GDPR

Policy & Procedure

Zoe Bird

TABLE OF CONTENTS

GDPR OVERVIEW

The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

No personal data may be processed unless it is done under a lawful basis specified by the regulation, or if the data controller or processor has received explicit, opt-in consent from the data's owner. The business must allow this permission to be withdrawn at any time.

The regulation gives individuals 8 Rights defined as:

1. *The right to be informed – all organisations must be completely transparent in how they are using personal data (personal data may include data such as a work email and work mobile if they are specific to an individual).*
2. *The right of access - individuals will have the right to know exactly what information is held about them and how it is processed.*
3. *The right of rectification - individuals will be entitled to have personal data rectified if it is inaccurate or incomplete.*
4. *The right to erasure - also known as 'the right to be forgotten', this refers to an individual's right to having their personal data deleted or removed without the need for a specific reason as to why they wish to discontinue.*
5. *The right to restrict processing - an individual's right to block or suppress processing of their personal data.*
6. *The right to data portability - this allows individuals to retain and reuse their personal data for their own purpose.*
7. *The right to object - in certain circumstances, individuals are entitled to object to their personal data being used. This includes, if a company uses personal data for the purpose of direct marketing, scientific and historical research, or for the performance of a task in the public interest.*
8. *Rights of automated decision making and profiling - the GDPR has put in place safeguards to protect individuals against the risk that a potentially damaging decision is made without human intervention. For example, individuals can choose not to be the subject of a decision where the consequence has a legal bearing on them, or is based on automated processing.*

Personal Data is defined as

> *an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location number, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

GDPR FOR LSP

As a business we collect various levels of personal information

- *Staff Records (Including but not limited to Training Records, Sick Records, Personal Development Records, Pay Details, Contract Details)*
- *Customer Data (including but not limited to Incidents within the O2 Academy)*
- *Supplier Information (including but not limited to Self-Employment Status, Bank Details)*
- *Market Research Information (including but not limited to Spending Habits, website usage)*

Some of this data we have a legal requirement to collect and by entering into a contract with us the Data Subject has provided consent. There are also statutory limits for how long we have to hold this data for. Other data we must gain consent from the data subject before collecting and we must ensure we have a process for accepting requests from data subjects to change their marketing preferences.

DATA COLLECTION

Before collecting data from a 'Data Subject' you must be able to answer 'Yes' to at least one of the following statements:

1. *Personal Data is collected in the Vital Interest of the Individual (unlikely to apply to LSP)*
2. *Personal Data is collected is in the Public Interest (Potentially within the O2 Academy)*
3. *Personal Data is collected as it is necessary to implement a contract (Applies to Staff and Suppliers)*
4. *Personal Data is collected for a legal obligation (Applies to Staff, Suppliers and O2 Academy)*
5. *The Individual has provided Opt In Consent (Marketing)*
6. *LSP has a legitimate interest in the data (Marketing but a little harder to prove)*

If you have a right to collect Data based on one of the statements above you must ensure that the data you collect is

- *Appropriate for the purpose of collecting it*
- *Not excessive (Don't collect unnecessary data as it'll be nice to have in the future)*

When collecting data you must advise the 'data subject' of the following

- Why you are processing the data
- What is the legal basis for processing the data
- Who you are sharing the data with
- If the data will be shared outside the EEA
- How long you will keep the data
- What are the individual's rights
- Contact Details of the Companies Data Controller and Data Protection Officer
- How to complain to the Information Commissioner's Office

STORING DATA

Once we have collected data we must ensure that Data is stored securely and not shared without having gained consent.

Electronic Documents

- *All documents should be stored on the X Drive*
- *Include a Destruction Date in the file/folder name (See Retention Schedule)*
- *If emailing externally to the leicester.ac.uk network you should password protect the file (Only share if you have consent)*
- *If you plan on taking personal data off site, consider if there is an alternative, if no alternative only transport on an encrypted device, delete from the device as soon possible after using*
- *If you access work materials from a phone avoid opening confidential files, if you do open a confidential file then delete from Your files after using*
- *When working on files including personal data redact (anonymize) data when you no longer need information on the individuals only an overview position.*

Paper Records

- *Scan files where possible and store as electronic files following procedures for electronic documents, securely shred after storing electronically*

- *Paper records should be stored within a locked drawer/cupboard, destruction dates should be recorded (See Retention Schedule)*
- *Personal Data should only be posted where absolutely necessary, if posted should be clearly labeled Private & Confidential and the Envelope Secured*
- *Data required by the HR team should be hand delivered to the Payments Team on Campus where it will be collected and delivered by Hand by a University Member of Staff*
- *When working on files including personal data redact (anonymize) data when you no longer need information on the individuals only an overview position.*
-

Emails

- *Emails that contain an attachment with personal data should have the attachment stored on the x Drive and the attachment removed from the Email (Do not Forget Sent Boxes)*
- *Emails that contain direct content with personal data should be stored directly on the X Drive. The email should then be flagged for deletion within 1 year of receipt (The original will remain on the X Drive in line with the Retention Schedule)*

DATA RENTENTION SCHEDULE

Data Stored	Destructions Cycle
Board Minutes/Company Articles	Keep Indefinitely
Governance Polices	Superseded + 10 Years
Company Strategy	Keep Indefinitely
Statutory Access Requests	Last Action + 3 Years
Data Request from Police regarding Staff/Student	Greater off Last Action + 6 Years Or Individual Leaves the University
Data Requests from police	Last Action + 3 Years
Financial Regulations	Financial Year Created + 6 Years
Financial Forecasts/Budgets	Financial Year Created + 2 Years
Audited Financial Accounts	Financial Year Created + 6 Years
Pension Schemes	Termination of Employment + 75 Years
Purchasing (Purchase Order/Authorisation/Goods Receipt)	Financial Year Created + 6 Years
Payroll Data	Financial Year Created + 6 Years
Management Accounts	Financial Year Created + 2 Years
Purchasing Regulations	Keep Indefinitely
Successful Tender Documents	Contract Completion + 6 Years
Unsuccessful Tender Documents	Financial Year Created + 2 Years
Purchasing Terms & Conditions	Keep Indefinitely

Employment Terms and Conditions	Keep Indefinitely
Personnel Records	Termination of Employment + 6 Years
Recruitment	Vacancy Filled + 8 Months
CCTV Recording	Created + 30 Days
O2 Banning List	Completion of Studies
O2 Entry Register	Entry Time + 30 Days
Incident Logs	Created + 2 Years
Fire Inspection Logs	Created + 31 days
Lost Property Logs	Created + 2 Years
Security Breaches or incidents, including theft reports	Last Action + 4 Years

ACCESS REQUESTS

'Data Subjects' are allowed to request any data we hold on them, these requests can be made in writing or verbally. No Charge can be made for these requests unless they become excessive requests, then we can charge for the administration to prepare the request. All requests should be responded to within 1 month of receipt.

The process of dealing with this request will be as follows:

1. *The request will be received from the Data Subject*
2. *The request will be forwarded to the Director of Business Analysis (BA) to co-ordinate*
3. *The BA will confirm the identification of the individual making the request*
4. *The BA will record the request and all relevant information the on the Data Access Request Log*
5. *The BA will request information from all managers/leaders/University Teams within the Partnership*
6. *Managers/Leaders should provide paper copies of all data held within 15 days of being requested. If you hold no data on the data subject this should also be documented*
7. *The BA will organize and prepare the data and liaise with the Data Subject to release the information held. Some Data will be redacted before release.*
8. *The BA will provide the Data subject with a summary of data held, why it is held, what it is used for, when it will be destroyed and copies of all the data held.*

DELETION REQUESTS

'Data Subjects' have a right to be deleted where we do not have a statutory reason to retain the data and where the Data Subject is removing consent

The process of dealing with a 'Right to Be Forgotten' request is:

1. *The request will be received from the Data Subject*
2. *The request will be forwarded to the Director of Business Analysis (BA) to co-ordinate*
3. *The BA will confirm the identification of the individual making the request*
4. *The BA will request information from all managers/leaders/University Teams within the Partnership*
5. *Managers/Leaders should provide a summary of all data held within 10 days of being requested. If you hold no data on the data subject this should also be documented*
6. *The BA will review the data held and determine if this is data than can be deleted/redacted or if statutory regulations apply.*
7. *The BA will work with the manager/leader/ University team to ensure the safe destruction/redaction of data (where required)*
8. *If not all data can be deleted/redacted the BA will liaise with the Data Subject to confirm remaining Data held what it is used for and when it will be destroyed.*

DATA REVIEWS

Staff should review their areas continually as part of working practice and delete/redact data when relevant according to the Retention schedule.

The Director of Business Analysis will co-ordinate a yearly review in August of all files, emails and paper records to ensure they are compliant.

The Director of Business Analysis will review all policies and procedures in August

DATA BREACH

If the Partnership becomes aware of a data breach we must report this to the ICO within 72 hours. For more serious breaches we would also need to contact the individuals without undue delay.

Examples of Data Breaches are:

- *access by an unauthorised third party;*
- *deliberate or accidental action (or inaction) by a controller or processor;*
- *sending personal data to an incorrect recipient;*
- *computing devices containing personal data being lost or stolen;*
- *alteration of personal data without permission; and*
- *Loss of availability of personal data.*

If you suspect a data breach

1. *If you suspect a data breach has happened this should be reported to the Director of Business Analysis (BA)*
2. *The BA will assess and document the scale and scope of the breach*
3. *The BA will report to the CEO/Board on the breach and a recommendation on reporting and disclosure.*
4. *The BA will work with the CEO/Board and where necessary the University of Leicester to make any necessary reporting requirements*
5. *The BA will work with the CEO/Board and where necessary the University of Leicester to make any necessary operational changes to process/storage to prevent further data breaches.*

DEFINITIONS

Consent

When requesting consent it should meet all of the following:

- *Be easy to understand, concise, and specific.*
- *Explain what data are you collecting, why you want it, how long will you keep it.*
- *Include the name of your organization and any third parties.*
- *Remind data subjects that they can withdraw consent at any time.*
- *Be kept under periodic reviews.*

Data Controller

means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Personal Data

means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Processor

Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;