BLSupdate.com

General Data protection Regulation (GDPR)

General Data Protection Regulation (GDPR)

Aims of this course:

- To understand General Data Protection Regulation (GDPR) is and who it applies to
- To learn the important definitions regarding GDPR
- The six principles and the key changes
- Learn the significance of UK GDPR compliance
- Learn how to formulate a policy

What is the UK GDPR?

The General Data Protection Regulation is known as GDPR which came into effect on 25th May 2018. The European GDPR (EU GDPR) is implemented into UK data protection law as of January 1, 2021. In the UK, what is now known as the UK GDPR is mainly still based on the same principles as the EU GDPR.

The UK GDPR, meanwhile, creates its own areas of:

- National Security

- Intelligence Services

- Immigration

The changes amend the Data Protection Act of 2018, which sits alongside the UK GDPR.

If you are a UK business or organisation that collects and stores personal data in the UK, you must comply with the UK GDPR.

What is the Information Commissioners Office? (ICO)

The Information Commissioner's Office (ICO), the UK's primary data protection authority, takes over as the lead regulator, supervisor, and enforcer of the UK GDPR on January 1, 2021. With the new UK GDPR powers, the Secretary of State can now make decisions without consulting the ICO.

What is personal Data?

The GDPR stipulates that the regulation applies to:

"the processing of personal data entirely or partially by automated means and to the processing other than by automated means of personal data which form part of or are intended to form part of a filing system."

Personal data refers to details about a named or identifiable natural person.

The focus of the data is this person.

The context

The context in which the information is held is crucial.

The ICO provides the following helpful example to clarify this:

“Because there are many people with the name John Smith, it's possible that name alone is not necessarily considered personal information. But when the name is paired with other details (such an address, a place of employment, or a phone number), it will typically be enough to clearly identify one person.”

Having said that, it also clarifies how a person can sometimes be identified without the use of a name. It reads:

"Just because you don't know someone's name doesn't mean you can't recognise [them]. Even if many of us may not know the names of every neighbours, we can nevertheless recognise them.”

Is this personal data?

It is advised to stay on the side of caution if you are unsure if the data your organization/business maintains constitutes personal data.

To achieve this,

- ensure that all data is securely stored.
- You merely maintain the necessary data.
- You don't keep it on hand for more time than is essential.

Who Is Covered by the UK GDPR?

The UK GDPR applies to: **Processors and Controllers**

The Controller:

- explains the purpose of the data collection and the methods used + may be any business or entity
- must ensure that the processor complies with data protection laws
- must ensure that all personal data is used for a purpose that is clear, legal, and transparent.

What does lawful mean?

Lawful can mean:

- if a person has given permission for their personal data to be used
- to stand by a contract
- to protect the subjects interests
- to protect the controllers interests

Data can only be processed if one of these applies

The processor acts on the controllers behalf

What information does the UK GDPR apply to?

According to the UK GDPR, "personal data" includes:

- Cultural details
- IP address
- Information on health
- Financial details

This is a result of how information on people is gathered changing with technology.

Both manual filing methods and automated personal data processing are covered by the UK GDPR.

The UK GDPR may apply to personal data that has been pseudonymized, such as key-coded, depending on how challenging it is to link the pseudonym to a specific person**.**

What are the UK GDPR Rights?

1. The right to know what personal data they have on themselves

2. Access to their stored data is a right

3. The ability to correct something so that it can be fixed

4. The erasure right

5. The ability to limit processing such that information exchange is constrained

6. The right to carry data to allow for secure information transfer the option to object to specific data processing practises.

8. The appropriateness of automated judgements and profiling

Key Changes

The UK GDPR website says:

The aim of the UK GDPR is to protect all citizens from data breaches in an increasingly data driven world . This will make data protection consistent throughout the UK

The UK GDPR fulfils the following:

The UK – It applies to the processing of personal data by controllers and processors in the UK, regardless of whether the processing takes place in the UK or not

Penalties – there are many serious penalties and consequences for serious infringement and non-compliance. Companies may be fined for inadequate security to personal data

Consent - The request for consent must be specific. Individuals have authority over their personal data when it is utilised by a business, and consent must be demonstrated. Individuals have the right to withdraw their permission at any moment. To comply with the UK GDPR, you must follow this or stop collecting data. There should be no natural or passive acceptance, such as opt-outs or pre-checked boxes. Individuals must perform a consent action in order to meet the UK GDPR obligations.

Breach notification – Under the UK GDPR, notifications of breaches are mandatory, where the breach of data is probable to 'result in a risk for the rights and freedoms of individuals. This has to be done within the first 3 days of the breach.

Right to Access - The right for data subjects to get clarification from the data controller as to whether or not personal data concerning them is being processed, where, and for what purpose is one of the rights stated by the UK GDPR.

Right to be forgotten – also known as Data Erasure, the data subject has the right to erase his/her personal data

Data Portability - The GDPR in the United Kingdom involves data portability. This is the right of a data subject to receive personal data about themselves that they have previously submitted in a "commonly used and machine readable format" and to transmit that data to another controller.

Privacy by design – controllers must hold and process only the data absolutely necessary for the completion of its duties, as well as limiting access to personal data

Data protection officers – Under the UK GDPR, its not necessary to notify the Data Protection Authority of data processing activities.

The UK GDPR and data protection Act 1998

The ideas underlying the UK GDPR are based on the Data Protection Act of 1998.

There is a necessity for accountability. This means you must demonstrate how you adhere to the principles, for example, through documentation.

The definition of 'sensitive data' in the UK GDPR is similar to that in the Data Protection Act, and refers to information such as an individual's ethnicity, political opinions, physical traits, mental characteristics, criminal crimes, and/or trade union activity.

What are the principles in the UK GDPR?

The principles of the Data protection Act underline the 6 privacy principles of the UK GDPR:

Lawfulness, Fairness and transparency:

Lawfulness: Processing must meet the above-mentioned legal requirements.

Fair: what is processed must correspond to how it is described

Transparency: the subject must be aware of the data processing that will take place.

Purpose Limitations: personal data can only be obtained for specific purposes and used for those purposes

Data minimisation: only data necessary for the purpose must be collected

Accuracy: data must be accurate and up to date

Storage limitations: data must not be held longer than needed

Integrity and confidentiality: processors must handle data protectively against accidental loss, damage, loss or unlawful processing

An EU/EEA GDPR Representative?

The EEA includes EU member states as well as Iceland, Liechtenstein, and Norway.

If you have no offices or installations in the EU/EEA but you:

- provide goods/services to people in the EEA
- monitor people's behaviour in the EEA

Depending on where some of the individuals whose personal data you are processing are situated, you may need to select an EU/EEA GDPR Representative who is based in that region.

A basic service contract with the representative; a legal firm, consultancy, or private company; is the simplest approach to designate a representative. The representative must be able to represent you in relation to your EU GDPR duties. Individuals whose data you are processing must have access to the representative's contact information. When you collect their data, you can include them in your Privacy Notice or information. The representative's details must be easily accessible to regulatory authorities, such as on your website. The presence of a representative has no bearing on your personal obligation or liability under the EU GDPR.

Is a representative always required for a UK organisation?

You don’t need a representative if:

- you are a public authority
- your processing is of low risk and does not involve the large scale use of special category or criminal offence data

Documentation

What kinds of data documents could you have?

Documents held by your organisation may include:

- Forms of registration and incident records
- Personal files,
- accident data,
- medical information,
- and staff files/contact information

DBS keeps track of bank information.

Where do you keep this data?

Data could be held in many different devices, such as;

- phones
- paper files
- displays
- websites
- computer files

What are privacy or data protection impact assessments (DPIAs)

These are tools to help you determine the most effective ways to fulfil your data protection processes while also upholding individual privacy expectations. A DPIA is not required for every process; only those that you perceive to be high risk for the data subject or new technology require one. As an example, consider the deployment of a new system that collects any personal information.

Risk Assessments

The UK GDPR has a risk based approach.

The risk assessment allows settings to:

- determine the level of risk their data carries, if threatened.
- identify threats that could be harmful to an organisation,

such as:

- intruders
- breaches
- criminals
- disgruntled employees

Aim to reduce the risks.

There are 3 clear areas when considering risk assessment:

ASSESS - Assess it, identify the risk, prioritise

ACT - Classify your data, take required action, manage the risk

RECORD - Ongoing monitoring, Incident tracking

With this in mind, data held by your setting can be measured and actioned in this way.

What is needed in a Data Protection Impact assessment?

What Information Is Required for a Data Protection Impact Assessment? (DPIA) The minimum criteria are as follows:

a systematic description of the processing the processing's purposes and the controller's legitimate interests the processing's necessity and proportionality in regard to the purpose

an assessment of the threats to data subjects' rights and freedoms

the safeguards in place to deal with and protect personal data

compliance with the UK GDPR in terms of data subjects' rights

Remember to do a DPIA only if your procedures or systems change. If you do construct a DPIA, make sure to go through it on a regular basis.

What is a privacy notice?

Consider what legal basis you are processing this information under when developing your privacy notices.

The following information should be included in your privacy notice:

- The type of data you're gathering (names, addresses, dates of birth, ethnicity, and so on).
- Who is collecting it and how is it being collected (paper forms, electronic forms, a parent portal, etc.)?
- Why is it being gathered?
- What will be done with the data?
- Who will you share the information with?
- Will there be an impact on the individual (data subject) in question, and are any individuals likely to object or complain?

A UK GDPR File

Make a GDPR file for the United Kingdom.

Add UK GDPR and data sharing to your file and make sure it is discussed and documented on a regular basis.

Include it in meetings on a regular basis and document it in your minutes.

Copies may be kept in the UK GDPR file.

A Contingency Plan

- Make a backup plan and keep it up to date.
- Include information technology in your list.
- This will require you to focus on data storage and security.
- Include everyone or a group.

This will increase awareness of the UK GDPR and the significance of compliance.

Consider solutions for backing up data so that normal service may be resumed.

- Having an encrypted external hard drive or USB drive that is regularly used to back up the main computer records is one option. This drive must then be securely stored.
- Think about employing a cloud storage system. You must ensure that the cloud provider you select has high levels of security, is compliant with the UK GDPR, and has UK data sovereignty. This signifies that the data is being stored in the United Kingdom.

Many of the major cloud providers have data centres in the United Kingdom.

How Do You Demonstrate UK GDPR Compliance?

You must provide paperwork to verify that you are in compliance with the UK GDPR.

Your computer could include a folder that contains all of your electronic files.

A ring binder could retain hard copies as well as minutes of UK GDPR meetings and employee GDPR training.

How Much Will It Cost?

Organisations that determine the purpose for which personal data is processed (controllers) must pay the ICO a data protection fee unless they are exempt.

What are the Three Payment Tiers?

In terms of costs, parliament has established three tiers:

- Tier 1 consists of micro-enterprises.

You have a maximum turnover of £632,000 for the fiscal year or no more than 10 employees. Tier 1 has a charge of £40.

- Tier 2 consists of small and medium-sized businesses.

You have a maximum annual turnover of £36 million and a staff of no more than 250 people. Tier 2 has a charge of £60.

- Tier 3 consists of major organisations.

If you do not match the criteria for tier 1 or tier 2, you must pay the £2,900 tier 3 cost. Unless and until they notify us otherwise, we consider all controllers to be entitled to pay a fee in tier 3.

Who is Exempt?

Not every controller is required to pay a charge.

If you solely process personal data for one (or more) of the following purposes, you do not have to pay a fee:

- Administration of personnel
- Public relations, advertising, and marketing
- Accounting and record keeping. Non-profit objectives
- Personal, familial, or domestic matters
- Keeping a public register
- Judicial duties
- Personal data processing without the use of an automated system, such as a computer

You can check your eligibility for payment by completing a self-assessment on the ICO website.

Let's clarify the paperwork you must prepare.

Documenting your processing activities is essential because:

- it is a legal requirement, so the documents can be made available upon request
- the documentation can show your compliance with the UK GDPR
- a lot of the information is similar to what you need to say in your privacy notice, so it can help you draught this
- knowing what personal data is held and where it is will help you respond to requests from people who would like access to their personal information.
- It will help you evaluate your own data protection practises, ensuring best practises, and it will help you make sure the personal data you retain is relevant, necessary, current, and safe.
- You will have a better understanding of the personal information you possess, its purpose, and its intended retention period.

What do controllers have to document?

if you are a controller for the personal data you process, you would need to document the following;

- The name and contact information for your organisation.
- The name and contact information of your data protection officer, who is responsible for assisting with UK GDPR compliance, if relevant.
- The name and contact information of any joint controllers, or any other organisations that determine why and how personal data is processed along with you, if relevant.
- The reasons for using personal data, such as customer management, marketing, or recruitment.
- The various categories of people—for example, employees, clients, and members—whose personal data is processed.
- The sorts of personal data you process - the various forms of information you process about people, such as contact information, financial information, and health data.
- Names of any third nations or foreign organisations that you may have transferred personal data to that are not in the EU.
- the security measures in place for rare transfers of personal data to foreign nations or entities, where applicable. As defined by the UK GDPR, an extraordinary transfer is a one-time, non-repetitive transfer of a limited group of individuals' personal data that is justified by a vital business requirement.
- The retention schedules for the various categories of personal data, indicating how long you plan to keep the data. For example, internal policies or standards established by the industry may determine this.
- An overview of your technical and organisational security measures, including your protections for protecting personal data

What do processors have to document?

- The organisations name and contact details
- The name and contact details of your data protection officer, a person designated to assist with UK GDPR compliance, if applicable
- The name and contact details of every controller you are acting on behalf of
- The name and contact details of your representative, which is another organisation who represents you if you are based outside the EU but offer services to people in the EU
- If applicable, the name and contact details of each controllers representative, which is another organisation that represents the controller if based outside the EU but offer services within the EU
- The categories of processing you carry out on behalf of each controller, the things you do with the personal data like payroll processing etc.
- The name of any third countries or international organisations that you transfer personal data to
- The safeguards in place for exceptional transfers of personal data to the EU, third countries or international organisations. An exceptional transfer us a non-repetitive transfer of a small number of peoples personal data
- A general description of your technical and security measures e.g. encryption training etc.

A Checklist

When aiming for compliance with the UK GDPR, "you will need to have audited all areas of your organisation, as you will have data in many places."

Once more, doing this as a team might be more thorough, involve everyone, and emphasise the significance of adhering to UK GDPR compliance.

The UK GDPR introduces a new requirement: documentation. You must provide proof.

Next Checklist from the ICO

Requirements for processing activity documentation

You keep all necessary records if you are the controller or processor of the personal data you process.

If you process data on criminal convictions and offences or special categories, you will document:

- the condition for processing you rely on in the Data Protection Bill
- the lawful basis for your processing
- whether you retain and erase the personal data in accordance with your policy document
- your processing activities in writing your processing activities in a granular way with meaningful links between the different pieces of information
- routine checks of the personal data you handle, and updating your records as necessary

Processing Activity Documentation

This might be included in your documentation.

When preparing to document your processing actions, you can perform the following:

- Conduct information audits to determine what personal data our company stores
- Disseminate questionnaires, and consult with employees throughout the organisation to gain
  a more complete picture of our processing activities
- Examine your rules, processes, contracts, and agreements to address issues like data retention, security, and sharing.
- Examine your rules, processes, contracts, and agreements to address issues like data retention, security, and sharing.

What should your UK GDPR Policy include?

Where relevant in connection to processing operations, measures shall include the controller's execution of suitable data protection policies.

Remember, a policy is:

- a high level document that states principles of practice not a document which deals with the how, what and when
- enforceable
- workable

The Six Principles

1. Lawfulness, Fairness, and Transparency - Personal data shall be treated lawfully (for a specific purpose), fairly (the process should be the same as indicated to the Data Subject), and transparently (the Data Subject is aware of the processing that will take place).

2. Purpose Limitation - The use of data must be clearly declared and limited to that use.

3. Data Minimization - Only necessary data should be stored.

4. Accuracy - Personal information must be correct and up to date. Procedures should be established to identify unnecessary data.

5. Storage Restrictions - Data should only be stored for the amount of time necessary for the purposes mentioned.

6. Integrity and Confidentiality - Data security must be maintained at all times.

Accountability - The Data Controller is accountable for the data and must be able to demonstrate compliance. When collecting, holding, and storing data, the Data Controller must demonstrate that all six principles are followed.

Data Collection

Data Sources - Where do you get your data?

Who is providing consent as a data subject?

Data Subject Notification - Data Subjects must be notified when their personal information is being utilised.

Data Utilisation

Data Processing - When and how do you process personal information?

Special Data Categories - The Data Subject must consent to the collection of this sensitive information.

Children's Data - Because children are unable to provide consent, it must be obtained from the person with parental responsibility. It is worth emphasising that if Data Processing is required by law, permission is not required.

Data Quality – Maintain data quality by keeping it correct and up to date.

Retention of Data

The setting will not keep data for any longer than is required for the chosen purpose.

Data Security - How will you safeguard the data?

- Prevent unauthorised access to personal information.
- Avoid loss and modification.
- The Data Processor follows instructions from the Data Controller.
- Data that is used for multiple reasons must be treated independently.

Data Subject Requests - Data Subject Rights are:

- information access
- data portability
- objection to processing
- data erasure
- objecting to automatic decision making
- profiling
- restriction of processing

Transfer of Data

The Data Subject must agree to the transmission of data.

Handling Complaints/Breach Reporting - A Data Subject may file a complaint with the Office of Data Protection.

Policy Retention:

Publication - Who can access this policy?

Effective Date - This policy goes into effect on.....

Revisions - Who will make changes to this document?

Questions

1. What is considered to be personal data?

- information about a person

- anonymised data

- a company email address

2. What does DPIA mean?

Data Protection Impact Assessment

Data Protection Initial Assessment

Data Protection Incident Assessment

3. What is the UK's supervising body for Data Protection?

The ICO

The OCR

The ACCA

4. Data subjects now have the right to have their personal data deleted, what is this known as?

The right to be forgotten

The right to change your name

The right to change data

5. If there's a data breach, how quickly should it be reported to authority?

Within 72 hours of the data breach

Within 24 hours of the data breach

Within 1 month of the data breach

6. To whom does the GDPR apply?

- Any and all organisations

- Anyone who is a UK passport holder

- Anyone over the age of 18

7. What is the penalty for DDPR breaches?

- Heavy fine

- A warning

- A police visit

8. Does everyone need a DPO (Data Protection Officer)?

- No, it's not compulsory

- Yes, everyone needs one

- Depends on the situation

9. When did the GDPR come into effect in UK law?

- May 2018

- January 2021

- December 2019

10. The UK GDPR requires you to…

- Demonstrate you follow and work with the documentation

- Agree to terms and conditions

- Read and sign