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.

Extraterritoriality

What the ….?!

One of the more complex issues with the new GDPR is what's being called "extraterritoriality". Under Article 3 the GDPR will apply to any personal data transferred outside the EU/UK zone.

Under these new rules, if any company collects data from EU/UK citizens, it will be under the same legal obligations as a company within the EU/UK zone even if they don't have any servers or offices there! This is most likely to affect US companies.

Extraterritoriality is particularly relevant to core web services such as search, social networking, e-commerce etc.

WARNING!

Under the old rules in the Data Protection Directive there was some wiggle room that allowed data collectors to escape having to follow the regulations. A common practice was for service or app providers to keep their data processing outside the EU.

The idea was that if the main processing and servers weren't located in the EU zone, then the rules didn't apply. Companies such as Google, Facebook, and other social networking companies were following this approach.

This will no longer be possible! You have been warned!

The Bad News ….

What Happens if I Don't Comply with the GDPR rules?

The GDPR has a tiered penalty structure. Remember that GDPR rules apply to both data controllers and processors.

Non-compliance results in fines of up to 4% of global revenue.

A company can be fined up to 2% of global revenue for not having their records in order (article 30), not notifying the supervising authority and data subject about a breach (articles 33, 34), or not conducting impact assessments (article 33).

And keep in mind, the GDPR breach notification (which has to be done within 72 hours of the breach) requires more than just saying you have had an incident.

You'll have to include categories of data, records touched and approximate number of data subjects affected.

More serious infringements merit up to a 4% fine of global revenue. These infringements include violations of basic principles related to data security (article 5) and conditions for consumer consent (article 7) and violations of the core Privacy by Design concepts of the law.

Data Protection Officers

The GDPR regulators (in the case of the UK, this is the Information Commissioner's Office) are hoping to keep everything in line by requiring companies to have a Data Protection Officer (DPO).

The DPO should be responsible for creating access controls, reducing risk, ensuring compliance, responding to requests, reporting breaches within 72 hours, and creating a strong data security policy.

The DPO is an optional requirement for businesses with fewer than 250 employees however, they do need a named person with overall responsibility for data protection.

Employee Data

Currently, many employees will only have a brief clause in their employment contract, giving "consent" for the employer to hold and process their personal data.

Under GDPR this will need a complete overhaul. It will become much harder to rely on employee's "consent" as a valid reason to hold and process data - consent will have to be informed, freely given, specific and unambiguously shown. Privacy Notices will become necessary.

Employees will have much greater rights, including increased rights to object to certain processing and the right to be forgotten, to have data corrected and to restrict how data is used.

There are also far more obligations on employers to inform employees where and how data will be held and used as part of "fair processing" notices.

Subject access requests rights will be expanded and employers will have an obligation to comply with them without undue delay and within one month (against the current 40-day period), with a potential extension of up to two additional months.

Privacy Notices

Under the GDPR, employers will need to provide the employees, workers, contractors and applicants with detailed privacy notices detailing the following:

- How long data will be stored for;
- If data will be transferred to other countries;
- Information on the right to make a subject access request; and
- Information on the right to have personal data deleted or rectified in certain instances.

Employee Information Audit

Co-operation and understanding of the new GDPR obligations across the business is critical and organisations will need HR, legal, IT and compliance teams to take a combined approach.

The most important steps for businesses to take include:

- Carry out a data audit. Carefully assess current HR data and related processing activities and identify any gaps with the GDPR.
- Write privacy notices and ensure they comply. All information provided must be easy for employees and job applicants to understand.
- Assess the legal grounds for processing personal data. Where consent is currently relied on, check whether or not it meets GDPR requirements and remember that consent may be revoked at any time.
- Develop a data breach response programme to ensure prompt notification. Allocate responsibility to certain people to investigate and contain a breach, and make a report. Train employees to recognise and address data breaches, and put appropriate policies and procedures in place.
- Determine whether or not a data protection officer must be appointed and if so, think about how best to recruit, train and resource one.

Maintaining Records

There is a specific obligation to maintain written records of processing activities. The record of processing activities must include:

- Name and contact details of the company, any joint controller and the data protection officer (if applicable)
- The purposes of the processing
- A description of the categories of data subjects
- A description of the categories of personal data
- A description of the categories of recipients to whom data has been or will be disclosed
- The anticipated time limits for erasing different categories of data; and
- A general description of the technical and company security measures adopted.

Your Next Steps …

1. Data Protection by Design

Minimise data collection and retention, gain consent from consumers when processing data, get rid of data beyond its original purpose.

Create a data aware culture.

2. Records of Activity

Create asset register of sensitive files; understand who has access; know who is accessing it; know when data can and should be deleted.

3. Right to be Forgotten

Be able to locate and target specific data and automate removal.

Find it, flag it, remove it.

4. Breach Notification Process

Prevent and alert on data breach activity; have an incident response plan in place.

Be able to detect abnormal data breach activity, policy violations and real-time alert on it as it happens.

5. Impact Assessments

Quantify data protection risk profiles.

Assess the processing of sensitive, high-risk data.

6. HR / Employee Provisions

Carry out an HR audit; update your Data Protection Policy; ensure you have privacy statements in place for employees and candidates. Have a process for subject access requests. Train employees in the new data protection rules, ensure compliance.

7. Contact Dynamic HR Services

To purchase a pack with a Data Protection Policy, Privacy Statements, Subject Access forms and letters contact me at Dynamic HR Services:
020 8798 3470 /
natalie@dynamichrservices.co.uk

Dynamic HR Services

I am Natalie, your unconventional HR and business strategy consultant. I do things differently and I am much more than 'just HR'.

WHAT I DO

I support small businesses to build the foundations of HR and business ensuring everything implemented contributes to their overall profitability and growth.

I work with directors and business owners to launch established businesses into the next stage of their growth by improving their people, their brand, reputation and profitability.

At all stages, company values and people are at the centre of everything I endorse.

HOW I DO IT

Utilising over a decade's worth of experience, I have taken many large business people-practices and honed them for successful use in micro and small businesses.

Combining HR, branding and wider business strategy, with your people at the centre, I support you to take your business to the next level.

I start with the HR foundations (company vision and values, employment contracts, policies, processes) and then help you align your customer and employee journey giving you a firm basis for success.

WHY IT WORKS

I take the experience I gained by working with hundreds of businesses and provide you with a step by step process including tried and tested techniques that will set your business apart from competitors, ensure you have the right people on board and support you towards growth and profitability.

WHO I AM

A national award-winning HR Consultant with an unconventional approach.
Mentor and coach to start-up businesses. Chair Trustee of the charity Speed of Sight
Proud owner of a rescue dog, avid horse rider, self-development junkie
I am not just HR!

Get in Touch: 020 8798 3470 / natalie@dynamichrservices.co.uk