Introduction.

The GDPR (General Data Protection Regulations 2016) is the EU regulation covering people's pesonal data. Together with the Data Protection Act 2018 (DPA), it's designed to protect individuals' personal information in an era of mass digital data use. The GDPR is in force across the EU and supersedes previous data protection laws. Both the GDPR and the DPA will be referred to as 'Data Protection Legislation' throughout this module.

The Data Protection Legislation imposes much tougher restrictions on how personal data is used and it applies to organisations who use personal data of individuals in the EU.

Almost all organisations deal with some kind of personal data – even if it's only their employees – so it's almost certain to affect you and your organisation.

What counts as personal data?

Under the GDPR, Data Subjects have the right to request copies of personal data held on them. The following are examples of this.

- Address and contact details.
- Credit scoring history.
- Correspondence to and from an individual.

Even ‘informal’ information held on a Data Subject is covered.

Restrictions & consequences.

Certain types of personal data have special restrictions on them. And whatever type of personal data you're handling – if the law is broken, the consequences can be serious.

What are examples of 'special categories of personal data'?

The following are examples of 'special categories of personal data':

- Sex life or sexual orientation.
- Genetic data.
- Biometric data.
- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade-union membership.
- Physical or Mental Health.

When can special categories of personal data be processed?

Special categories of personal data can only be processed if certain conditions are met (ideally more than one):

- Consent has been given explicitly.
- Information is required by law.
- To protect the individual's vital interest.
- Data already made public by Data Subject.
- For research purposes.
- For reasons of substantial public interest.
- When it is necessary for the establishment, exercise or defence of a legal claim.

Any other conditions set out in Article 9 of the GDPR or Schedule 1 or the Data Protection Act 2018.

What are the implications of failing to comply with the GDPR?

Under the GDPR there is an increase in fines to up to €20 million for some failures to comply. This is based on the type of breach:

- A business could be fined up to €10,000,000 or 2% of global income if (for example) they fail to maintain records of processing or report breaches.

- They could be fined up to €20,000,000 or 4% of global income if the violation relates to fundamental issues (e.g. individuals' rights, or conditions for consent).

- Our partners can refuse to do business with us.

There could also be serious damage to reputation.

In addition, the ICO has the rights to audit; issue warnings; order a controller to comply with a data subject's request; and impose a temporary or definitive limitation including a ban on data processing.

Data Protection impact assessments (DPIAs).

A DPIA is a process that helps identify and minimise the privacy risks of projects that involve the processing of personal data. A DPIA also helps to strike a balance between operational aims and the likely impact on indviduals.

UCL staff must conduct DPIAs for projects that are likely to result in a high risk to the privacy of individuals (i.e. whenever Special Categories or Criminal records data is processed). Even if the project does not involve a high risk to individuals, it is good practice to conduct a DPIA.

DPIAs should be kept to date and re-written should the project or system change substantially.

A DPIA helps to:

- Describe the nature, scope, context and purposes of the processing;
- Assess how necessary and reasonable the processing is;
- Identify and assess risks to individuals; and
- Identify additional measures to mitigate those risks.

UCL has produced some guidance on DPIAs and easy-to-use templates for the purposes of (a) research and (b) professional services. For more information on Guidance for DPIA please refer to appendix A in the accompanying PDF titled ‘Supporting Appendices’.

A DPIA should be completed before processing begins.

Key themes.

The GDPR is underpinned by some of the following key themes.

Worldwide.

When organisations anywhere in the world offer goods and services to anyone in the EU or monitor their behaviour, Data Protection Legislation applies. The GDPR also applies to organisations established in the EU that process any personal data.

The territorial scope of the GDPR stated in Article 3 is:

"1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

    (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

    (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."

Enhanced rights.

The GDPR enhances the rights of individuals (Data Subjects) over their personal data, including the right to:

- Access their personal data.
- Rectification.
- Erasure.
- Restrict processing.
- Data portability.
- Object.
- In relation to automated decision making and profiling.
- To be informed.

The rights do not always apply and in circumstances, such as research, only a very limited set of rights apply.

Data protection by design and default.

The GDPR expects organisations to put data security and privacy foremost when designing new systems and ways of processing:

- Ensure systems are secure and respect privacy rights by design and from the outset.
- Minimise the collection of personal data to only that which is necessary for the purpose of processing.
- Anonymise and encrypt wherever possible.
- Use privacy enhancing technologies.

Responsibilities and accountabilities.

The GDPR creates new and enhanced requirements for organisations. They must:

- Document their data processing activities.
- Provide evidence of how personal data is protected.
- Be transparent, lawful and fair in their use of personal data.
- Have a legal basis for processing personal data, e.g. the consent, contractual necessity or a legal obligation.

Principles-based processing.

The Data Protection Legislation is a principles-based piece of legislation, meaning that all processing of personal data should observe the following principles:

- **Lawfulness, fairness and transparency.**
  Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

- **Purpose limitation.**
  Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

- **Data minimisation.**
  Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- **Accuracy.**
  Personal data shall be accurate and, where necessary, kept up to date.

- **Storage limitation.**
  Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- **Integrity and confidentiality.**
  Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- **Accountability.**
  Personal data shall be processed in a manner that organisations will be able to demonstrate compliance with the above principles.

Transparency, fairness and privacy notices.

Under the new Data Protection Legislation, all organisations must ensure that they use personal data fairly and transparently.

For UCL this means that:

- We must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned; and

- We must be clear, open and honest with people from the start about how we will use their personal data.

One of the best ways to meet the requirements of 1 and 2 above is to issue privacy notices to people whose personal data we are using.

UCL has developed several organisation-wide privacy notices. For more information on Guidance for privacy notices please refer to appendix B in the accompanying PDF titled ‘Supporting Appendices’. Please read these documents and familiarise yourself with their contents.

They are designed to set out how UCL will use people’s personal data at an organisational level.

In addition to these organisation-wide privacy notices, staff may also have to develop their own privacy notices to ensure they inform people about how their personal data will be used.

Doing so will help meet the fairness and transparency requirements of the new Data Protection Legislation.

These ‘local’ privacy notices should refer to UCL’s organisation-wide notices. On guidance on how to write such privacy notices please see appendix C in the accompanying PDF titled ‘Supporting Appendices’.

Privacy notice.

The following should be included in a privacy notice.

- The purposes of processing.
- Lawful basis of processing.
- The information rights available to individuals.
- Categories of personal data used.

There is no requirement to list out information security measures, eg encryption, or statements on how seriously UCL takes data protection!

Key requirements.

The GDPR allows organisations to collect and process personal data, provided they comply with some key requirements. These are:

- Data is used lawfully, fairly and transparently.
- Data processing procedures are documented.
- They provide evidence of how they are protecting data.

Organisations must document their processing activities and provide evidence of how they are protecting data and using it lawfully, fairly and transparently.

Personal data can come in many forms. It is not only data belonging to customers or clients, but staff, suppliers and anyone else whose personal data the organisation comes into contact with.

The GDPR is about privacy and accountability, not about deleting data. Organisations can still store and process personal data, and in many cases, they may be required to.

The GDPR doesn’t just cover data belonging to customers or clients. Nor must data be ‘single-use only’

Personal data breach.

In the event of a personal data security incident you should:

- Keep a company record of this breach.
- Notify all staff affected.
- Notify the UCL Information Security Group (ISG@ucl.ac.uk), who will assess the incident and report it within 72 hours.
- The UCL Data Protection Officer will notify the relevant supervisory authority (if outside of the UK).

Data security isn't just about protecting information from outside threats like hackers. In fact, the single most common form of data breach at UK organisations is simple human error, such as inadvertently emailing the wrong person. Under Data Protection Legislation, there are strict rules for organisations on what to do in the case of a data incident like this.

Please ensure you read the guidance on reporting an incident, you can find the guidance on reporting an incident in appendix D in the accompanying PDF titled 'Supporting Appendices'. The Information Security Group (ISG) and the Data Protection Officer (DPO) will then be able to review the nature of the breach and take any further action required.

Tip: Remember, the Data Protection Legislation not only gives EU residents more control over their personal data, but aims to make organisations accountable for how they use and process it.

Protecting personal data.

If you were to lose your bag, would you know what personal data was potentially being compromised?

The following are just a few examples of what could be compromised:

- Unencrypted removable media (e.g. USB stick).
- Computers or phones without strong passwords.
- Paper-based records containing personal data.
- Unsecured devices with voice activation/notifications enabled.

Everyone in our organisation may have access to someone's personal data, even away from the office. So stop now and make a note of anything you regularly have on your person that might contain personal data. What could you do to minimise future risks?

Remember: as soon as you become aware of a 'near miss' or potential data breach, please follow the guidance on reporting an incident in appendix D in the accompanying PDF titled 'Supporting Appendices' as personal data breaches must be disclosed to the ICO (UK regulator) within 72 hours. You do not have to make a decision about whether or not to inform the ICO - the security team does this – but your swift response will help them do that.

An encrypted laptop is reasonably secure.

Lawfulness of processing: the six bases.

All processing of personal data must meet one of the following six conditions in Data Protection Legislation. There is information on Article 6(1) in appendix E in the accompanying PDF titled ‘Supporting Appendices’.

- Public task.
- Consent.
- Contract.
- Legal obligation.
- Vital interests of an individual.
- Legitimate interests.

There are only six lawful bases for processing personal data. All processing of personal data must meet one of these conditions to be lawful. If special category personal data is being processed, a further condition will be required in addition to the six above.

Just because the Police request personal data from UCL does not make it lawful - a disclosure to the Police will still need to meet a condition for lawfulness in GDPR. Consent given on behalf of others is unlikely to be valid. ‘Need to know’ is not a lawful basis.

Lawfulness of processing: public task.

One of the conditions for processing personal data is if processing is necessary for UCL to perform a task in the public interest (‘public task’).

As a public authority incorporated under a Royal Charter, UCL can use this condition for a wide range of its core functions, such as teaching and learning, research and its activities around innovation, and further ‘ancillary’ functions that support these core purposes.

UCL has published a Statement of Tasks in the Public Interest that can be viewed in appendix F in the accompanying PDF titled ‘Supporting Appendices’ that sets out what types of processing falls within scope of ‘public task’.

Within Scope?

Those functions that fall within scope of the public task condition are:

- Teaching and learning for undergraduate and postgraduate courses.
- Activities around innovation.
- Ethical research.
- Ancillary functions to support core purposes.

Public task’ only covers the processing of personal data, not special category personal data. For special category personal data, a further condition must be found.

While clearly legitimate UCL interests, processing personal data for purposes such as information security, marketing, merchandising, or alumni are likely to fall outside of the scope of ‘public task’.

Lawfulness of processing: Legitimate interests

One of the six conditions for processing personal data is if processing is necessary for the purposes of the legitimate interests pursued by UCL or a third party (‘legitimate interests’). This UCL can rely on this condition if:

(a) a legitimate interest exists and

(b) such an interest would fall outside the scope of the ‘public task’ condition. There is a guidance note on ‘legitimate interests’ in appendix G in the accompanying PDF titled ‘Supporting Appendices’.

Legitimate interests?

To use ‘legitimate interests’ as a lawful basis for processing, the following steps must take place:

- Check to see if the purpose is included in the ‘Statement on Public Task’. If it is, then you cannot use ‘legitimate interests’ condition.
- Identify the legitimate interest(s).
- Complete a Legitimate Interests Assessment (LIA) prior to processing the personal data.
- Balance the ‘legitimate interest(s)’ you wish to use against the impact on individuals.
- Conduct a necessity test.

Legitimate interests’ only covers the processing of personal data, not special category personal data. For special category personal data, a further condition must be found.

Remember that the ‘legitimate interests’ condition is not available to UCL if the purpose is already covered in the Statement of Public Tasks, there is information on the Statement of Public Tasks in appendix F in the accompanying PDF titled ‘Supporting Appendices’, so it is not available for UCL core purposes such as teaching/learning and research activities. A LIA should be conducted before processing begin.

Lawfulness of processing: Consent.

One of the conditions for processing personal data is ‘consent’.

As a public authority, UCL is limited in the ways it can rely on consent because there is often an imbalance of power between a public authority and an individual; this means that consent would not be valid as it would not have been freely given. The definition of consent is:

“Any freely given, specific, informed and unambiguous indication of the individual’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”

Consent will still be relied on in some circumstances, eg to meet ethical requirements in research or to meet confidentiality obligations, but it will not often be the lawful basis of processing for UCL for the purposes of complying with Data Protection Legislation.

Who is subject to GDPR?

A controller or processor established within the EU.

- You have to comply with the GDPR in respect of all personal data you process.
- The location of the personal data or the data subjects is irrelevant – all personal data you process is subject to the GDPR.
- The nationality of the data subjects is irrelevant.

A controller or processor established outside the EU that processes the personal data of individuals located within the EU in connection with (a) offering goods or services to those individuals; or (b) monitoring their behaviour within the EU.

- You have to comply with GDPR only in respect of the personal data of the individuals located within the EU that you are targeting or monitoring.
- You do not need to comply with GDPR in respect of other personal data you process.

A controller established outside of the EU that uses (a) a processor located inside the EU to process personal data on its behalf or (b) servers and other equipment located in the EU to process personal data.

- You have to comply with GDPR only in respect of the personal data processed by your processor or equipment located within the EU.
- You do not need to comply with GDPR in respect of other personal data you process.

Controllers and processors.

Both ‘controllers’ and ‘processors’ have requirements in Data Protection Legislation.

Definitions.

A controller is a person or organisation that, alone or jointly with others, determines the purposes and means, i.e. the ‘why’ and ‘how’, of processing personal data.

A processor only uses personal data on behalf of the controller. Both ‘controllers’ and ‘processors’ have requirements in Data Protection Legislation.

Contracts.

There must be a contract in place between a controller and a processor.

If the processor uses personal data for any other purpose than what is set out in the contract it will become a controller.

UCL’s role.

UCL often takes the role of a controller. It often outsources functions to suppliers or third parties who are its processors. UCL Procurement should be contacted for advice on contracts for services. UCL Research Contracts should be contacted for guidance on contracts relating to research.

Shared data.

When UCL shares personal data with another controller, for instance with another university as part of a research project, a data sharing agreement should be put in place.

Knowledge Check.

Here are some statements on controllers and processors:

- UCL will be a controller when it uses personal data for teaching and learning purposes.
- A data sharing agreement should be used when personal data is shared between two controllers.
- Processors can be based overseas.
- An organisation that is employed by UCL to provide confidential waste services should only process personal data according to UCL instructions.

Both processors and controllers are responsible for ensuring adequate security measures are in place. If UCL is using a processor a contract will be necessary. UCL can be a joint controller with other organisations if both organisations jointly determine the ‘how’ and ‘why’ of processing of personal data.

For advice on drafting data sharing agreements, contact data-protection@ucl.ac.uk

Data Subject rights.

Under the GDPR, ‘Data Subjects’ enjoy enhanced privacy rights.

Subject access.

Data Subjects have a right to request that a Controller supply them with a copy of their personal data. This includes correspondence to and from an individual.

Stop data processing.

An individual has the right to obtain a restriction of processing in certain limited circumstances.

Object to processing.

Individuals have the right to object to processing in certain limited circumstances.

Correct inaccurate information.

Controllers must maintain only accurate information about individuals.

Erasure.

The ‘right to be forgotten’. Individuals have the right to request that businesses delete their personal data in certain limited circumstances.

Portability.

This is a new right for Data Subjects - individuals have the right to obtain a copy of their personal data from the Controller in a commonly-used format, and have it transferred to another Controller.

Automated decisions.

Individuals have the right to object to significant decisions, including profiling, made solely by automated means.

Compensation.

Individuals have a right to claim compensation for damages caused by infringement of the GDPR from the Controller or the Processor.

Requests for information under Data Protection Legislation.

Under data protection (and freedom of information) legislation and individuals have rights to request information. Such requests are not ‘business as usual’ and should be passed immediately to the Data Protection Office (data-protection@ucl.ac.uk). On receipt of such requests, UCL must respond within tight timeframes to comply with the law and the clock begins to run down from the moment UCL receives such a request.

Requests for personal data may come in from individuals or organisations, like the Police. There is no requirement for requesters to cite the legislation so all staff need to be able to recognise such requests.

Valid or not?

Let's now work through a series of specific potential requests under Data Protection Legislation, seeing whether each one is valid - or not. We'll then conclude by reviewing some key points.

'I want to see a copy of my HR file'.
Correct, this is the right of access.

'My details are wrong. Please correct them'.
Correct, this is the right to rectification.

'I would like copies of previous versions of the HR policy'.
Incorrect, this does not involve personal data so would not be handled under Data Protection Legislation.

'Please remove my personal information from SITS'.
Correct, this is the right to erasure.

'Do not disclose my personal data to the Mr Jones'.
Correct, this is the right to restrict processing.

'Give me a copy of UCL's annual accounts'.
Incorrect, this does not involve personal data so would not be handled under Data Protection Legislation.

'(from the Police) I want to see details of a student of yours, Jim Jones'.
Correct, this is a Police request and might be disclosed under an exemption in Data Protection Legislation.

'Please provide information held in the application system in electronic form'.
Correct, this is the right to data portability.

'I object to UCL using my personal data for marketing purposes'.
Correct, this is the right to object.

Key Points.

Requests that are not ‘business as usual’ and do not involve personal data are usually handled under Freedom of Information (FOI). Note that there is no requirement to state the legislation.

If you receive any of the above examples these should be forwarded to the Data Protection Office on data-protection@ucl.ac.uk

If you are on annual leave and/or are not able to monitor your email, you should set an out of office message as per the guidance on Out of Office message in appendix H in the accompanying PDF titled ‘Supporting Appendices’.

Information security.

The majority of the fines for data protection breaches involve lapses in security.

- The new Data Protection Legislation puts greater obligations on UCL to ensure that ‘appropriate technical and organisational measures’ are in place to provide information security.

- Such ‘measures’ would include pseudonymisation, encryption and a risk-based approach to security. These will help ensure the confidentiality, integrity and availability of systems and services and the personal data held within them.

- While ISD manage information security for many central systems and services, (e.g. email and central filestores), individual members of staff also have a responsibility to work in a secure and compliant manner.

- The scope of information security is wide and covers subjects like remote and mobile working, storage, access to manual records and secure transfer of data.

- Risks increase when personal data is taken outside UCL’s secure computing environment.

Ensuring Information Security.

For data protection purposes, the following measures would help ensure information security?

Using encryption on laptops.

Locking filing cabinets containing personal data.

Using a Virtual Private Network when off campus.

Given the rising profile of information security and the ever-evolving threats of working online, UCL has developed a dedicated online module to provide staff with the necessary training.

Using public Wi-Fi without additional protection (e.g. Virtual Private Network) is high risk. Transferring sensitive information from UCL's secure computing environment to another organisation increases the risks of processing personal data. Using non-UCL email dramatically increases the information security risks for UCL.

Pseudonymisation and anonymisation.

The new Data Protection Legislation encourages UCL to use techniques to minimise the use of personal data wherever possible. Techniques such as pseudonymisation and anonymisation can help achieve this goal.

Anonymous data.

Anonymous data is information that does not relate to an individual.

Data Protection Legislation will not apply to anonymous data as there is no privacy risk in using it.

Pseudonymous data.

Pseudonymous personal data still relates to an individual and so remains as personal data, but identifiable information has been ‘masked’ in some way.

For example, this may be done by replacing names with numbers, e.g. ‘00000045’ for ‘John Smith’. Such masking reduces the risk of processing.

UCL should use pseudonymised personal data where practically possible.

Why pseudonymise?

A member of staff has a spreadsheet containing a list of staff names and contact details and wants to email this to a partner organisation for some legitimate business purpose. They should pseudonymise (e.g. swap names for numbers) the personal data:

In the event it was emailed to the incorrect recipient, the risk of unauthorised disclosure is reduced.

It observes the data protection principle of ‘data minimisation’.

It will help protect the privacy of individuals in the spreadsheet.

In the event the data is accidentally lost, the risk of a data security breach is reduced.

Data Protection Legislation still applies to pseudonymised personal data. Concerns around consent are not relevant in this example.

Personal data incidents, breaches and ‘near misses’.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data where there is a likely to be a privacy risk to individuals.

- This can be whenever any personal data is lost, destroyed, corrupted or disclosed without proper authorisation. Examples of such breaches might include sending an email containing a spreadsheet of personal data to an unintended recipient; losing an unencrypted laptop on the train; or posting a confidential letter to the wrong person.

- Under the Data Protection Legislation, UCL has only 72 hours to report such breaches from the moment we become aware of it.

- This means that staff (or anyone using personal data on UCL’s behalf) must report any incidents, ‘near misses’ or breaches as soon as possible to isg@ucl.ac.uk

- Prompt reporting enables UCL to meet its obligations under Data Protection Legislation and put in place measures that can limit the extent of the damage.

- If you are unsure about whether or not to report the incident, err on the side of caution and report it to Information Security Group.

The guidance for reporting a loss of personal data can be found in appendix D in the accompanying PDF titled ‘Supporting Appendices’.

Report- or not?

The following incidents should be reported to isg@ucl.ac.uk.

- An unencrypted laptop with access to your Outlook UCL email is left in a cafe.
- A database containing staff names and user IDs is accidentally published on the UCL website.
- An email containing staff sickness logs is sent to a wrong recipient outside UCL.
- An email containing confidential HR records is emailed to the wrong person inside UCL.

Where there is no personal data or sensitive information lost or where there has not been a breach, there is no need to report the incident. However - if in doubt, report it. There are significant risks around not reporting data breaches and the ISG team can only report breaches that it is made aware of.

Conclusion.

You've now completed this introduction to the GDPR.
Take a moment to reflect on how the points we've covered apply to your own job. What might you need to do differently now?

The 5 Rs

- Respect personal data.
- Reduce the data you collect.
- Remove identities from data if possible.
- Restrict access to data (e.g. via encryption).
- Review and delete if no longer required.

Legal checklist

The ICO highlights some key steps to ensure organisational GDPR compliance:

- Ensure key people are aware.
- Audit the personal data you hold.
- Review privacy notices and how you get consent: is parental consent required?
- Check ability to comply with Subject Data Rights.
- Identify lawful basis for data processing.
- Review processes for handling breaches.
- Decide how to implement privacy by design.
- Make someone responsible for data protection.
- Operate across EU borders? Check who your 'lead regulator' is.