General Data Protection Regulation (GDPR) – Key Facts & FAQ's

GDPR comes into force on **25 May 2018**

- GDPR replaces the Data Protection Act 1998.
- The main principles are much the same as those in the current Data Protection Act 1998 (with the purpose of protecting personal data).
- The main changes focus on enforcing data protection laws more effectively in order to provide stronger consumer protection.
- GDPR puts the control of personal data back into the hands of the individual.
- It means that organisations need to carefully consider the reasons for gathering data, and only obtaining and storing the data they actually require.

GDPR Key Changes - Summary

Consent
For some processes, you can no longer assume you have consent. You will need explicit consent to collect, store and use personal data. You will also need to be able to evidence that consent has been gained.

Data use
You will require opt-in consent to use personal data in any other way than what it was originally intended. Do not be tempted to use personal data for anything other than its original purpose. If you would like to use information in a different way, you will need to obtain consent.

Right to erasure
Individuals have the right to request erasure or, right "to be forgotten" in limited circumstances. This may affect the way you process and store data and how long you retain data.

Clear unambiguous communications
Organisations will have to use clear wording in all communications throughout the customer journey.

Enforcement
It will be easier for consumers to make a complaint, making it straight forward for them to take legal action.

Stronger enforcement will be introduced with fines of up to £17 million (€20 million) or 4% of an organisation's annual turnover, whichever is the larger.

NOTTINGHAM TRENT UNIVERSITY

FAQ's

What is GDPR?

The General Data Protection Regulation will replace the Data Protection Act 1998 in the UK and across EU member states. The GDPR intends to create consistency and strengthen data protection principles and practices across the EU. The GDPR administers a more up to date law on data protection, with stronger emphasis placed on the rights of individuals and how their personal data is used within organisations.

When will GDPR become law?

GDPR will come into force in all EU nations on 25 May 2018

How will GDPR impact me?

GDPR will impact everyone that processes or controls data within an organisation across the world. The GDPR has an extraterritorial effect, so non-EU countries will also be affected. For example if a UK company process data in the UK about an American citizen then it will need to comply with GDPR. Alternatively, if an American company processes data in the USA about UK citizens, then it will also need to comply with GDPR.

On a personal level, all individuals will have more control and rights over their data and how it is used.

What are the implications of the UK leaving the European Union?

Although the UK is intending to exit the EU within the next few years, the GDPR will still have an impact and the UK will still need to comply with the GDPR.

What are the GDPR Principles?

These principles underpin the GDPR, and set out the conditions for processing personal data:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. 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."

What is Personal Data?

Personal Data, or personal information, means any information about an individual from which that person (a "Data Subject") can be identified. It does not include data where the identity has been removed (anonymous data). Information will fall under the category of Personal Data if a person can be identified either directly or indirectly, in particular by

reference to an identifier such as a name, an identification number, location data, an online identifier or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. For example personal data may include names, addresses, email addresses and telephone numbers; it may also include images in photographs or video recordings and recorded telephone conversations.

What is Special Category / Sensitive Personal Data?

GDPR defines certain information as Special Category Data, which has a specific set of rules around which this can be processed, this includes data such as:

- Trade Union membership
- Racial or ethnic origin
- Political opinions or religious beliefs
- Sexual orientation
- Physical or mental health
- Genetic or biometric data

What is Data Processing?

Processing means any operation or set of operations performed on personal data or on sets of personal data which includes using, viewing and storing personal data.

What is the difference between a Data Controller and a Data Processor?

- A Data Controller determines the purposes and means of processing personal data.
- A Data Processor is responsible for processing personal data on behalf of a Data Controller.

What are the conditions for lawful processing of personal data?

- The data subject has given consent to the processing of their data.
- Processing is necessary for the performance of a contract with the data subject.
- Processing is required for compliance with a legal obligation.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or a third party, except where such interests are overridden by the interests or rights and freedoms of the data subject

What are the new requirements for consent?

GDPR sets a much higher standard for an individual to give consent over how organisations use their personal data. The key elements of consent are:

- Consent should be given freely, be specific, informed and unambiguous.
- Consent requires a positive “opt in”, the use of pre-ticked boxes or default consent is not allowed.
- The data subject will have the right to withdraw consent at any time.
- Consent must be clear and concise, and separate from other terms and conditions.
- Evidence of consent must be retained. You should retain, who, when, how and what you told individuals, and it should be reviewed regularly.

What are a Data Subjects Rights?

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- **Request correction** of the personal information that we hold about you. This enables you to ask us to correct any incomplete or inaccurate information we hold about you.

- **Request erasure** of your personal information in limited circumstances. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- **Object to processing** of your personal information where we are processing your personal information on the basis of our legitimate interest (or that of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction or suspension of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Object to any direct marketing** (for example, email marketing or phone calls) by us, and to require us to stop such marketing.

- **Object to any automated decision-making** about you which produces legal effects or otherwise significantly affects you.

- **Request the transfer** of your personal information to another party.

What is a Data Protection Officer (DPO)?

The appointment of a DPO under the EU General Data Protection Regulation (GDPR) is only mandatory in the following situations:

- when the organisation is a public authority or body, or
- when the organisation's core activities consist of either; (1) regular and systematic monitoring of data subjects on a large scale; or (2) Large-scale processing of special categories of data.

The GDPR requires that the DPO operates independently and without instruction from their employer over the way they carry out their tasks.

What is Data Protection by Design?

Data Protection by Design is an approach to projects, where privacy and data protection risks are identified at the start of any project which includes the use of personal data.

What is a Data Privacy Impact Assessment (DPIA)?

A DPIA is a process that will enable you to identify data protection risks within any project that uses/processes personal data, and will make you aware of any safeguards that you may need to put into place to eliminate/minimise those risks. A DPIA must be used where a project/system outcome is likely to result in a high risk to an individual's interests. DPIAs must be signed off/approved by the DPO.

What is a Data Breach?

A Data Breach is defined 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".

How do I report a data breach?

Any incident or breach concerning personal data should be escalated to the DPO, as soon as possible and within 24 hours of the incident/breach coming to your attention.

GDPR required that data incidents/breaches must be notified to the ICO within 72 hours, and must include details of the data subject and whether the breach might pose a high risk to their rights and freedoms.

What are the penalties for non-compliance under GDPR?

Violations regarding record-keeping, security, breach notification, and privacy impact assessment obligations, can result in a penalty of up to €10 million or 2% of global gross revenue, whichever is greater.

More serious violations related to lawful processing of personal data such as consent, data subject rights and cross-border data transfers, can result in a penalty of up to €20 million or 4% of global gross revenue.

What does Pseudonymisation mean?

This means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, providing that such information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identifiable natural person. For example removing the names of individuals and providing a code for identification – only the person with the key can identify the individuals directly.

What about processing children's data?

The processing of the personal data of a child shall be lawful where the child is at least 13 years old. Where the child is below the age of 13 years, processing must only be carried out when consent is given or authorised by the holder of parental responsibility over the child.

Who should I contact if I have a Data Protection Query?

The Data Protection Officer (DPO) or the Legal Services Team on DPO@ntu.ac.uk