Guidance notes for the GDPR readiness checklist

From: Legal Services **Date: October 2017**

These guidance notes should be read in conjunction with the GDPR readiness checklist at: https://intranet.soton.ac.uk/sites/gdpr/Pages/Implementing-GDPR.aspx

A. BACKGROUND

The General Data Protection Regulation (GDPR) has been adopted by the UK and will come into force from 25 May 2018. The UK's proposed Data Protection Bill 2017 will replace the current Data Protection Act 1998 and will implement the GDPR standards across all general data processing as well as providing clarity on the definitions used in the GDPR in the UK context.

The GDPR is designed to strengthen citizens' fundamental rights in the digital age by placing greater obligations on those who hold and obtain data and by strengthening the rights of individuals. The University of Southampton ("the University") is taking steps to be GDPR compliant by May 2018.

Whilst the GDPR builds upon the foundations created by Data Protection Act 1998, there are some new elements and significant enhancements. This guidance and the checklist are part of the steps that the University are taking to ensure that decision makers and key people are aware that the law is changing under GDPR and to be GDPR ready.

If you would like to find out more, read the Information Commissioner's 12 step guidance at: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf.

B. HELPFUL TERMS AND USEFUL INFORMATION

- **Data Controller:** the organisation that determines the purposes for and the manner in which any personal data is processed, in this case, the University
- **Data Subject**: Any living individual whose personal data the University holds
- **Data subject Rights:** under GDPR, the Data Subject has the following rights to:
    - Request access to any data the University holds about them

- Prevent the processing of their data for direct-marketing purposes
- Ask to have inaccurate data held about them amended
- Prevent processing that is likely to cause unwarranted substantial damage or distress to them or anyone else
- Object to any decision that significantly affects them being taken solely by a computer or other automated process and they have the right to request you to reconsider any such decision taken
- Ask to have inaccurate data held about them amended
- Obtain and reuse their data for their own purposes across different services e.g. banking industry allowing customers access to their transactional information in a way that can be uploaded onto price comparison sites
- Request that their personal information be deleted or removed in certain circumstances

GDPR Principles

Personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not processed further for any purpose that is incompatible with those purposes. NB: Archiving in the public interest, scientific or historical research or statistical purposes are not considered incompatible with the initial purposes
- Adequate, relevant and limited to what is necessary for the purposes for which they are being collected
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary. It can be stored for longer periods for archiving in the public interest, historical and scientific research or statistical purposes
- Processed in a manner that ensures appropriate protection

A new principle is that the Data Controller now needs to demonstrate compliance with the principles ("accountability principle"). This means that the University can no longer just say that it complies with the GDPR principles, but must also demonstrate that compliance.

- **Information Asset:** is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. It has a recognisable and manageable value, risk, content and lifecycle. An information asset may have a number of owners during its life cycle, for example:

    - personal information collected for outreach purposes (Outreach), used for the purposes of application (Student Services), used during the student's time at university (Student Services) and finally for alumni purposes (Office of Development and Alumni Relations) when they leave.
- **Information Asset Owners**: manage the information assets that they 'own.' Information Asset Owners may be assigned ownership of several assets of their organization.

Personal Data

This is data that relates to a living individual who can be identified from the data, either on its own or in combination with other information. It also includes expressions of opinion about the individual and any indication of the intentions of the data controller or any person in respect of that individual.

Even things we do not traditionally consider to be personal information such as staff/student identification numbers or online identifiers e.g. cookies are as they can be used to identify the individual.

Sensitive personal data consists of information about

- racial or ethnic origin
- political opinions
- religious beliefs or beliefs of a similar nature
- physical or mental health or condition
- sexual life
- the commission/alleged commission of an offence alleged/committed by the data subject and any related court proceedings, trade union membership
- genetic (i.e. inherited or acquired genetic characteristics e.g. blood type) and biometric data (e.g. fingerprints or photographs) where processed to uniquely identify an individual

C. GDPR READINESS CHECKLIST GUIDANCE NOTES

These notes have been designed to assist you in completing the GDPR Readiness Checklist at: https://intranet.soton.ac.uk/sites/gdpr/Pages/Implementing-GDPR.aspx.

1. Is it Personal Data?

This checklist only applies to personal data as defined above, so firstly you need to identify whether what you are processing is personal data. Part of that exercise is to also to identify whether it is sensitive personal data, as you may need to obtain explicit

consent from the data subject if you are not relying on any other lawful basis to process this type of personal data.

To comply with the accountability principle under GDPR, the University needs to document what personal data it holds, where it came from, how it is stored and whom it is shared with. To achieve this, the University is currently conducting an information audit. This audit will be cascaded through GDPR Work Stream Leads to Information Asset Owners to enable the University to document what personal data it holds and to assess whether the information held meets the requirements of the GDPR. This audit will include any personal data held by staff members collected in the course of their work such as contact details for individuals in the private/public sector who assist with student employment/placement opportunities.

3. Legal basis for processing

There are a number of grounds for processing data. Obtaining the consent of the data subject is just one of them. You must set out the correct legal basis for processing the personal data that you are collecting. Other grounds for processing besides obtaining consent are:

- A contract with the individual: e.g. to supply goods or services the data subject has requested or under an employment contract
- Compliance with a legal obligation: you are required by UK or EU law to process the data for a particular purpose
- Vital interests: the protection of someone's life either the data subject or someone else
- A public task: carrying out your official functions or a task in the public interest and you have a legal basis for processing under UK law

If you are unsure of your basis for processing or you have any queries or concerns contact gdprlegal@soton.ac.uk.

Every time we collect personal data about individuals, we must provide the data subject with a Privacy Notice which sets out our identity (the University of Southampton), why we are collecting their personal data, what we will use it for, how it will be held and shared (if appropriate). It also sets out the data subject rights. A general Privacy Notice template and Guidance notes can be found on the GDPR intranet site: https://intranet.soton.ac.uk/sites/gdpr/Pages/Implementing-GDPR.aspx

Consent

Where the legal basis for processing the data is the consent of the data subject, you must always ensure that the data subject has freely given a specific, informed and unambiguous consent to the processing including any sharing of their data. The consent must be by way of a statement or by a clear affirmative action.

Where you are relying on consent to process sensitive personal data, you must have the data subject's explicit consent to the processing. Therefore, you must identify whether you are collecting any sensitive information as defined in the 'Helpful terms and useful information' section. If you have any queries, contact Legal Services at gdprlegal@soton.ac.uk.

GDPR provides special protection for children's personal data. If any information is collected about anyone under 13 years of age we require a parent or guardian's consent in order to process their data lawfully.

Remember that any consent needs to be freely given, specific, informed and unambiguous and must be by way of a statement or by clear affirmative action. Therefore, it has to be a positive indication ('opt-in') of agreement to personal data being processed – it cannot be inferred from silence, pre-ticked boxes or inactivity.

GDPR is very clear that controllers (i.e. the University) must be able to demonstrate that consent was correctly obtained.

For more information about consent, see the General Consent Form and Guidance at: https://intranet.soton.ac.uk/sites/gdpr/Pages/Implementing-GDPR.aspx

5. Data Protection Impact Assessments

Data Protection Impact Assessments (DPIA's) are similar to the risk assessment that the University already conducts but is only in respect of personal data. Where you are involved in any new project or implementing any new systems that may involve a high risk to a data subject's rights and freedoms, a DPIA should be conducted. The DPIA register is held with Legal Services. You can contact them on: legalservices@soton.ac.uk
A copy of the template DPIA can be found at: https://intranet.soton.ac.uk/sites/gdpr/Pages/Implementing-GDPR.aspx

The Information Commissioner's Office (ICO) have produced guidance on DPIAs which you can find here: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

7. Data storage

If data is being stored externally outside of the University, especially where the storage is outside the EEA we need to be satisfied that the controller or processor is providing adequate safeguards and that the data subject still retains their rights and remedies. Check any current agreements that you have with service providers situated outside the EEA to ensure that appropriate protections have been secured. If this is a new project, then appropriate provisions will need to be included in any contract for services and the Data Protection Officer will need to be satisfied that there are adequate safeguards in place, so please contact Legal Services at: gdprlegal@soton.ac.uk and the University's Head of Information Security at gdprsecurity@soton.ac.uk.

If you would like to read further about GDPR, see here: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

8. Prevention of data breaches

The University must ensure that it has the correct procedures in place to protect personal data and to detect, report and investigate data breaches. A data breach may be anything from a staff member emailing sensitive data to the wrong person to having a computer compromised by a virus etc.

Under GDPR, the University can be fined up to four per cent of its global annual turnover so as you can appreciate this is a significant increase in risk to the University.