GDPR readiness compliance checklist

GDPR comes into force in May 2018. This checklist is designed to help you assist the University in getting ready for GDPR.

To begin, you will need to identify whether you are collecting and processing personal data. This checklist is to be read in conjunction with the compliance checklist guidance notes available on the GDPR intranet site: https://intranet.soton.ac.uk/sites/gdpr/Pages/Implementing-GDPR.aspx

1. Is it personal data?

☐ Does it identify a living person?

☐ Is it capable of identifying a living person if you, or someone else, combine it with other personal data you hold?

2. Is information you are collecting sensitive personal data? Is it about a person's:

☐ Racial or ethnic origin?

☐ Political opinions?

☐ Religious or philosophical beliefs?

☐ Trade Union membership?

☐ Genetic or Biometric Data?

☐ Health?

☐ Sex life or sexual orientation?

Or is it about a person's:

☐ Criminal convictions or criminal proceedings?

3. If you are collecting and processing personal data what is the legal basis that allows you to do that? Is it

☐ Necessary for compliance with a legal obligation to which the University is subject?

☐ Necessary for the performance of a contract to which the data subject is a party?

☐ Necessary to protect the individual's vital interest?

☐ Necessary for the performance of a task carried out in the public interest or in the exercise of some vested official authority?

☐ With the data subject’s consent? If so, is the consent:

☐ Unambiguous, specific, informed and freely given?

☐ Obtained for each processing activity?

☐ Adequate, relevant and limited to what is necessary for purpose?

☐ Where data is collected from children, is parental consent required (under 13)?

A template consent form is available on the intranet site: https://intranet.soton.ac.uk/sites/gdpr/Pages/Implementing-GDPR.aspx

4. If you are collecting and processing sensitive personal data, what is the legal basis that allows you to do that? Is it:

☐ With the data subject’s explicit consent?

☐ Necessary for carrying out obligations under employment or a collective agreement?

☐ Necessary to protect the individual’s vital interest?

☐ Personal data manifestly made public by the individual?

☐ Necessary for the establishment, exercise or defence of a legal claim?

☐ Necessary for reasons of substantial public interest under UK law?

☐ Necessary for purposes of medical treatment, assessing the working capacity of the employee, the provision of health or social care or a contract with a health professional?

☐ Necessary for reasons of public interest in the area of public health?

☐ Necessary for archiving purposes in the public interest or scientific and historical research or statistical purposes?

5. Is a Data Protection Impact Assessment (DPIA) required (high risk processing)? Assess whether it is:

☐ A system or process that analyses a person’s financial situation, location, health, personal preferences, reliability or behaviour.

☐ A research project or trial that may have a high risk impact on the data subject’s personal data?

☐ Video surveillance systems.

☐ Data in large scale filing systems on children, genetic or biometric data.

If there is any possibility that a proposed new system, process, clinical trial or research project may have a high risk impact on a data subject's personal data you must consult with the University's Data Protection Officer first.

6. Privacy notice

☐ Have you completed a privacy notice informing the data subject of your reasons for collection and their rights at the same time you have collected the information?

A template privacy notice is available on the intranet site: https://intranet.soton.ac.uk/sites/gdpr/Pages/Implementing-GDPR.aspx

7. Data storage.

Check where you are storing your data:

☐ Is it being stored in a way that is secure and that stops any unauthorised access e.g. a secure system that is password protected, locked cabinet storage etc?

☐ Is it being stored externally by third parties?

If so, have you checked:

☐ That the third parties are GDPR compliant?

☐ That the University has appropriate data sharing and non-disclosure agreements in place with the third parties.

☐ If storage is outside the EEA that appropriate protections are in place?

8. Prevention of data breaches

The University needs to implement:

☐ An information audit: consider what personal data and/or sensitive personal data you hold and/or have access to

See guidance notes at: https://intranet.soton.ac.uk/sites/gdpr/Pages/Implementing-GDPR.aspx

☐ A review of organisational and technical measures in place to prevent unlawful destruction, loss, alteration, disclosure of access to personal data.

☐ Pseudonymisation and encryption.

☐ A review of its ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services.

☐ A review of its ability to restore availability and access to data in timely manner in the event of physical/technical incident.

☐ Processes for regular testing, assessing and evaluating the effectiveness of security measure in place.

☐ Measures to ensure processors are employing adequate technical and organisational measures for address and contacts.

☐ Privacy policies are updated as necessary.

☐ A system is established for documenting processing operations.

☐ A data breach response plan.