

GDPR YOUR DATA PROTECTION RIGHTS

Tech & Tea Seminar
By CommuniTech



General Data
Protection Regulation

OUTLINE

- ❖ What is GDPR
- ❖ Brief history behind GDPR
- ❖ What GDPR means for organisations
- ❖ What GDPR means for you
- ❖ Explicit consent
- ❖ Privacy by Design
- ❖ The right to be forgotten
- ❖ What about Brexit



What is GDPR

- ❖ GDPR = General Data Protection Regulation
- ❖ It is a REGULATION and not a DIRECTIVE
- ❖ It means you have greater control over who does what with your personal data
- ❖ It aims to protect your privacy and data
- ❖ It applies to all EU citizens – even to companies outside the borders of the Union

Types of data

- ❖ Name
- ❖ Physical and email address
- ❖ Social media posts
- ❖ Medical history and records
- ❖ IP addresses
- ❖ Bank details
- ❖ Photos and images
- ❖ Minor [under 16] need parental consent for data processing



Brief history behind GDPR

1995 EU Data Protection Directive

1998 UK Data Protection Act (DPA)

2013 European Commission makes a proposal for an updated data protection

2014 European Parliament approves first draft of regulation

2015 Council of European Union approves first draft

2016 Approval and Adoption

2016 – 2018 Period of grace

25 May 2018 – GDPR is enforced across all EU Member States

What GDPR means for organisations

- ❖ Must obtain explicit consent
- ❖ Must keep your data only for as long as necessary
- ❖ Must keep a record of all data processing transactions
- ❖ Must be able to produce a data audit trail
- ❖ Must store your data securely and safely
- ❖ Must report any data breaches to the Information Commissioner's Office [ICO] within 72 hours and take other steps

What GDPR means for you

- ❖ Greater privacy and more control
- ❖ Explicit consent
- ❖ Privacy by Design
- ❖ The right to be forgotten
- ❖ No marketing spam, unsolicited calls, or marketing emails
- ❖ Organisations will be mindful and cautious when requesting your data

Explicit consent

Explicit consent means exactly that: consent must be objectively and unambiguously obtained. The reasons for requesting your data must be clear.

Consent cannot be:

- ❖ Hidden or buried in text
- ❖ A pre-ticked box
- ❖ For more than one specific type of data



Privacy by Design

All organisations processing personal data must implement Privacy by Design into the entire lifecycle of the data. This means:

- ❖ Obtaining explicit consent and keeping a record of agreement
- ❖ Knowing where the data is at all times
- ❖ Only providing access on a 'need to have' basis
- ❖ Data retention only for as long as necessary
- ❖ Informing you of any changes regarding the use of your data and getting consent
- ❖ Reporting serious data compromise in 72 hours

The right to be forgotten

You can ask an organisation to stop processing and storing your data. They will also have to delete all traces of your data and provide evidence of this. The right to be forgotten means:

- ❖ Companies have to comply within 30 days
- ❖ Companies must clearly show the right to be forgotten when getting consent
- ❖ There are some exceptions – the right to exercise freedom of expression, legal obligations, public interest obligations, public health purposes and to defend legal claims

Non-compliance and positives

Non-compliance

- ❖ 20 million euros or 4% of net annual turnover
- ❖ Bad news for Facebook

Positives

- ❖ You enjoy better data protection
- ❖ Compliant companies develop a reputation of being trustworthy and reliable



GDPR and Brexit

No difference. The UK DPA has been replaced by the GDPR.

Following Brexit, the same laws will apply as today but under a different name; probably not using the term 'regulation'.

