



CLEMENCE HOAR CUMMINGS
CHARTERED ACCOUNTANTS AND BUSINESS ADVISORS



Guide to GDPR

What is the General Data Protection Regulation?

The General Data Protection Regulation (GDPR), is a new legal framework being introduced for all EU member states in May 2018. It will replace the existing UK Data Protection Act (DPA) with tighter laws and tougher penalties for organisations who fail to comply.

The key differences are found in how data is stored and used. Companies will be forced to maintain records of 'consent', and consumers will be gifted the right to be 'forgotten'.

Why does it matter?

The penalties for non-compliance are tough. Really tough. The Information Commissioner's Office (ICO) can issue fines of up to four per cent of global turnover, or €20 million, whichever is higher.

Comparatively, current rules mean ICO has the power to charge a maximum of £500,000. And there are more than just financial penalties if winning the trust of your customers is key to your business. A potential breach could cause irreparable reputational damage to any organisation.



What information does GDPR apply to?

All 'personal' data is protected by GDPR. That includes online and offline identifiers, such as IP addresses and phone numbers. As a general rule of thumb, any information which falls within the scope of the DPA, will also fall within the scope of the GDPR.

The key terms

Data Subject – a living individual to whom personal data relates.

Data Controller – a person who determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data Processor – a person who acts on the Controller's behalf.

Personal data – any information relating to an identified or identifiable natural person (Data Subject), such as a name, identification number, location data, or online identifier (such as an IP address).

Sensitive personal data – data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or data concerning health or sex life.

Personal Data Breach – a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The six commandments of GDPR

- I Processed lawfully, fairly and in a transparent manner in relation to individuals.

For processing to be deemed 'lawful', you need to identify a lawful basis to process personal data. You must document all interactions with the data, including how, when, and where you obtained it, and how consent was agreed. Pre-ticked consent boxes are not deemed 'transparent' under GDPR.

- II 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.

Data stored should be used for the purpose you initially stored it for, and should not be used to benefit your organisation in any further endeavours. For example, if your data subject gave consent to receive email marketing, they should not be contacted via telephone or post.

- III Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Personal data held should be no more revealing than necessary to fulfil its specified, explicit, and legitimate purpose.

- IV Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay.

- V 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.

Data should be deleted as soon as it is no longer necessary to achieve the specified purpose. For example, a competition entrant who did not consent to receive further email marketing.

- VI 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.





The penalties

The current penalties pale in comparison to what can be issued under GDPR.

As of 25 May 2018, any business that fails to comply faces the following fines:

Tier 1 – if a data breach puts ‘highly important’ data at risk

Fines of up to 20 million euros or four per cent of the previous year’s global annual turnover, dependent on which figure is greater.

Tier 2 – any other data breach

Fines of up to 10 million euros or two per cent of the previous year’s global annual turnover, dependent on which figure is greater. To put these fines into perspective, the new penalties are around 20 times higher under GDPR. That means ICO could have collected £122 billion in fines if GDPR was law in 2015 (based on Tier 1 data breaches).

Don't be like them

Most significant data breaches in history:

1. Yahoo (2013, 2014). 1.5 billion customers affected. Personal data and security questions leaked in data breach. Yahoo is now facing numerous lawsuits after failing to disclose the breach sooner.
2. Zomato (2017). 17 million customers affected. Email addresses and passwords stolen in cyberattack.
3. TalkTalk (2015). Four million customers affected. Hackers exploited weakness in firm's website to steal personal records.

TalkTalk was fined £400,000 and lost more than 90,000 customers as a direct result of the data breach.
4. Moonpig (2015). Three million people affected. Software flaw in firm's android app let a researcher access the records of any Moonpig account holder.
5. Bupa (2017). 500,000 customers affected. Employee inappropriately copied and removed information including names, dates of birth and contact information.

A close-up photograph of a hand's index finger pressing a circular button. The button has a glowing blue ring around its edge. The text 'STOP / START' is embossed on the top half of the button's face. In the center of the button is a black circle containing a white arrow pointing upwards and to the right, with the words 'DISASTER RECOVERY PLAN' written in white, bold, sans-serif capital letters below it. The background is a dark blue, textured surface.

Offence is the best defence

From employee blunders to cyber-attacks, a potential data breach can happen at every level of your business. That's why preparation and due-diligence will be your first line of defence in protecting your customers' data.

Where are your weaknesses?

1 Cybersecurity

Almost half of UK companies identified a cyber breach or attack in the past 12 months, according to gov.uk, with those holding personal data more likely to be attacked than those which do not. The most common breaches or attacks were via fraudulent emails, followed by viruses and malware. However, almost all of these attacks could have been prevented using the Government-backed Cyber Essentials Scheme.

2 Employees

Your workforce, who represents your business, needs to understand the significance and risks of breaching GDPR. Without the right training, an employee could unwittingly hold the door open to a cyber-attack or disclose personal data. You should consider additional training in cybersecurity, confidential waste destruction, and data protection best practice.

3 Internal processes

The way you handle and process data may be your biggest vulnerability. To comply with the law, your business will need to keep a rigid record of how, when, and why stored data was used. You must also delete and update data where necessary. Consider appointing a data officer to oversee all data-related operations.



GDPR Dos and Don'ts

Do - maintain a record of how, where, and why consent was obtained.

Do - delete personal data when a customer exercises his or her right to be forgotten.

Do - report a breach to the relevant authority and affected.


Do - inform your employees about cybersecurity best practice.

Don't - use consent by default to store data.

Don't - further process data in a manner that is incompatible with its original purpose.

Don't - leave more than 72 hours to report it.

Don't - wait for GDPR to come to you. Seek assistance now.



GDPR redefines and sets a new standard for consent. It's all about the customer wanting to give his or her information away, and less about marketing trickery. As a result, consent requires a positive opt-in, spelling the end for pre-ticked check boxes or any other method of consent by default.

Neither should consent be a precondition of using a service. Request for consent should be explicit, in that it is separate from your terms and conditions, is clear and specific, and any relevant third party organisations are named.

Blanket consent is not enough. Remember, make a record of how, when, and where consent was given.

To recap consent is:

- Actively given ✓
- Explicit ✓
- Specific ✓
- Unbundled ✓
- Documented ✓

The ICO checklist for consent

Asking for consent

- We have checked that consent is the most appropriate lawful basis for processing.
- We have made the request for consent prominent and separate from our terms and conditions.
- We ask people to positively opt in.
- We don't use pre-ticked boxes, or any other type of consent by default.
- We use clear, plain language that is easy to understand.
- We specify why we want the data and what we're going to do with it.
- We give granular options to consent to independent processing operations.
- We have named our organisation and any third parties.
- We tell individuals they can withdraw their consent.
- We ensure that the individual can refuse to consent without detriment.
- We don't make consent a precondition of a service.
- If we offer online services directly to children, we only seek consent if we have age-verification and parental-consent measures in place.

Attribution: Information Commissioner's Office, GDPR consent guidance, licensed under the Open Government License.

The customers' right to be forgotten

Also known as the right to erasure, customers have a right to request that their data is deleted permanently should there be no compelling reason for its continued processing.

When should data be “forgotten”?

- When a customer has requested erasure;

and

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed; or
- When the individual withdraws consent; or
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.

Under certain circumstances, a company can refuse to erase data. For example, it could continue to use the information to:

- Exercise the right of freedom of expression and information
- Comply with a legal obligation or for the performance of a public interest task or exercise of official authority
- Support legal claims
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific, historical, or statistical.

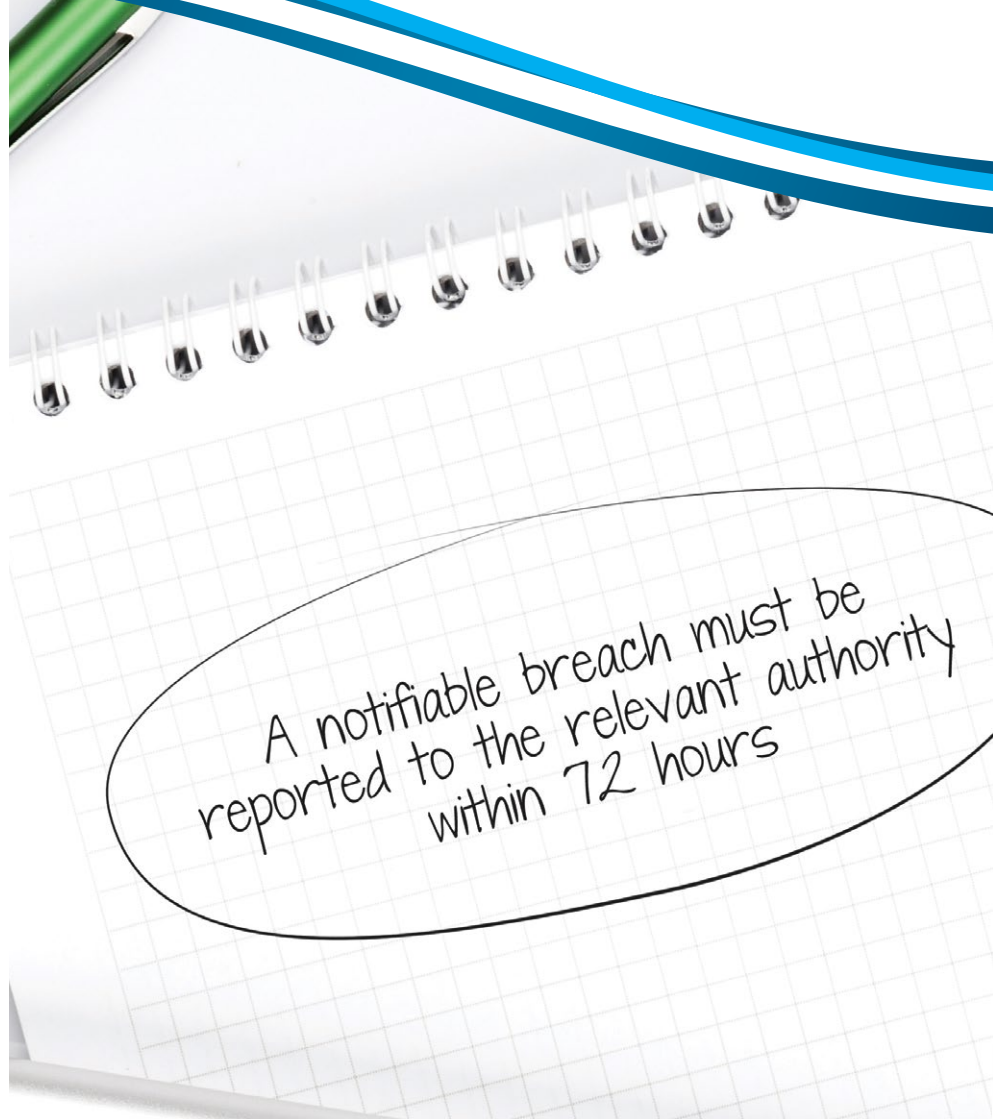


GDPR requires all organisations to report certain types of data breach to the relevant authority and individuals affected.

The breach must be reported if it will have a significant detrimental effect on individuals.

For example, a breach that could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage will need to be reported.

A notifiable breach must be reported to the relevant authority within 72 hours of the organisation becoming aware of it. If warranted, the public must be notified immediately.





Clemence Hoar Cummings
1 - 5 Como Street,
Romford, Essex,
RM7 7DN

T: 01708 333300
E: info@chc.uk.com
W: www.chc.uk.com

