What is GDPR?

- The General Data Protection Regulation (GDPR) was developed with a focus on social media and cloud providers, but will affect all organisations (controllers or processors) that handle personal data of European individuals
- The aim is to strengthen and unify data protection to give control back to individuals
- It will replace the 1998 Data Protection Act from the 25th May 2018

Is it different to Data Protection?

- Same basic principles as current data protection law, but strengthened
- There is more emphasis on accountability
- New rights for individuals, and strengthening of existing rights
- Mandatory Breach reporting
- Data Protection Impact Assessment when building new systems

What are the implications?

Individuals will have –

- The right to access
- The right to be forgotten
- The right to data portability
- The right to be informed
- The right to have information corrected
- The right to restrict processing
- The right to object
- The right to be notified

For the OPCC this will mean that we have to identify what personal data is held, where it came from, who it has been shared with, how accurate is it and what do you need to keep?

We have also reviewed our Fair Processing Statement which sets out how we as an office handle personal data. We have also updated our contact form on the internet

We can no longer charge £10 for subject access requests and it is estimated there could be a 30% increase. However in nearly six years we have only received two!

What are our responsibilities?

To state the obvious, our main responsibility is to ensure we are not in breach of the regulation. The Governance Team have undertaken an audit of the information we hold and the vast majority is held by the team in the form of casework and correspondence. We are currently deleting and destroying data that is no longer needed and I would urge you all to review what personal data you currently hold, where it came from, who you share it with, how secure it is, and whether you need to keep it.

Most data breaches occur due to human error or poor data security we need to keep under review manual and electronic files, folders, drawers, cabinets, walls, emails, notebooks, etc to ensure that we are not holding or displaying personal data in breach of the act.

The simple act of leaving your screen unlocked could lead to the OPCC being in breach of the GDPR. So be on your guard!

What do we do if it goes wrong?

Any data breach MUST be reported within 72 hours to the ICO. We have now have an online form to report any breach which will then go to the Chief Executive and the Data Protection Officer to consider what action needs to be taken. For example, a breach within the 'policing family' could be effectively dealt with without a referral to the ICO. However it is vital that it is still reported and all actions are recorded. However any breach to an outside organisation or individual must be reported.

Non-compliance can lead to fines of up to 20,000,000 euros or 4% of annual turnover.

However, for the Public Sector that figure reduces to €9,000,000 or approximately £8.5m.

As a small organisation, the GDPR should not have a huge impact on our business. We need to ensure that we treat personal data carefully and with common sense. If in doubt ask and keep what you hold under review.

The Big Picture

Key changes of the GDPR

Fines of up to 4% of annual global turnover

€'000 → **€'000,000**

Previously fines were limited in size and impact. GDPR fines will apply to both controllers and processors.

Increased territorial scope

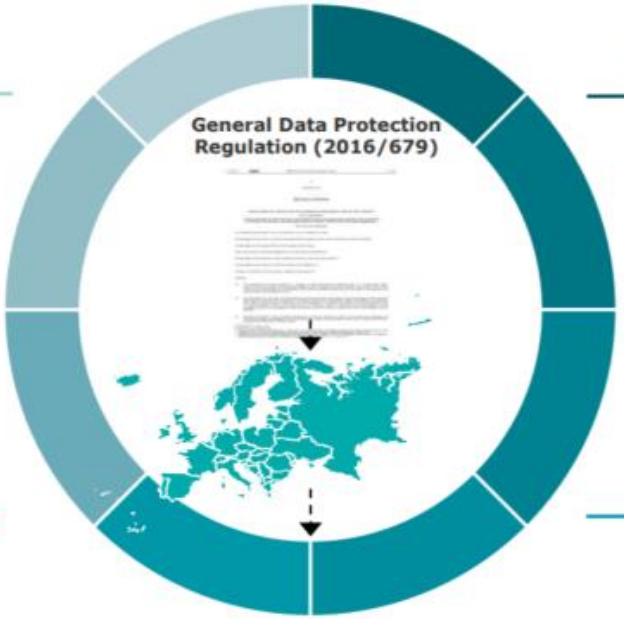
GDPR will apply to all companies processing the personal data of data subjects residing in the EU, regardless of the company's location.

Explicit and retractable consent

Must be provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Right to access and portability

Data subjects can request confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format.



Breach notification within 72 hours

Now mandatory that breaches, which are likely to "result in a risk for the rights and freedoms of individuals", are reported within 72 hours of first having become aware of the breach.

Privacy By Design

Now a legal requirement for the inclusion of data protection from the onset of the designing of systems, rather than a retrospective addition.

Right to be forgotten

Entitles the data subject to have the data controller erase his/ her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.

Mandatory Data Protection Officers

Appointed in certain cases (public authorities, when monitoring of data subjects on a large scale and when processing special categories of data). To facilitate the need for a company to demonstrate their compliance to the GDPR and compensate for GDPR no longer requiring the bureaucratic submission of notifications/ registrations of data processing activities or transfers based on Model Contract Clauses.