. **Data minimisation** - Personal data must be adequate, relevant and limited to what is necessary in relation to purposes for which they are processed.

4. **Accuracy** - Personal data must be accurate and, where necessary, kept up to date. Inaccurate personal data should be corrected or deleted.

5. **Retention** - Personal data should be kept in an identifiable format for no longer than is necessary (with exceptions for public interest, scientific, historical or statistical purposes).

6. **Integrity and confidentiality** - Personal data must be kept securely.

Lawful basis for processing
Processing of Personal data
To legally process personal data at least one of the following conditions must be met:

1. **Consent** - The individual has given consent to the processing for one or more specific purposes. Consent will be much harder to obtain under the Regulation.

2. **Necessary for performance of a contract** - The processing is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual prior to entering into a contract.

3. **Legal obligation** - The processing is necessary for compliance with a legal obligation to which the data controller is subject. Only legal obligations under Union or Member State law will
satisfy this condition. However, that law need not be statutory (e.g. common law obligations are sufficient).

4. **Vital interests** - The processing is necessary in order to protect the vital interests of the individual or of another natural person. This is typically limited to processing needed for medical emergencies.

5. **Public functions** - The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Those functions must arise under Member State or EU law.

6. **Legitimate interests** - The 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. Controllers should undertake a legitimate interests assessment which involves a “careful assessment of” the underlying processing to ensure it properly balances the interest of the controller against any potential intrusion to the individual’s privacy. In particular, would the individual “reasonably expect” that processing for that purpose will take place.

**Processing of special categories of personal data**

GDPR places much stronger controls on the processing of special category data. Where sensitive personal data is processed, it must also satisfy at least one of the following special category personal data processing conditions:

1. **Explicit consent** - The individual has given explicit consent. However, Union or Member State law may limit the circumstances in which consent is available.

2. **Legal obligation related to employment** - The processing is necessary for a legal obligation in the field of employment and social security law or for a collective agreement.

3. **Vital interests** - The processing is necessary in order to protect the vital interests of the individual or of another natural person. This is typically limited to processing needed for medical emergencies.

4. **Not for profit bodies** - The processing is carried out in the course of the legitimate activities of a not-for-profit body and only relates to members or related persons and the personal data is not disclosed outside that body without consent.

5. **Public information** - The processing relates to personal data which is manifestly made public by the data subject.

6. **Legal claims** - The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

7. **Substantial public interest** - The processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law.

8. **Healthcare** - The processing is necessary for healthcare purposes and is subject to suitable safeguards.

9. **Public health** - The processing is necessary for public health purposes and is based on Union or Member State law.
10. **Archive** - The processing is necessary for archiving, scientific or historical research purposes, or statistical purposes and is based on Union or Member State law. Member States can introduce additional conditions in relation to health, genetic, or biometric data.

**Data subject rights**

The GDPR provides the following rights for individuals:

1. **The right to be informed** – Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement which is usually satisfied by the provision of a privacy notice (described in further detail below) at the point the personal data is collected by the University.

2. **The right of access** – Individuals have a right to access their personal data which is commonly referred to as a Subject Access Request. Please click here for further information on how to submit a subject access request.

3. **The right to rectification** – Individuals have a right to have inaccurate personal data rectified, or completed if it is incomplete. This right is closely linked to the accuracy principle. Please click here for further information on how to submit a rectification request.

4. **The right to erasure** – Individuals have a right to have personal data erased which is also known as the right to be forgotten. This right is not absolute and only applies in certain circumstances. Please click here for further information on how to submit an erasure request.

5. **The right to restrict processing** – Individuals have the right to request the restriction or suppression of their personal data. This right is not absolute and only applies in certain circumstances. Please click here for further information on how to submit a restriction request.

6. **The right to data portability** – Individuals have the right to obtain and reuse their personal data for their own purposes across different services. This right allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without it affecting usability. Please click here for further information on how to submit a data portability request.

7. **The right to object** – Individuals have the right to object to the processing of their personal data in certain circumstances, including an absolute right to stop their data being used for direct marketing. Please click here for further information on how to submit an objection request.

8. **Rights in relation to automated decision making and profiling** – Individuals have the right not to be subject to a decision based solely on automated decision-making using their personal data. Please click here for further information on what University processes involve automated decision making and how you can request human intervention or challenge a decision.

A response to all rights must be sent within one month, however as mentioned above most of the rights are qualified and specific exemptions may also apply.
Accountability and Governance Obligations

Accountability is a new explicit data protection principle under the GDPR which makes the University responsible for, and must be able to demonstrate, compliance with Data Protection Legislation. The University is proactive in its approach to data protection and achieves its accountability obligations by having in place a number of appropriate technical and organisational measures. Accountability is an ongoing obligation which must be regularly reviewed and helps the University show how it respects individual’s privacy.

Data Protection by design and default

Data Protection by design and default enables the University to comply with its obligations under Data Protection Legislation and document the decisions it makes. Integrating and documenting data protection consideration into everything the University does can be achieved by:

- Appointing a Data Protection Officer – see below for details.
- Implementing policies, procedures, processes and training to promote and embed data protection by design and default – see below.
- Using a Legitimate Interests Assessment – template and guidance coming soon.
- Conducting systematic Data Protection Impact Assessments (‘DPIAs’) on processing activities – template and guidance coming soon.
- Engaging with suppliers to complete an Information Security Assessment when work they are conducting on behalf of the University’s involves the processing of personal data.
- Having appropriate privacy provisions in written agreements in place when sharing personal data or engaging a data processor to conduct work on the University’s behalf which involves the processing of personal data.
- Maintaining a record of processing activities through an Information Asset Register – see below.
- Applying pseudonymisation techniques.

Data Protection Officer

Some organisations are required to appoint an independent Data Protection Officer (DPO). If you wish to make a complaint or have any queries or concerns about how the University has handled your personal data you can contact the University’s DPO via email or post:

Ms Anjeli Bajaj (DPO)
infocompliance@warwick.ac.uk
Data Protection Officer
Information and Data Compliance Team
University of Warwick
University House
Kirby Corner Road
CV4 8UW
Record of Processing Activities
There is a requirement to maintain documentation of the University’s processing activities which currently the University satisfies by registering with the Information Commissioner’s Office. The University registration number is Z5856740 and further details of the Data Protection register entry be found on the Information Commissioner’s website.

Staff Data Protection policy, guidance and training
The following staff policy and guidance are in place:

- Golden Rules for handling personal data
- Consent guidance and consent form
- GDPR Key Terms and key Personal data
- Information records management
- FAQs

Data Protection training for University staff is available via:

- Information Security Essentials Course
- GDPR e-learning module
- Data Protection Awareness Training
- Face to face training – run regularly throughout the year and on request.

Privacy notices
An important aspect of complying with data protection legislation is the requirement to process data fairly and lawfully. In order for the processing to be fair, the University must provide data subjects with accessible information to data subjects about how their personal data will be used. The most common way to do this is through a privacy notice. A privacy notice (also known as a ‘privacy statement’, ‘fair processing notice’ or ‘data collections notices’) is a term used to describe all the privacy information an organisation is obligated to make available to an individual when they are collecting personal data.

Links to the University’s core privacy notices can be found below:

- Student Privacy Notice
- Staff Privacy Notice

Security
A key principles under Data Protection Legislation is that organisations process personal data securely by means of ‘appropriate technical and organisational measures’. The University is required to ensure the confidentiality, integrity and availability of the systems and services it uses to process personal data. The University fulfils this requirement via the policies, procedures, guidance and training contained within its Information Security Framework.
## International Data Transfers

The GDPR imposes restrictions on the transfer of personal data outside the EEA. Currently the EEA countries are:

<table>
<thead>
<tr>
<th>Country</th>
<th>Country</th>
<th>Country</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>Belgium</td>
<td>Bulgaria</td>
<td>Czech Republic</td>
</tr>
<tr>
<td>Cyprus</td>
<td>Denmark</td>
<td>Estonia</td>
<td>Finland</td>
</tr>
<tr>
<td>France</td>
<td>Germany</td>
<td>Greece</td>
<td>Hungary</td>
</tr>
<tr>
<td>Iceland</td>
<td>Ireland</td>
<td>Italy</td>
<td>Latvia</td>
</tr>
<tr>
<td>Liechtenstein</td>
<td>Lithuania</td>
<td>Luxembourg</td>
<td>Malta</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Norway</td>
<td>Poland</td>
<td>Portugal</td>
</tr>
<tr>
<td>Romania</td>
<td>Slovakia</td>
<td>Slovenia</td>
<td>Spain</td>
</tr>
<tr>
<td>Sweden</td>
<td>UK</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Personal data may only be transferred outside the EEA in compliance with the following circumstances:

**Adequacy decision by the Commission**

Data transfers outside the EEA may be made where the European Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection. Currently, the following countries are considered as having adequate protection:

<table>
<thead>
<tr>
<th>Country</th>
<th>Country</th>
<th>Country</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Andorra</td>
<td>Argentina</td>
<td>Canada*</td>
<td>Faroe Islands</td>
</tr>
<tr>
<td>Guernsey</td>
<td>Israel</td>
<td>Isle of Man</td>
<td>Jersey</td>
</tr>
</tbody>
</table>
New Zealand       Switzerland       Uruguay       Japan

* (Commercial organisations only):

**Transfers subject to appropriate safeguards**
Organisations are able to transfer personal data where the organisation receiving the personal data has provided adequate safeguards including, but not limited to:

- binding corporate rules; or
- standard data protection clauses in the form of template transfer clauses adopted by the Commission.

**Derogations from the prohibition of transfers outside the EEA**
The GDPR provides derogations from the general prohibition on transfers of personal data outside the EU for certain specific situations.

The University’s DPO and Information and Data Compliance Team should be consulted before any International Data Transfers occur.

**Personal Data Breaches**
A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, authorised disclosure of, or access to, personal data. The University has procedures in place to contain, mitigate, manage and notify a personal data breach:

[Personal Data Breach Procedure](#) and [Breach Reporting Form](#) or email: [DPO@warwick.ac.uk](mailto:DPO@warwick.ac.uk)

**Changes to this Policy**
First published: 23 May 2018.
Next review date: November 2020 or change in legislation.

<table>
<thead>
<tr>
<th>Version control</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Version number</td>
<td>Date issued</td>
<td>Department</td>
<td>Updated information</td>
</tr>
<tr>
<td>V.01</td>
<td>23.05.2018</td>
<td>IDC</td>
<td>Updated in line with GDPR. Approved by Chair’s Action on behalf of Steering Committee.</td>
</tr>
<tr>
<td>V.02</td>
<td>18.11.2019</td>
<td>IDC</td>
<td>Minor updates approved by the Steering Committee.</td>
</tr>
</tbody>
</table>