DYNAMIC hr

GDPR (General Data Protection Regulation) **Guide**

What you need to know

This guide is for general information purposes only and does not constitute legal, or other professional advice. We would advise you to seek professional advice before acting on this information.

Contents Page

What is the EU General Data Protection Regulation (GDPR)?

The GDPR is an evolution of the EU's existing data rules, the Data Protection Directive (DPD) which is implemented in the UK through the Data Protection Act 1998.

The GDPR harmonises data protection laws across the EU and updates the current 20-year-old regime to take account of globalisation and the ever-changing technology landscape.

The GDPR has new requirements for documenting IT procedures, performing risk assessments, rules on breach notifications and tighter data minimisation – establishing a single law to enforce data protection rules and regulation and the right to personal data protection.

It legislates common sense data security protocols including:

- Minimising collection of personal data
- Deleting of personal data that's no longer necessary
- Restricting access, and
- Securing data through its entire lifecycle.

What type of data is protected?

Personal data such as names, addresses, telephone numbers, account numbers, email and IP addresses.

Who does it affect?

The GDPR applies to EU based companies and companies that collect data of EU citizens, regardless of their physical presence in the country.

How does it affect you?

It means there are new regulations and requirements for collecting, recording, and storing personal data and processing activities, new regulations on breach notifications, penalties on violations, and more.

What are the new requirements?

Privacy by Design – The GDPR has formalised principles of Privacy by Design (PbD) into their regulations including minimising data collection and retention, and gaining consent from consumers when processing data.

Data Protection Impact Assessments (DPIA) – Companies will have to first analyse the risks to their privacy when certain high-risk or sensitive data associated with subjects is to be processed.

The Right 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.

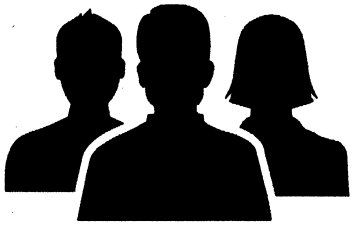
Extraterritoriality – Even if a company doesn't have a physical presence in the EU but collects data about EU data subjects (through a website, for example) then all the requirements of GDPR are in effect. In other words, the new law will extend outside the EU. This will especially affect e-commerce companies and other cloud-based businesses. Businesses can no longer store data in a non-EU country and avoid the data protection laws!

Breach Notification – 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 be notified but only if the data poses a "high risk to their rights and freedoms".

Fines – Serious infringements can merit a fine of up to 4% of a company's global revenue. These infringements can include violations of basic principles related to data security – especially Privacy by Design principles. A lesser fine of up to 2% of global revenue can be issued if company records are not in order, or if the supervising authority and data subjects are not notified after a breach.

GDPR highlights that awareness of your data— where sensitive data is stored, who's accessing it, and who should be accessing it— is now more critical than ever.



GDPR – Privacy by Design

Privacy by Design (PbD) is a well-intentioned set of principles to get company bosses to take consumer and employee data privacy and security more seriously.

Overall, PbD is a good idea and you should try to abide by it.

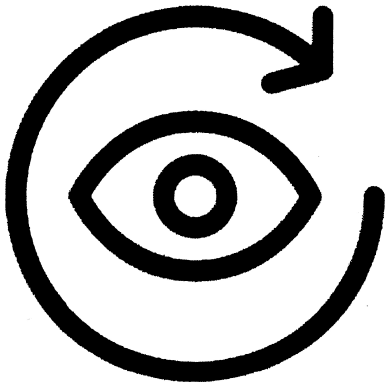
But with the General Data Protection Regulation (GDPR), it's more than that, it's the law if you do business in the EU zone!

Privacy by Design sets out good general advice on data security that can be summarised in one word: **minimise**!

In essence, minimise collection of consumer and employee data, minimise who you share the data with, and minimise how long you keep it.

Less is more: less data for the hacker to take means a more secure environment.

If you implement Privacy by Design into your working practices, you are well on your way to mastering the GDPR.



What about big data?

Big data is an evolving term that describes any voluminous amount of structured, semi-structured and unstructured data that has the potential to be mined for information.

Often used to enhance decision making, provide insight and discovery as well as support and optimise processes.

The burning questions is; can big data and privacy live together happily ever after?

Privacy by Design suggests yes as long as you stick to the following rules:

- Minimise data collected (especially personal information) from consumers and employees
- Do not retain personal data beyond its original purpose
- Give consumers and employees access and ownership of their data

The Right to Be Forgotten

Probably the most controversial part of the new laws is the "right to be forgotten".

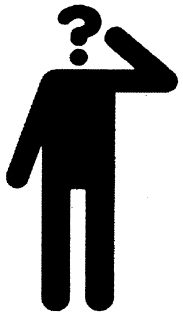
For most companies, this is really a right for consumers to erase their data.

The GDPR has strengthened existing rules on deletion and then adds the right to be forgotten.

There's now language that would force the controller to take reasonable steps to inform third-parties of a request to have information deleted.

Discussed in Article 17 of the GDPR, it states that:

"The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where ... the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; ... the data subject withdraws consent on which the processing is based ... the controller has made the personal data public and is obliged ... to erase the personal data".



The Key Lesson

The consumer or data subject can make a request to erase the data held by companies at any time.

Third Parties

What if the data controller gives personal data to other third-parties, such as a cloud-based service for storage or processing?

The regulations still apply: as data processors, that cloud service will also have to erase the personal data when asked to by the controller.