GDPR

GDPR. Bet you don't even know what that stands for, do you?

On second thoughts, since nobody's shut up about it since it was first posited, you probably do.

But if you don't, that's okay. It's General Data Protection Regulation. And it's new.

It's coming on the 25th May 2018.

There's quite a lot of changes to the law, so we're going to break it down, bit by bit.

Basically, if you're handing people's data, you absolutely need to know this.

In fact, everyone should know it.

NAME _____

LITMOS HEROES

Saving the world from boring learning

GDPR

How to use this workbook

- It's yours. Take it away with you.
- Flick through the chunks of learning. We've put small takeaways at the end of every bit to help drive the points home.
- Take your time to go over the points at your own pace
- Make notes, scribble on it, draw some hilarious pictures... go on, we dare you
- Complete the final quiz, and make everyone in your life proud of you

WHO SHOULD READ THIS?

- Anyone working a business that handles any data belonging to EU citizens.
- Anyone currently concerned with the original data protection act.
- Anyone who wants to avoid a mahoosive fine.

KEY INSIGHTS

- What's actually going to change in the law
- What your company need to do to adapt
- What constitutes 'Personal Data'
- Data Protection Principles
- Data Breaches – and what to do if you spot one
- Subject Rights – the rights of people whose data we handle
- The role of the 'Data Protection Officer'
- Fines for not complying
- Some new concepts to GDPR, like pseudonymisation and absolute consent (Don't panic. We'll put it all in plain English.)

INTRODUCING GDPR

Okay. The General Data Protection Regulation is a brand-new set of laws that relate to how we handle people's personal data.

It's how we keep it secure, while ensuring the rights of the individuals we hold data for.

It's the biggest change to happen to data protection in a good 20 years, with nastier fines for not complying.

It effects everyone who holds the data of EU citizens, no matter where they're based in the world.

People have more rights, and more people are covered.

"Hang on, you said in 20 years. What was there before this?"

Good question. But interrupt me again and you'll know about it.

Before this was the good old Data Protection Act.

Look, we're not being rude. The DPA is great in many ways, but it didn't offer as much protection or protect anywhere near as many people.

GDPR is different in other ways, too. Let's look at some of the key features of it.

DATA

Under GDPR, here's what constitutes personal data:

- Names
- ID numbers
- Locations
- Online identifiers, like Internet Protocol (IP) numbers and addresses
- Or any other factors specific to individuals, like:
- Physical
- Physiological
- Genetic
- Mental
- Economic
- Cultural
- or social identity

SUBJECT RIGHTS

When we say subject, we mean the person whose data you have.

Subjects have the following rights:

- Right to be informed
- Right of access
- Right of rectification
- Right to erasure or deletion, also known as the 'Right to be forgotten'
- Right to restrict processing
- Right to data portability, and
- Right to object

Basically, people's rights have now been strengthened.

You now have a month to process any subject access request, whereas previously you had 40 days.

So, companies will probably need to develop policies to outline who will handle and validate these requests.

Individuals can also request that their data be permanently deleted.

But – just to throw in a curveball – they don't have the absolute right.

In limited circumstances, you can reject a request for deletion. This is if the request is clearly unfounded or excessive, or you can justify your rejection with a legal obligation.

You need to tell the person why you're rejecting it, and that they can complain to the Supervisory Authority if they want to.

See? It's serious business.

DATA PROTECTION PRINCIPLES

In GDPR, there are 6 core principles for protecting people's data.

To make them easy to remember, we use the acronym PLAIDS.

Just think of a little Scottish man wearing plaid tartan. Ahh, he's so cute. And he plays the bagpipes. Maybe he goes for country walks in the highlands? With one of those shaggy cows?

Sorry – we're overthinking him.

Here are the 6 data protection principles:

- Purpose limitation – only using data for the exact reason you collected it, with the original purpose being specified to the individual.
- Lawfulness, fairness and transparency – Is everything legal and fair? Are you being totally clear about your intentions for collecting and using data?
- Accuracy – All data needs to be up to date and, well, correct
- Integrity and confidentiality – Data will need the right security. Both technically, like encryption, and organisationally, like making it difficult to access. This limits unlawful processing, accidental loss, or damage.
- Data minimisation – only processing the data you need for the task you're doing. If you don't need extra information, you shouldn't be looking for it.
- Storage limitation – This is deleting data when it's no longer needed. The Data Protection Officer (whom we'll discuss later) should create a data retention schedule to highlight how long you should be keeping it.

See? PLAIDS.

Kind of. It's not exact, but it should give you a clue when you're remembering.

DATA BREACHES

Look alive - this is a really big one!

What happens if you mess up?

It's called a breach.

You are breaching data if you, or anyone else, uses it in any way it's not supposed to be used.

A personal data breach is, by definition:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

Whereas beforehand, you were under no obligation to report a data breach, you now have a countdown of 72 hours to report it to your friendly local Supervisory Authority.

This is what you'll need to do:

1) describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects and personal data records concerned

2) communicate the name and contact details of your data protection officer, or another contact point, where more information can be obtained

3) describe the likely consequences of the personal data breach, and

4) describe the measures taken, or proposed to be taken, by the controller to address the personal data breach. This includes anything done to stop possible adverse effects.

Plus, in any 'high risk' circumstances, like if a customer's financial details have been compromised, you'll need to contact the individual directly and notify them.

TAKEAWAY

Basically, data breaches are about to be taken a lot more seriously.

So if a person's information has been misused in any way, you need to report it.

Also, it's good to be informed on the rights people have regarding their data.

Read over it a few times so it sinks in.

GOVERNANCE AND ACCOUNTABILITY

Yikes. There's a lot to keep an eye on with this new GDPR malarkey, isn't there?

Surely it would be a great idea to assign a person to regulate all these changes and make sure you're complying, right?

One step ahead of you.

That is going to be the role of the Data Protection Officer. (See page xx – ed.)

That could even be you. But maybe it's not.

You'll need a DPO if your company is:

- an organisation that carries out the "regular and systematic monitoring of individuals on a large scale". This is going to apply to a lot of companies.
- an organisation that carries out the large-scale processing of special data categories, such as health records, or information about criminal convictions.
- or, if you're a public authority.

The Article 29 Working Party are an advisory body, and have published a guide for the role. You can find it here: ec.europa.eu/newsroom/document.cfm?doc_id=43823

Hold your DPO-based excitement for the next section, where we'll go over the DPO's role more.

The other thing for Governance and Accountability is: you'll need to find out who your supervisory authority is. Each EU country has their own. And, where you might have previously, you don't need to register with them anymore.

The main supervisory authority will be the 'main establishment' of the organisation in the EU.

However, other EU authorities, or 'Concerned Supervisory Authorities' might become involved if complaints are raised directly to them.

DATA PROTECTION OFFICER

The DPO's tasks are the following:

1) Reviewing data flows and conducting data mapping exercises with third part vendors.

Data mapping exercises will include any information regarding the entities processing data on behalf of the company. Things like names, purposes, data subjects, categories of data and any security measures in place

2) Implementing and ensuring the Privacy by Design or Privacy by Default principles under the GDPR.

'Privacy by Design' means that privacy is considered at the start of each project (rather than as an afterthought). For example, if you're developing a new product or service, considering sharing data with third parties, or using data for a new purpose, you should consider privacy at the earliest possible stage.

'Privacy by Default' means that the default settings are the most privacy friendly already.

The advantage of ensuring these principles are that you improve privacy awareness across your organisation and, more importantly, you identify privacy risks at the earliest possible stage.

The concepts of Privacy by Design and Privacy by Default are defined under the GDPR. It's pretty flexible in terms of what each organisation uses, as long as they consider the data breach risks for the individuals covered.

3) Conducting privacy impact assessments (PIA) or risk assessments. Under the old law these were considered best practice, but now: they're mandatory.

4) Ongoing privacy awareness training and audits. That means ensuring employees undergo regular training on privacy and security.

5) Record keeping. Under the new accountability principle we've looked at, the DPO will need to keep records that demonstrate compliance with the requirements under GDPR.

So not too much for them to do, then...

TAKEAWAY

Basically, a DPO is there to be the Data Protection Representative.
They'll make sure everything in your organisation is above board and in compliance with the new laws.

Don't forget to read the Article 29 Working Party guidelines online if you want to know more about the role. Easily searchable stuff.

FINES

Here we go – it's the biggest change under the GDPR, and probably the one you'll be most worried about. Brace yourself.

Fines just got a whole lot hurtier. Nothing to worry about, as long as you're complying.

There's are two tiers to fines. They are the following:

Tier 1

Reasons for fines include:

- Failure to appoint an independent and fully supported DPO (told you they were important)
- Failure to complete a Privacy Impact Assessment – a PIA – for high-risk activities
- Failure to notify the supervisory authority of a data breach within 72 hours
- Failure to notify a data subject of a data breach without undue delay

The cap is set at whichever is higher: 2% of global turnover or €10 million, for certain categories. And then there's Tier 1's big brother, Tier 2.

Tier 2

Reasons for fines include:

- Failure to adhere to the 6 data protection principles (remember PLAIDS)
- Failure to demonstrate data subject consent
- Failure to comply with data subject access requests
- Failure to comply with the right to erasure and data portability requirements
- Failure to ensure adequate legal mechanisms for data transfer to countries outside the European Economic Area

The cap here is whichever is more: 4% of global turnover or €20 million.
And just because the fine is in Euros doesn't mean it only affects companies in the EU.
If your company deal with the personal data of any people in the EU, you're included in this. Sorry not sorry.

TAKEAWAY

You should do whatever you can to avoid fines. Its just not worth the hassle.

Let's just say, your company will not thank you...

Yep. We'd hate to be in that meeting.

NEW CONCEPTS

Right. Last section to learn.

It's not just new takes on current laws that the GDPR is introducing. There's some brand-new stuff in here, too, just to keep you on your toes!

Take a gander over the following new concepts:

1) Pseudonymisation

Yes, it's a big word. We're not even sure how to pronounce it. The 'p' is silent.

But it just means taking any data, and making it not directly identifiable. Like by hashing or scrubbing the data.

However, the GDPR specifically defines this process and incentivises it by reducing the requirements if the data has been pseudonymised.

For instance, depending on the circumstances, individuals would not necessarily need to be notified if pseudonymised data is stolen.

Accordingly, engineering teams should consider pseudonymisation during the design phase of any project. They'll want to ensure that, where possible, encryption and pseudonymisation techniques are applied.

2) Consent

Consent must be absolutely explicit. Under the GDPR, it must be:

"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Meaning, there can't be two ways about it.

You can't get consent from inactivity, or silence.

No ambiguity, and no tricking anyone into it.

Companies will need to ensure that, where consent is relied on, certain characteristics are applied.

So...

- There's an active opt-in
- It's not hidden in a mess of T&Cs
- There's clear record keeping of the consent being received
- They can withdraw consent at any time (and they know this)

This will apply to HR and Marketing particularly.

HR will need to:

- Audit HR data that is being stored
- Review where they've relied upon consent
- Potentially consider alternative options to justify data processing (like legitimate interests)
- Ensure general transparency regarding the data being processed and the purpose for such processing

Marketing will need to:

- Assess scenarios where they are relying on consent to collect and process personal data. Where they are relying on consent, they should establish that there is a clear affirmative action, and consent is unbundled (and that they have a clear record of this). In many cases, this may require asking third party marketing vendors about compliance with GDPR consent.

Again, everyone in your organisation will need to be aware of the enhanced responsibilities of the affected departments, and there needs to be adequate training to reflect this.

3) Right not to be profiled by automatic means

This right allows people to ask what information is being taken by automatic means, and to request that there are no automatic decisions made using their data.

Even if they don't make any such a request, an individual should always be notified before any automatic decision-making takes place.

Bear in mind: this right doesn't apply if there's any human intervention.

So, there are many processes that could involve a degree of profiling or human decision-making that'd be excluded from this definition.

4) Accreditation

The GDPR endorses and encourages the use of accredited third parties to provide assurances to customers of compliance.

You don't have to sign up to these schemes, obviously. But it can provide customers with comfort that an organisation is trying to comply with the requirements. It can also improve general privacy good practice, transparent processing, and mitigate against enforcement action.

TAKEAWAY

Excellent! You've now even taken a look at some brand-spanking new concepts arriving with the GDPR.

So things like pseudonymisation, explicit consent, right not to be profiled, and accreditation.

Just remember – they're not as complicated as they sound.

You can always flick back over these pages to refresh your memory if you forget.

QUIZ

1) Can you remember what the fines for the two tiers were? Write them here:

.....

.....

2) List as many bits of information that constitute personal data you can think of:

.....

.....

3) How long do you have to report a data breach, and who do you report it to?

.....

.....

4) Talk to us about the DPO. What is their role?

.....

.....

5) And lastly, what has changed about consent and the way we receive it?

.....

.....

FINAL SUMMARY

Massive Congratulations!

You've reached to the end of the GDPR Workbook!

Either that means you've read and completed it all, or you just happened to open it on the last page. Hopefully it's the first one.

Now, you should know about the changes from the original data protection act, some of the key terms within GDPR, the fine process, DPOs and all the new concepts.

We know there's a lot to take in, but it's all really important.

We wouldn't bother telling you all this stuff if it wasn't crucial. It's just here to protect people and their personal information.

It's what you'd want when it's your data being processed.

So, it's a great thing.

Now, you can go forth, be excellent, and protect people's data.