Data Protection Training

DATA GOVERNANCE TEAM
UNIVERSITY OF SUFFOLK

University
of Suffolk

This training aims to provide staff with a clear understanding of the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 when handling applicant data.

It is critical to ensure that applicant data is managed securely and in compliance with UK law.

Learning Objectives

By the end of this training, you will:

- Understand what is considered personal data and sensitive personal data.

- Learn the six lawful bases for processing personal data under UK GDPR.

- Understand your responsibilities when collecting, storing, and transferring applicant data.

- Learn how to comply with the rights of individuals, such as the right to access and deletion by sharing requests with the University of Suffolk.

- Recognise the importance of data security and measures to prevent data breaches.

Section 1: Understanding Key Terminology

What is Personal Data?

Personal data is any information relating to an identified or identifiable individual. Examples include:

- Name
- Passport number
- Email address
- Location data

Special Categories of Personal Data

Sensitive personal data (or special category data) includes information that could reveal an individual’s:

- Racial or ethnic origin
- Health data
- Religious beliefs
- Sexual orientation

Extra care must be taken when handling these types of data, and it often requires explicit consent to process.

Section 1: Understanding Key Terminology

Special Categories of Personal Data

Sensitive personal data (or special category data) includes information that could reveal an individual's:

- Racial or ethnic origin
- Health data
- Religious beliefs
- Sexual orientation

Extra care must be taken when handling these types of data, and it often requires explicit consent to process.

Data Subject

The applicant whose personal data is being processed is referred to as the data subject.

Data Controller and Data Processor

- Data Controller: The University of Suffolk determines the purposes and means of processing personal data.
- Data Processor: Staff at your organisation, processing data on behalf of the University.

Section 2: Lawful Basis for Processing Personal Data

Under the UK GDPR, personal data can only be processed if there is a lawful basis for doing so. The six lawful bases are:

1. Consent: The individual has given clear consent for their data to be processed.

2. Contract: Processing is necessary for a contract with the individual, e.g., processing applications.

3. Legal Obligation: Processing is necessary to comply with the law, such as visa requirements.

4. Vital Interests: Processing is necessary to protect someone's life.

5. Public Task: Processing is necessary for official functions, typically by public authorities.

6. Legitimate Interests: Processing is necessary for the legitimate interests of the University or for your organisation, except where these interests are overridden by the individual's rights.

For recruitment purposes, consent and contract are typically the most relevant lawful bases.

Section 3: Data Protection Principles

The UK GDPR outlines seven key principles for handling personal data:

1. Lawfulness, Fairness, and Transparency: Process data lawfully and in a transparent manner.

2. Purpose Limitation: Collect data for a specified purpose and only use it for that purpose.

3. Data Minimisation: Collect only the data that is necessary.

4. Accuracy: Keep personal data accurate and up to date.

5. Storage Limitation: Only keep personal data as long as necessary.

6. Integrity and Confidentiality: Ensure personal data is secure and protected against unauthorised access or breaches.

7. Accountability: Be able to demonstrate compliance with GDPR principles.

Section 4: Individual Rights Under UK GDPR

Applicants, as data subjects, have specific rights under UK GDPR:

1. Right to Access: Applicants can request access to their personal data.
2. Right to Rectification: They can ask for their data to be corrected if inaccurate.
3. Right to Erasure ("Right to be Forgotten"): In certain circumstances, applicants can request their data be deleted.
4. Right to Restrict Processing: They can request the limitation of how their data is processed.
5. Right to Data Portability: They can request their data be transferred to another service provider.
6. Right to Object: They can object to data processing in some circumstances, such as direct marketing.

Agents must ensure that they respect these rights and communicate any such requests to the University of Suffolk promptly.

Section 5: Data Security and Breaches

Security Measures

Data security is critical to prevent breaches. Best practices include:

- Encryption: Use encryption to secure data during transmission, especially when sharing data electronically.

- Password Protection: Ensure strong passwords are used for access to applicant data.

- Physical Security: Store physical documents containing personal data in secure, locked environments.

- Access Control: Limit access to personal data to only those who need it for their role.

- Double Check: Check details carefully before adding personal data to an applicant's record or sending an email containing personal data, to ensure that the information is correct and secure. Work to a principle of "check twice, send once".

Section 5: Data Security and Breaches

Data Breaches

A data breach occurs when there is unauthorised access, loss, or exposure of personal data. If a breach occurs:

- Report **immediately** to the University of Suffolk International team or to the Data Governance team on datagovernance@uos.ac.uk

- Quickly identify and secure affected data to prevent further unauthorised access or data loss.

Failure to report breaches can lead to significant fines under UK GDPR so it is important that this is reported to the University of Suffolk immediately.

Section 6: Practical Steps for Compliance

1. Limit Data Collection: Only collect the data necessary.

3. Secure Data: Ensure data is encrypted and stored securely.

4. Data Sharing: Share data only with authorised personnel and ensure that the University is aware of any third-party sharing.

5. Respond to Data Requests: If an applicant requests access to or deletion of their data, pass these requests to the University immediately.

Quiz: Test Your Knowledge

Question 1: What is considered personal data under UK GDPR?

a) Name

b) Email address

c) Racial or ethnic origin

d) All of the above

Question 1: What is considered personal data under UK GDPR?

a) Name

b) Email address

c) Racial or ethnic origin

d) All of the above

Question 2: How should sensitive data like health or ethnicity be handled?

a) With extra care (e.g. explicit consent)

b) No special handling needed

c) Use only for marketing purposes

d) Shared freely if relevant

Question 2: How should sensitive data like health or ethnicity be handled?

a) With extra care (e.g. explicit consent)

b) No special handling needed

c) Use only for marketing purposes

d) Shared freely if relevant

Question 3: What should you do if you suspect a data breach has occurred?

a) Ignore it

b) Inform the data subject directly

c) Report it immediately to the University

d) Fix the issue and move on

Question 3: What should you do if you suspect a data breach has occurred?

a) Ignore it

b) Inform the data subject directly

c) Report it immediately to the University

d) Fix the issue and move on

Question 4: Which of the below scenarios would be classed as a high-risk personal data breach? (Select all that apply)

a) Computing devices containing personal data being lost or stolen

b) Alteration of personal data without permission

c) Access by an unauthorised third party

d) Sharing your organisation's telephone number with an applicant

e) Sharing one file containing highly sensitive special category personal data

Question 4: Which of the below scenarios would be classed as a high-risk personal data breach? (Select all that apply)

a) Computing devices containing personal data being lost or stolen

b) Alteration of personal data without permission

c) Access by an unauthorised third party

d) Sharing your organisation's telephone number with an applicant

e) Sharing one file containing highly sensitive special category personal data

Question 5: What are the potential consequences of a UK GDPR Breach?

a) Fines related to data breaches

b) Litigation relating to data breaches

c) Reputational damage

d) All of the above

Question 5: What are the potential consequences of a UK GDPR Breach?

a) Fines related to data breaches

b) Litigation relating to data breaches

c) Reputational damage

d) All of the above