

GDPR Credo



In a nutshell

Stands for '**General Data Protection Regulation**'

The **biggest change** to **data protection** in 20 years

Effective from the **25th May 2018**

Will be taking place of the **Data Protection Act**



Purpose

The aim is to provide stronger protection to people's personal data
Gives people more control and more rights

It protects even more people - now all EU citizens

Even if your organisation is outside of Europe, if you deal with EU citizens' data, you're included



Data Breaches & Fines

A breach is any misuse of personal information, including loss, sharing and alteration of data

Any data breaches now must be reported to the supervisory authority within 72 hours

Not complying with the GDPR can cost your company €20 million, or 4% of your annual global turnover



More Protection

People have much more rights, including the 'right to erasure' – which deletes their information permanently

Only in very certain circumstances, you can say no

All subject access requests must be dealt within a month

Other rights include right of access, right to be informed, rectification, portability, right to object, and rights in relation to profiling



Data Protection Officers

There to make sure everything you do is GDPR compliant

Actions they will undertake include carrying out Data Protection Impact Assessments (DPIA)

They check everything is above board, assessing that the information being collected respects the GDPR (i.e., including potentially managing subject access & deletion requests)



Data Protection Principles Six Core Principles:

1. Purpose Limitation
2. Lawfulness, fairness & transparency
3. Accuracy
4. Integrity & Confidentiality
5. Data minimisation
6. Storage Limitation



GDPR is around the corner: Are you ready?

Spread awareness in your company

Find out where your data came from and who you share it with

Start checking that your procedures line up to the GDPR, like the way you delete people's data and the lawful basis for your processing activity

Potentially re-think some policies: like gaining parental consent for underage people, and how you process privacy related requests from individuals