The SUT 2024 GDPR Checklist

If you’re going to collect data about people, you have a responsibility under the GDPR to collect and process it lawfully.

# Contents of the Checklist

[Special Category Data 1](#_Toc167873511)

[How to collect and Process Data 3](#_Toc167873512)

[The DPIA 4](#_Toc167873513)

# Special Category Data

You must have special consideration for any attempt to capture information (or cause information to be linked to a person whether accurate or not) where the data is about:

## 1. Racial or Ethnic Origin

* Information revealing an individual's race or ethnicity.

## 2. Political Opinions

* Data regarding an individual’s political beliefs or affiliations.

## 3. Religious or Philosophical Beliefs

* Information about a person’s religious beliefs or their lack of beliefs.
* Includes data related to philosophical beliefs.

## 4. Trade Union Membership

* Information indicating whether an individual is a member of a trade union.

## 5. Genetic Data

* Personal data relating to inherited or acquired genetic characteristics, which give unique information about an individual’s physiology or health.

## 6. Biometric Data

* Data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a person, used for the purpose of uniquely identifying an individual (e.g., fingerprints, facial recognition).

## 7. Health Data

* Information related to the physical or mental health of an individual, including data on health services received, which reveals information about their health status.

## 8. Sexual Orientation

* Information about an individual's sexual orientation or sexual life.

## 9. Data Concerning a Natural Person’s Sex Life

* Information about a person’s sex life or sexual behaviour.

## Processing Conditions for Special Category Data

Under GDPR, processing of special category data is generally prohibited unless one of the following conditions applies: (I’ve greyed out the ones you’re not going to rely upon)

* Explicit Consent: The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.
* Employment, Social Security, and Social Protection Law: Processing is necessary for carrying out obligations and exercising specific rights in the field of employment, social security, and social protection law.
* Vital Interests: Processing is necessary to protect the vital interests of the data subject or another natural person, where the data subject is physically or legally incapable of giving consent.
* Non-Profit Bodies: Processing is carried out in the course of legitimate activities by a foundation, association, or any other not-for-profit body with a political, philosophical, religious, or trade union aim.
* Publicly Available Data: Processing relates to personal data which are manifestly made public by the data subject.
* Legal Claims: Processing is necessary for the establishment, exercise, or defense of legal claims or whenever courts are acting in their judicial capacity.
* Substantial Public Interest: Processing is necessary for reasons of substantial public interest, based on Union or Member State law.
* Healthcare and Social Care: Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care, or treatment or the management of health or social care systems and services.
* Public Health: Processing is necessary for reasons of public interest in the area of public health.
* Archiving, Research, and Statistics: Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

Understanding and properly handling special category data is crucial for GDPR compliance and for protecting the rights and privacy of individuals.

# How to collect and Process Data

## 1. Conduct a Data Audit

* Identify Data Held: Map out what personal data is collected, where it is stored, and how it is processed.
* Assess Data Necessity: Ensure that only necessary data is collected and stored, and delete any data that is no longer needed.

## 2. Obtain Clear Consent (Usually)

* Explicit Consent: Ensure that all members give explicit consent for their data to be used, with clear opt-in mechanisms.
* Transparent Information: Provide clear information about how data will be used at the point of collection.

## 3. Update Privacy Policies

* Clear Policies: Update privacy policies to be clear and concise, explaining how personal data is used, stored, and shared.
* Regular Reviews: Regularly review and update privacy policies to reflect any changes in data processing activities.

## 4. Secure Data Storage

* Encryption: Use encryption for sensitive data, both in transit and at rest.
* Access Controls: Implement strong access controls to ensure that only authorized personnel can access personal data.

## 5. Train Staff

* Regular Training: Provide regular GDPR training to all staff members, ensuring they understand data protection principles and their responsibilities.
* Awareness Programs: Run awareness campaigns to keep GDPR compliance at the forefront of employees' minds.

## 6. Implement Data Minimization

* Limit Data Collection: Collect only the data that is necessary for the purpose for which it is being processed.
* Anonymization: Where possible, anonymize data to reduce the risk associated with storing personal information.

## 7. Ensure Data Accuracy

* Regular Updates: Regularly review and update personal data to ensure it is accurate and up-to-date.
* Member Access: Allow members to access and update their personal information easily.

## 8. Prepare for Data Breaches

* Breach Response Plan: Develop and implement a data breach response plan to quickly address and mitigate any breaches.
* Notification Procedures: Establish procedures for notifying affected individuals and the relevant authorities in the event of a breach, where necessary.

## 9. Use Data Protection Impact Assessments (DPIAs) if necessary

* Assess Risks: Conduct DPIAs for any new processing activities or significant changes to existing activities to identify and mitigate risks.
* Document Findings: Document the findings of DPIAs and the measures taken to address any identified risks.

## 10. Maintain Records of Processing Activities

* Documentation: Keep detailed records of all data processing activities, including purposes, data categories, and retention periods.
* Transparency: Be prepared to provide this documentation to regulatory authorities if requested.

By implementing these straightforward measures, a Students’ Union can significantly reduce its risk under GDPR and ensure better protection of personal data.

# The DPIA

A Data Protection Impact Assessment (DPIA) is a process designed to help organizations identify and minimize the data protection risks of a project or processing activity. It is a key part of GDPR compliance and is required for processing activities that are *likely to result in a high risk to the rights and freedoms of individuals*.

I recommend treating any **major** data collection in an SU as requiring a DPIA, although it’s not strictly necessary. Most of the activities of an SU are not going to result in a high risk to the rights and freedoms of a person – but we have a responsibility to get it right, and these skills are not going to go away.

## Key Components of a DPIA

### Description of Processing Activities:

* + Nature: What type of data will be processed?
	+ Scope: What is the extent of the data processing (e.g., volume of data, duration of processing)?
	+ Context: Under what circumstances is the data being processed?
	+ Purposes: Why is the data being processed? What are the intended outcomes?

### Assessment of Necessity and Proportionality:

* + Ensure that the data processing is necessary and proportionate to achieve the intended purpose.

### Risk Assessment:

* + Identify Risks: Determine the potential risks to data subjects' rights and freedoms.
	+ Evaluate Risks: Assess the severity and likelihood of these risks.

### Mitigation Measures:

* + Identify measures to mitigate identified risks.
	+ Ensure these measures are implemented effectively to protect personal data.

### Consultation with Stakeholders:

* + Consult with relevant stakeholders, including data subjects, to gather input on the processing activity and potential risks.

### Documentation and Reporting:

* + Document the entire DPIA process, including the findings, decisions made, and actions taken to mitigate risks.
	+ Maintain records of the DPIA for accountability and transparency.

## When is a DPIA Required?

A DPIA is required in situations where data processing is likely to result in a high risk to individuals, such as:

* Systematic and extensive profiling: Automated processing, including profiling, that has significant effects on individuals.
* Large-scale processing of sensitive data: Processing large volumes of special category data (e.g., health, racial or ethnic origin, political opinions).
* Public monitoring: Systematic monitoring of a publicly accessible area (e.g., CCTV in public spaces).

## Benefits of Conducting a DPIA

* Risk Reduction: Helps to identify and mitigate data protection risks.
* Compliance: Demonstrates compliance with GDPR and other data protection regulations.
* Transparency: Builds trust with data subjects by showing a commitment to protecting their data.
* Decision Support: Provides a structured process for making informed decisions about data processing activities.

## Steps to Conduct a DPIA

### Preliminary Assessment:

* + Determine if a DPIA is necessary based on the nature of the processing activities.

### Data Mapping:

* + Map out data flows and processing activities to understand what data is being processed and how.

### Risk Analysis:

* + Identify potential risks to data subjects' privacy and data protection.

### Consultation:

* + Engage with stakeholders, including data subjects, data protection officers, and relevant authorities if necessary.

### Implementation of Measures:

* + Identify and implement measures to mitigate identified risks.

### Review and Approval:

* + Review the DPIA findings and obtain approval from senior management or the data protection officer.

### Documentation:

* + Document all aspects of the DPIA process and keep records for accountability.

### Monitor and Review:

* + Regularly monitor the processing activities and review the DPIA to ensure ongoing compliance and risk mitigation.

By conducting DPIAs, organizations can proactively address privacy risks, comply with legal requirements, and enhance the trust of their members and other stakeholders.

# Sample Consent Statement

### Survey Consent

Ballybreag Students’ Union will process the data provided by you for the purposes of determining student demands for services at Ballybreag SU. With your explicit consent, we will also enter you into a prize draw to win XXXXX.

**Data Usage:**

The data collected will be used solely for the purpose of understanding student demands and entering you into the prize draw, if you consent to this.

Reports generated from the data will not contain any personally identifying information and will be retained for a period of [specify period, e.g., "one year after the completion of the report"].

**Right to Withdraw:**

You may withdraw your participation at any time during the survey. If you do not complete the survey, you will not be entered into the prize draw and none of the data you provide will be used in the study.

If you wish to withdraw your consent after completing the survey, please contact [contact information]. Upon withdrawal, your data will be deleted and not used further.

**Data Retention and Destruction:**

We will retain the collected data until 25th June 2024, after which it will be securely destroyed and will no longer be retrievable or processed.

**Consent:** Please indicate your consent to the following:

I consent to the use of my data for determining student demands for services at Ballybreag SU.

I consent to being entered into the prize draw.