DITSU Policy on Data Protection under the GDPR

Contents

Introduction to the GDPR

The General Data Protection Regulation is a Europe-wide directive, which will replace Ireland's Data Protection Acts 1988 and 2003, on the 25th May 2018. Whilst Ireland has always had a strong policy on Data protection, not all countries in the EU, or Non-EU Companies who operate within the EU have been as strict. The new legislation will now cover all European countries, and organisations which operate within the EU, to balance the protection of the individual's privacy rights with the rights of organisations and governments to collect and use data for business and administrative purposes.

Changes include enhanced rights to access information held on a data subject, increased responsibilities of Data Processors and Controllers, and the right of the data subject to their privacy, and to be forgotten.

Data subjects include all individuals from whom data is collected by DITSU - including, but not limited to students; staff members and any other individuals with whom DITSU has dealings.

Data Protection Principles

The six principles that the GDPR cover focus on the intent with which any data is accessed and used being lawful, fair and transparent, and that it is for specified explicit and legitimate purposes. It also focuses on data being adequate, relevant and limited to what's necessary in relation to the purpose of the data access. Consideration is given to how accurate the data that's being held is and how it's kept up-to-date, also that it's only held in a form where the data subject could be identified for no longer than necessary. Finally, it also looks for confirmation of appropriate technical or organisational measures being in place in an organisation to protect against unlawful or unauthorised processing, as well as accidental loss or destruction.

Data Protection Rule 1 - Lawfulness, Fairness and Transparency
Transparency: Tell the subject what data processing will be done.
Fair: What is processed must match up with how it has been described
Lawful: Processing must meet the tests described in GDPR [article 5, clause 1(a)]

Data Protection Rule 2 - Purpose Limitations
Personal data can only be obtained for "specified, explicit and legitimate purposes" [article 5, clause 1(b)]. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.

Data Protection Rule 3 - Data Minimisation
Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". [article 5, clause 1(c)]. i.e. No more than the minimum amount of data should be kept for specific processing.

Data Protection Rule 4 - Accuracy
Data must be "accurate and where necessary kept up to date" [article 5, clause 1(d)]. Baselining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data.

Data Protection Rule 5 - Storage Limitations
Regulator expects personal data is “kept in a form which permits identification of data subjects for no longer than necessary”. [article 5, clause 1(e)] i.e. Data no longer required should be removed.

Data Protection Rule 6 - Integrity and Confidentiality
Requires processors to handle data “in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage”. [article 5, clause 1(f)]

What DITSU Needs to be Doing

Consent
Where data processing is based on consent (i.e. a signed form to with information to be added to a database), DITSU must be able to show that consent was given by the data subject.

If a data subject’s consent is given as part of a written document, the request for consent must be presented clearly and separately from any other matters, using plain language. Any part of such a document that conflicts with the GDPR will not be enforceable.

A data subject will have the right to withdraw their consent at any time. Before giving consent, the data subject must be informed of their right to withdraw their consent and it must be as easy to withdraw consent as to give it.

Collection of Data
Under the GDPR, when personal data is collected from data subjects, DITSU should provide the following information:

- Identity and contact details of DITSU
- Contact details for the data protection officer
- Purpose of the intended processing and its legal basis
- If the legal basis is a “legitimate interest” of DITSU, what that interest is
- The intended recipients of the data
- Any intention to transfer the data outside the EU and if so, data safeguards in that country
- The period for which the data will be stored or the basis for determining that period
- The data subjects right to request access, rectification, erasure, restriction of use, objection of use and data portability
- The data subjects right to lodge a complaint to a supervisory authority
- Whether DITSU must provide data as part of a statutory or contractual requirement and the consequences of not providing the data
- The existence and logic of any automated decision making or profiling processes

If DITSU intends to process data for a purpose other than the purpose for which it was collected, the controller must provide the data subject with information about this purpose before processing begins.

Right of Access
Data subjects have the right to see a copy of any personal data held by DITSU about them, and they can request this information free of charge. DITSU must respond to them within one month, but this can be extended for a further two months if the information sought is of a complex nature

They are entitled to the following information:

- The purposes of the processing
- The categories of data being held
- The identity of any recipients who may see this data
- The period for which it will be stored
- The right to lodge a complaint with a supervisory authority
- Where the information was not collected directly from them, information about the source
- The use of any automated decision-making processing and information about that process
- If data is being transferred to a country outside the EU, the data safeguards in that country

Right of Rectification, Restriction and Erasure
Data subjects have the right to request that DITSU rectifies inaccurate or incomplete personal data held on them.

Data subjects have a right to restrict DITSU from processing their personal data where:

- The accuracy of the data is in question
- The processing of the data is unlawful
- DITSU no longer needs the data for the purpose, but it is required by the data subject for other reasons
- Data subjects have challenged the legal basis for the processing

Once processing has been restricted, DITSU must inform the data subject before that restriction is lifted. The data subject can request DITSU to erase their data, and DITSU has an obligation to erase that data if one of the following applies:

- The data is no longer necessary for the purpose it was collected
- The data subject has withdrawn consent to the processing of their data
- The data subject objects to the processing of their data
- There is no lawful basis for the processing
- The data must be erased to comply with law
- The data was collected in relation to the offer of online services

The right of erasure also includes the right to have publicly available personal data erased or as far as technologically possible, removed from public availability. The GDPR also gives legislative effect to the ‘right to be forgotten’ procedure. Right to be forgotten is a right to have search engine results that relate to a person, or a certain incident, removed from internet search listings once that information is no longer relevant. For example, if an online search for your name turned up a link to a photograph of a person that they believe is no longer relevant for the purpose for which it was collected, they can request that the search engine remove that link from their search results. The right to be forgotten is not an absolute right and requests under the procedure are assessed on a case-by-case basis.

The right of erasure will not apply where processing is necessary because of an overriding freedom of expression, legal or public interest.

Right to Data Portability
Data subjects can request and receive personal data that they have previously provided to DITSU in a commonly used and machine-readable format. The right also means they can request DITSU to transfer their personal data to another controller.

Right to Object and Automated Decision Making
Data subjects have the right to object to the processing of their data at any time, for example to prevent your data being used for marketing purposes, including profiling.

DITSU must stop processing their data unless DITSU can show there are legitimate grounds or legal reasons for such processing that overrides the data subject's interests. Where a decision is to be made about a data subject that will have significant legal effects, they have the right to avoid any automated decision-making processing - DITSU must provide human intervention in the decision-making process if requested.

Privacy Notices
DITSU must have appropriate measures to comply with data subject's rights, and must provide information in a concise, transparent, intelligible and easily accessible form, using clear and plain language. If DITSU does not comply with a request from the data subject, DITSU must give reasons why, and let the data subject know that they have the right to make a complaint to the supervisory authority. These rights will not apply where the data can no longer identify the data subject.

Security of Personal Data
DITSU has an obligation to keep personal data secure. Under the GDPR, DITSU must consider implementing modern security measures appropriate for the risks involved in our activities. For example, risks may come from accidental or unlawful destruction of stored data, or unauthorised disclosure, access or alteration. The security measures may include anonymisation or encryption of data and restoring or backing up stored data. DITSU will need to review and evaluate these security measures to comply with any code of conduct that may be published in the future.

Data Breach Reporting
DITSU must notify the supervisory authority of a personal data breach without delay where that breach is a likely to result in a risk to the rights and freedoms of the data subject. Notification should be made within 72 hours of DITSU becoming aware of the breach. Data processors will be required to notify DITSU if the processor becomes aware of a breach. DITSU should also notify the data subject without delay.