General Data Protection Regulation

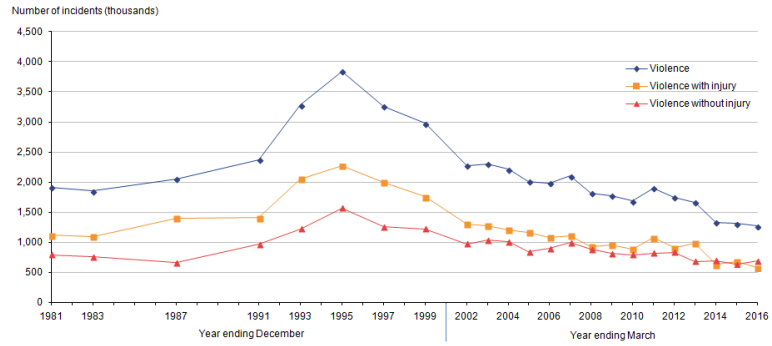
What is it?

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a Regulation by which the European Commission intends to strengthen and unify data protection for individuals within the European Union (EU). It also addresses export of personal data outside the EU. - Wikipedia

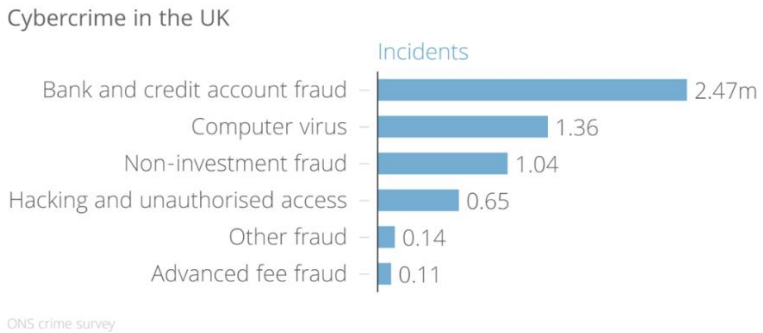
EU GDPR covers *personal* data.
Think names, addresses, phone numbers, account numbers, and more recently email and IP addresses.

Why do we need GDPR?

Traditional crime rates are dropping as the police become more efficient at detection and prevention. Figures from gov.uk



According to ONS (2017) modern criminals are switching to Cybercrime as a way to continue with their unlawful ways!



In addition, many businesses have networks that are home grown and not set up by experts. The IT industry doesn't yet have much regulation and so it's possible that local IT providers don't appreciate how to make best use of modern security features. The outcome is poorly set up networks with low security. These are prone to virus and direct attack.

Businesses now mainly rely on electronic data rather than paper copy. Electronic data is far easier to replicate and its becoming more difficult to detect that data has been accessed.

We have all heard stories of fraud, especially where elderly is concerned. The fraudsters first have to get a list of contacts to attack. These lists are the result of data theft.

The result is that the world needs to protect the innocent by ensuring that anybody who is storing data does so in a responsible way. Hence the birth of GDPR.

Many people will tell you that GDPR is a bad thing that will stop you from doing business. This simply isn't true. As long as you do some basic things then you can continue contacting customers and selling.

The differences from previous requirements.

- **Privacy by Design**
  Privacy by Design (PbD) has always played a part in EU data regulations. By with the new law, its principles of minimizing data collection and retention and gaining consent from consumers when processing data are more explicitly formalized.

- **Data Protection Impact Assessments (DPIA)**
  When certain data associated with subjects is to be processed, companies will have to first analyze the risks to their privacy. This is another new requirement in the regulation.

- **Right to Erasure and To Be Forgotten**
  There's been a long-standing requirement in the DPD allowing consumers to request that their data be deleted. The GDPR extends this right to include data published on the web. This is the still controversial right to stay out of the public view and "be forgotten".

- **Extraterritoriality**
  The new principle of extraterritoriality in the GDPR says that even if a company doesn't have a physical presence in the EU but collects data about EU data subjects — for example, through a web site—then all the requirements of GDPR are in effect. In other words, the new law will extend outside the EU. This will especially affect e-commerce companies and other cloud businesses.

- **Breach notification**
  A new requirement not in the existing DPD is that companies will have to notify data authorities within 72 hours after a breach of personal data has been discovered. Data subjects will also have to notified but only if the data poses a "high risk to their rights and freedoms".

- **Fines**
  The GDPR has a tiered penalty structure that will take a large bite out of offender's funds. More serious infringements can merit a fine of up to 4% of a company's global revenue. This can include violations of basic principles related to data security — especially PbD principles. A lesser fine of up to 2% of global revenue — still enormous — can be issued if company records are not in order or a supervising authority and data subjects are not notified after a breach. This makes breach notification oversights a serious and expensive offense.

Overall, the message for companies that fall under the GDPR is that awareness of your data—where is sensitive data stored, who's accessing it, and who should be accessing it—will now become even more critical.

When does it come into effect?

The GDPR comes into effect 25th May 2018. Many people have suggested that Brexit will mean we don't have to comply, however it will be in effect before we leave the EU and so we have to comply from the start!

Although our own paper has not yet been fully processed by Parliament, the UK equivalent of GDPR will be identical and so we simply need to be ready from day one!

What do I have to do?

- Get Permission to use data
  There are two ways to gain permission:
  - Vested interest
    A customer contacts and asks you to do something. You obviously need to be able to re contact them to complete any work. There is a vested interest for both of you to be able to communicate. You don't need to specifically ask permission just so long as you understand that you have the details for this purpose.
  - Ask for permission
    You want to change how you are using data, or you are using fresh data that you have not been given directly by the contact IE a mailing list.
    In this situation you will have to contact the individual to gain permission to contact them in future.

- Tidy up data
  Make sure that you understand what data you are holding and that its in a secure environment.
  If data is not needed for every day work, then store it in a different location that is more secure. As an example, store staff personal details in a different location to customer personal details.

- Make office secure for data
  Don't have removable media left on desks, easy access to PC's or server in public areas of the business.

- Work out what personal data you hold and how you use it.
  This means that if you obtained information for one purpose, don't start to use it for a different one unless you can justify it and also have sufficient background details so you can assess any impact from the change.

- Document and share processes
  Make sure that your staff all use data in a consistent way, and that the process and understanding of how data should be used is shared.
- Have a method to request a copy of personal data and also a method to "Opt Out"
  When an individual requests a copy of their data you must respond within 30 days. This means you need an easy way for the individual to contact you and also have a person responsible for processing the request. Consider adding an alias email address to make sure that all requests go to the best person.
  The same is tru for an individual who wants to "opt out" or request that you no longer hold personal data about them.

- Age data.
  Make sure that you review data regularly and destroy data that you no longer need.

- Register with ICO
  All Limited companies based in the UK must register with the ICO.
  https://ico.org.uk/for-organisations/register/

Practical steps – Andisa

- **Mapped and Cleansed data**
  We have broken our business down into sectors – Internal Admin, Customer support / consultancy and Hosting. We then worked out where we use and store data about individuals.
  If its given to third parties we made sure there were GDPR statements and contracts in place.
  We deleted old data and updated current data.
  We have made sure that customer data is stored in the same format and similar location for all customers.

- **Appointed a data controller.**
  Although this step was not compulsory for our size of business we decided that our data use is complex enough that it would be helpful if somebody central understood the rules and also our procedures for data management.

- **Adding a public process to request data and opt out.**

- **Set up different Wifi for internal systems, public areas and test systems.**

- **Physically moved equipment out of the public office.**

- **Added extra network for pure internal use.**
  This was better than adding a public network because the new network was designed to be secure, so we moved internal to a new network.

- **Scanned the network and scheduled to do this annually.**
  This is a step that audits the network regularly and spots potential problems.

- **Added DP and security to regular staff meeting and board agendas.**
  We decided that it would be a good idea to share the problems will all staff.
- **Scheduled updates on all software.**

- **Improved VPN access through Radius and group policy**
  Radius gives a simpler way to manage passwords and network access. We can now control not only who, but when and from where staff can access our network.

- **Decided to apply for CyberEssentials certification and used it as a USP**

- **Published a simple public statement of how we implement GDPR**

Summary

- Be pragmatic – it doesn't have to cost as long as you give proper respect.
- Be prepared – there is a game being played and the "GDPR police" will look for low fruit
- Be fair – treat customers as you would expect to be treated
- Understand your data. If you consider it then it becomes easy.