SOP Title Reference: **DP Guidance**	Last Reviewed: **05/02/2019**	Last Revised: **19/05/2020**	
Author: **Information Services**			

St George's University of London Policies and Procedures

Guidance on Data Protection

(see also related documents 'Data Protection Policy')

IT Services, St George's, University of London, Jenner Wing, Cranmer Terrace, London SW17 0RE

Contents

1. Introduction

This guidance has been drawn up to give a basic overview of the requirements of the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation (GDPR), and how they should be taken to apply within the framework of the University.

More detailed advice about the Act and any of the requirements outlined in this guidance, can be obtained from:

Data Protection Officer
Tel: 020 8725 0668
Email: dataprotection@sgul.ac.uk

The Data Protection Officer ensures that policies and procedures are in place to assist the Institution's employees in complying with the Act on a day to day basis.

Further information is also available via the Guide to Data Protection on the ICO website https://ico.org.uk/for-organisations/guide-to-data-protection/

2. Legislation

On 25th May 2018, the GDPR came into force across all member states of the EU.

GDPR became part of UK law via the updated Data Protection Act, with the DPA 1998 being replaced by DPA 2018.

As well as being the mechanism by which GDPR was introduced into UK law, DPA 2018 details the limited variations and exceptions (or ‘derogations’) to GDPR that apply specifically in the UK. For example, in the UK the age of consent for children is set at 13, meaning anyone aged 13 and over can give consent themselves for the processing of their personal data. For children under the age of 13 parental or guardian consent would be required.

DPA 2018 also covers those activities that fall outside the scope of the GDPR and that are not covered by other EU laws, for example the use of personal data for criminal law enforcement purposes, national security purposes and immigration purposes.

Finally, the DPA 2018 provides detail on the role of the Information Commissioner’s Office (ICO), their functions and their enforcement powers. The ICO is the regulator for data protection in the UK.

These are the reasons why we need both these laws and why they should always be read alongside each.

When the UK leaves the EU, the DPA 2018 will still apply and it's possible that little should change in terms of the data protection legislation that we need to adhere to. However, this is subject to the outcome of discussions with the EU.

3. Basic Principles

Data protection applies to the personal data of living, identifiable individuals.

Data protection legislation focuses on the privacy and legal rights of the individual when it comes to their personal data, and also provides a set of rules and guidelines for anyone processing that individual's personal data.

The requirements and standards laid out in the legislation revolve around 6 basic principles and these exist to ensure that personal data are:

1. Processed fairly, lawfully and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and, where necessary, kept up to date
5. Kept no longer than is necessary in relation to the original purpose
6. Processed securely, to ensure their confidentiality, integrity and availability

Data controllers are not only required to adhere to these principles, but must also be able to actively demonstrate that they are doing so. Examples of ways in which compliance with the principles is evidenced will include an organisation's Record Of Processing Activities (ROPA) and their Privacy Notices.

4. Lawful Basis

In order for the use of personal data to be 'lawful' you must have a valid legal basis to use it.

Data protection legislation lists 6 lawful bases for processing personal data, from which you must identify one that applies to your processing:

- Consent
- Necessary for the performance of a contract
- Necessary to comply with a legal obligation
- Necessary to protect the vital interests of the data subject
- Necessary to perform a task in the public interest or official functions
- Necessary for your legitimate interests

Not all of these bases are appropriate for the types of activities that the University carries out, so it is always best to see advice on this first.

If you are processing ‘special category’ personal data (see glossary) there is an additional list of legal bases. In order for your use of ‘special category’ personal data to be lawful you must identify one of the bases from the list above *and* one of the bases from the list below:

- Explicit consent
- Necessary for purposes of employment or social security/protection law
- Necessary to protect the vital interests of the data subject
- Legitimate activities of not-for-profit bodies
- Processing relates to personal data made public by the data subject
- Necessary for the establishment, exercise or defence of legal claims
- Necessary for reasons of substantial public interest
- Necessary for medical / healthcare purposes
- Necessary for public health purposes based on EU / member state law
- Necessary for archiving, scientific or historical research, or statistics

Again, not all of these will be applicable to the University’s uses of personal data, so you may want to seek advice before trying to identify an appropriate basis for your particular processing activity.

It’s also important to note the inclusion of the word ‘necessary’ in the definitions of the lawful bases on both these lists. The Information Commissioner’s Office (ICO) advises that ‘necessary’ does not necessary equate to having to be ‘absolutely essential’, but it must be more than just ‘useful’ and more than just ‘standard practice’. This means that if you can reasonably achieve the same outcome *without* using the personal data, you won’t have a valid lawful basis.

5. Individual’s Rights

Data subjects are assigned various rights under data protection law, and the University needs to ensure that it handles requests relating to these rights in a prompt manner and in line with the law.

These rights are

- Right to be informed – to be told how your personal data is being used, this is usually done through a ‘privacy notice’
- Right of access – to have access to your personal data, exercised through submitting a ‘data subject access request’
- Right to rectification – for individuals to request that inaccurate personal data is rectified
- Right to erasure – individuals can have personal data erased where appropriate, but is not absolute and only applies in certain circumstances
- Right to restrict processing – to restrict or suppress processing of an individual’s personal data, but is not absolute and only applies in certain circumstances

- Right to data portability – whereby individuals can obtain (in a machine-readable commonly-used format) and reuse (for their own purposes and across different services) the personal data they have provided to a data controller
- Right to object – for an individual to object to the processing of their personal data in certain circumstances, including direct marketing
- Rights related to automated decision making (including profiling) – the right not to be subject to a decision based solely on automated processing which has legal implications or similarly significantly affects that individual

A request exercising one of these rights will normally need to be responded to within on calendar month, and not all of the rights require the individual to make their request in writing.

It is important to know how to handle a request if you receive one, so you should also refer to the relevant procedural documents.

6. Privacy Notices

Data protection law requires that we are open and transparent about our use of personal data. This means ensuring that individuals are informed of how and why we use their personal data, and one way of providing this information is through a privacy notice.

Privacy notices must include specific pieces of information, such as the identity of the person processing the data ('data controller'), the purposes for which the data is being used, who the data will be shared with, how individuals can exercise their rights.

Privacy notices must also be presented in a format that is easily accessible, be provided at the time that the personal data is collected and be clear and concise.

If you need to draft a privacy notice please refer to the University's separate guidance on this.

7. Data Protection Impact Assessments

Where the use of personal data is likely to result in a 'high risk' to individuals, a Data Protection Impact Assessment (DPIA) should be carried out. GDPR makes DPIAs a mandatory requirement in certain scenarios, for example a DPIA would be expected whenever the use of 'special category' data is involved, e.g. health-related personal data.

However, it is good practice to carry out a DPIA for any new project involving the use of personal data or where existing personal data is going to be used in

a new way, and not just where there is a mandatory requirement for one. Screening questions will help establish whether a particular project requires a DPIA to be carried out.

A DPIA should be done during the initial phase of a project to ensure any risks can be identified and addressed at an early stage. The DPIA will then become a 'living' document which may need to be revised and updated at different stages throughout the course of the project.

Guidance (including screening questions) and a copy of the University's DPIA form can be obtained here:

8. Data Breaches

GDPR introduced a new obligation to report certain types of personal data breach within 72 hours of becoming aware of that breach. In such instances breaches must be reported to the relevant supervisory authority, i.e. the Information Commissioner's Office (ICO).

Where the breach involves a high risk of negatively impacting on individuals' rights and freedoms it will also be necessary to inform the individuals affected.

A data breach is defined in GDPR as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted stored or otherwise processed."

Examples of data breaches include:

- A letter or email sent to the wrong person by mistake
- Lost or stolen laptop or USB stick
- Documents not disposed of via the proper confidential waste mechanism
- Leaving your PC logged on and unattended, allowing unauthorised persons to access it
- Failing to securely wipe a PC's hard drive before disposing of it
- Equipment failure resulting in loss of data
- Inadvertently disclosing information to a telephone caller

Data breach incidents must be reported immediately following the University's breach reporting procedure.

9. Data Security

Data protection law imposes a data security requirement on organisations, a requirement to ensure the 'confidentiality, integrity and availability' of any personal data being processed.

- Confidentiality means ensuring that only authorised persons have access to personal data.
- Integrity means ensuring personal data are kept accurate and up-to-date.
- Availability means ensuring personal data is accessible whenever required

Anyone processing personal data needs to have suitable security policies, protocols and procedures in place to prevent that personal data from being compromised, either accidentally, negligently or intentionally.

Examples of measures for managing personal data securely include:

Keeping documents locked away when not in use
Using access controls to prevent unauthorised access to personal data
Backing up work routinely, so it can be easily restored if corrupted
Disposing of documents via approved confidential waste mechanisms
Training staff on data security awareness
Using encryption to protect data on portable and removable devices
Making sure amendments to personal data are processed promptly

All members of the university are expected to be responsible for handling personal data securely and in-line with the University's information security related policies.

10. Data Sharing

It may be necessary on occasion to share personal data. This will normally happen either where a legal obligation exists that requires us to share the data, or where there is a legitimate business need to do so.

When personal data is shared internally it must only be with SGUL members who are authorised to have access to that data. Internal recipients of personal data may only use it for the designated purpose(s). Where University personal data is being shared internally for a new purpose it may be necessary to review and update the relevant staff or student privacy notice.

Where personal data is transferred outside of SGUL a legal basis for doing so must be determined. Personal data must be shared in such a way as to ensure the security of that data once it leaves the institution. Special consideration must be made where data is being transferred outside of the EU. This will require ensuring either that the destination country has an Adequacy Decision from the EU indicating it has suitable data privacy legislation in place, or that any contract covering the transfer includes appropriate safeguards to protect the personal data.

Transfers of personal data should only take place once a formal contract or agreement is in place covering the sharing of the data. The University's in-

house General Counsel can review the legal aspects of data sharing contracts and agreements.

For further advice on data sharing please contact the Data Protection Officer to dataprotection@sgul.ac.uk, or where the sharing relates to research activities please contact the Joint Research & Enterprise Services (JRES).

11. Data Retention

Data protection legislation stipulates only that personal data should not be kept for longer than is 'necessary'. The Act itself does not provide specific guidance on how long you should keep personal data and it may be necessary to refer to other legislation for relevant guidance.

Information on retention periods for SGUL's records can be found in the University's Records Retention Schedules. Further advice on appropriate retention periods can be obtained from the Records Manager.

12. Accountability

Under data protection legislation all data controllers are subject to certain accountability obligations. The main obligations in this respect include the requirement to:

- Maintain records of all processing of personal data carried out across the organisation
- Document breaches involving personal data, and to notify both the ICO and the affected data subjects where relevant.
- Appoint an independent Data Protection Officer to advise on, and monitor, compliance
- Have contracts in place covering the sharing and transferring of personal data to other organisations
- Carry out Data Protection Impact Assessments on data processing activities that are likely to result in high risk to individuals' interests
- Implementing appropriate data protection policies, procedures and processes

Accountability means not only taking responsibility for complying with data protection legislation, but being able to demonstrate, through documented evidence, how this compliance is achieved.