EXONAR

Simplifying GDPR

Part 1: Understand the game - then score some easy wins and be 2-0 up by half-time

Our four-part guide to making life easier under the UK's new data protection laws

Welcome to Simplifying GDPR from Exonar.

What's in our series of guides?

Private sector, public sector or third sector, GDPR applies to all of us and the personal data we hold. We'll explain over this four-part series how to comply with GDPR – how to align the right technology, people and processes so that GDPR works for you and not vice versa.

Part 1: Introduction and tackling transparency

It's important to put GDPR into context and its implications for your organisation – plus how you can score some easy wins around transparency that will get you rolling towards complying with its principles. Oh, and Brexit too!

Part 2: Get the team signed up and on the pitch

Make certain you have explained GDPR to your organisation, identify and elect your board sponsor, form a posse from legal, compliance, technology and your key personal information owners like HR and customer services. Then get everyone in a room, work out your high-level programme plan and cost it across internal resource, external advice/resource, tech spend, training and ongoing costs. Then you'll all have a pretty clear view of how life is under GDPR.

Part 3: Data mapping and inventory

How to build that clear picture of the personal data you hold using the right technology strategy. Let's get going!

Part 4: Give yourself a simple life under GDPR

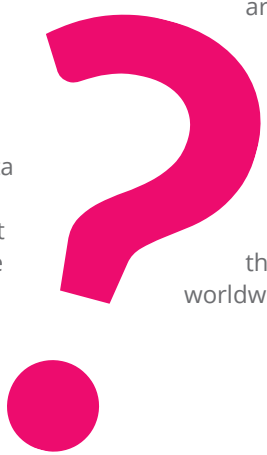
Your people may now be used to life under GDPR but do you know how to treat the personal data you hold? The good rules of thumb are: only capture and keep the data you need (always remembering the subject owns it, not you), maintain and monitor who has data access and embed an effective cyber security strategy. Oh, and training – lots of it.

Some basics & why bother?

So let's crack on with some basics

The introduction of GDPR is the biggest ever overhaul of data protection laws and it replaced the UK's Data Protection Act 1998 on May 25th, 2018. Sure, GDPR is a big jump in terms of process, liability and penalties for non-compliance with its principles - but it's not the complex tangle of Eurocrat legislation you could be forgiven for assuming.

At its heart, GDPR neatly simplifies the way we all handle the personal data of employees, customers, clients, suppliers, partners, members, subscribers, students and patients. Instead of data protection being an afterthought, the protections have become hard-wired into how we handle that data. We believe it's good for business too – more on that in a bit..



Why bother?

The nuts and bolts of GDPR are well-documented. But why was it created?

Every jurisdiction around the world has different views and laws for maintaining privacy and handling personal data. Effectively this means there are no common standards which are problematic in a data-centric world without digital borders. GDPR provides a set of common rights and protections for the digital privacy of all EU nationals and governs how personal data should be used and protected. Importantly, it applies to all firms and organisations based in the EU and also those based outside the EU who offer goods or services to EU citizens. Digital traffic and trade are so globalised that GDPR was, to all intents and purposes, the first worldwide personal privacy standard.

Data custodians & Brexit implications

We are all Data Custodians now

What do these common rules and expectations mean in the real world? Effectively, implementing GDPR strengthens the trust between your organisation and your audience You should now be able to demonstrate that you care for personal data, that you will not collect or use it inappropriately or without permission, and will provide or return it to the individual if requested – and even delete it when it is no longer relevant. GDPR is thus good for business: your brand reputation will be enhanced in line with the trust that's vital to positive customer service experiences. However, it's not just about changing the processes for managing personal data, it's also about how GDPR changes the way we view personal data. The reality is that GDPR makes us all data custodians now, not just data owners. Our new responsibilities are to the real owners of that personal data – the individuals themselves. That's a massive and fundamental shift in both perspective and customer engagement, one that seriously strengthens the part sound ethics play in underpinning good business practice.

Brexit - What happens when we leave the EU?

It's an obvious question and one where we can be absolutely crystal clear: all EU legislation will convert into UK law as part of the European Union (Withdrawal) Bill. No complications and no caveats. In addition, the 2017 Data Protection Bill is currently making its way onto the statute books.

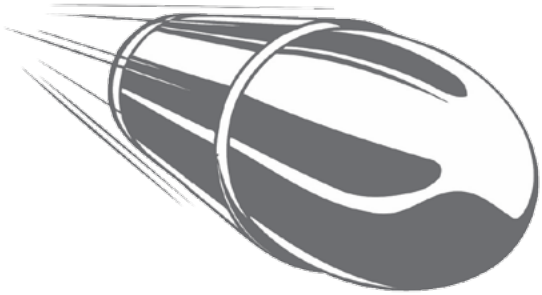
You can track its progress here https://services.parliament.uk/bills/2017-19/dataprotection.html. The Bill encompasses the principles and detail of GDPR with some additional controls and interpretation where allowed by GDPR. GDPR allows member states to set the age limit - between 13 and 16 - above which a child is regarded as capable of giving consent. The UK Government has chosen to set this limit at 13. There are enhanced rights for UK citizens to be forgotten, including requiring social media platforms to delete the information they posted below the age of 18 on their request. New criminal offences have been created for intentionally or recklessly re-identifying individuals from anonymised or pseudonymised data. It is also now a criminal offence to alter records with intent to prevent disclosure following a request from an individual to see what data you hold on them – a subject access request or SAR.

Silver bullets & reasons to be cheerful

There's no silver bullet

First, there is no such thing as an off-the-peg, end-to-end solution, policy, template or quick fix for ensuring your organisation is compliant with the principles of GDPR.

Second – and like good coffee – successful compliance is a balanced blend of complementary elements that work in harmony. In this case, it's people, technology, personal data handling processes, security and your own working culture.



But there are reasons to be cheerful

Yes, there are many new statutory rules to observe with GDPR but let's keep a sensible perspective. The Data Protection Act (DPA) has been law since 1998 – it's well established and broadly well-observed which means that we already work in an operational culture where taking care of personal data to universal legal standards is the norm.

GDPR is not something radically new, it is an extension of the DPA (granted with extra bells and whistles) thus most organisations were already doing the basics. Effectively the glass was half-full and by any stretch, that is a comfortable starting position.

Stepping back

Take a step back

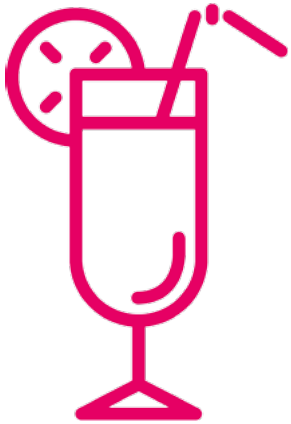
It's easy to be spooked by hyperbolic commentary, conflicting advice and the general frenzy of static that was and still is surrounding GDPR. Fines! Deadlines! Encryption! Consent! Our advice: chill out and use the opportunity to re-evaluate what personal data means strategically to your organisation. Ask yourself these questions.

- Why am I collecting personal data? Is it simply for employees, like payroll, HR and employment contracts? Or are you also collecting, controlling and handling customer, sales, marketing, subscriber, member or other forms of client or supplier related information? The key here is ensuring what you keep is detailed enough to cover what you need to know but sufficiently minimal to be wieldy, clear and standardised.

- What personal data do I have? This is the killer question that often prompts an embarrassed whisper of "I'm not sure!". Data storage (particularly the less well-structured forms) can often resemble a teenager's bedroom floor. Letting those data socks fester in the corner simply stores up problems come room inspection time. Now is the perfect opportunity to locate, classify, cleanse and standardise that data.

- Where is it? Another zinger. Stored centrally on your network? Residing on local drives, home office systems or personal work devices? How much is duplicated and/or out-of-date?

- Who has access to it? What are the permission, consent and protection levels? Who is responsible for its accuracy and applicability?



Your privacy manifesto

Think of GDPR as your privacy manifesto

What does life under GDPR actually mean in real terms? It's your attitude to data privacy: a manifesto if you like. In true Blue Peter style, here's an example we prepared earlier:

"As an organisation, we understand and can demonstrate what personal data of yours we're processing and storing, who else is doing so on our behalf, why we're holding it and how we're using it. Unless we have a legitimate reason or requirement for processing your data, as defined by the law, we will ask for your consent before doing so. You may withdraw your consent at any time.

"We recognise that the data we hold about you belongs to you, so we will take care to protect it from unauthorised access. However, should the worst happen and there be a data breach, we're ready and able to disclose the details in a responsible and timely fashion. We will take special measures to protect data regarding children or sensitive personal data that could affect your fundamental rights and freedoms - for example, where such data might put you at risk of unlawful discrimination.

"As an individual, you have rights regarding your data. You may request a copy of your personal data, request it is deleted - which we will do if there is no requirement for us to hold it - and request that any errors in your personal data are corrected. Where we are making an automated decision or carrying out profiling based on your personal data, we will ask for your consent if it isn't necessary for our legal obligations or because of a contract we have with you. Where we carry out this type of automated processing, we will provide the option of a manual review of the decision".

When you can read this manifesto – or a similar version of it that accurately reflects the way your organisation works - you can be confident you are prepared for life under GDPR. We say: write that privacy manifesto then let it be your guide and aide memoire.

Remember: it's just a spring clean for the May Queen
Relax into this: GDPR is your perfect opportunity to adapt existing DPA processes, get the right management technology in place and dust down the specifics of processes, data redundancy, accuracy, applicability, audit trails, consent, security and access.

Where do I start?

Where do I start? With those quick and easy wins

Now we're looking through the right end of the telescope, let's outline the basic things you can do that will – relatively quickly – give you that firm foundation for ensuring compliance with the principles of GDPR.

Get organised

Have you picked your GDPR team? You'll need a sponsor at board level and an implementation team comprising legal, compliance and technology plus key personal information owners like HR and customer services. More on this crucial recipe for success in Part 2!

Get that grandstand view of your data estate

Do you have relevant and up-to-date data categorisation and retention policies plus a clear definition of how your data estate should look when sparkly clean? How regularly have you

categorised and purged your data to remove old or duplicate information? It may seem counterintuitive but even if your organisation applies no methodical deletion or categorisation processes, at least it's a clearly understood starting point.

Check for relevance

This ties back to why you are holding the data in the first place and relates to one of the key principles of GDPR – to minimise the amount of personal data processing. If there's information in a record you don't need for any reason, then delete it – you'll begin the uniquely satisfying process of streamlining your personal data records and reducing your storage demands.

Think about the life of personal data

To crack the problem of data mapping (or knowing which systems hold personal data), think about the lifecycle of personal data – because it can be pretty lively. When an individual interacts with your organisation, how does their data seep into your various systems over time? For example: as a prospective customer I may make an enquiry on your website: my data is now captured in a marketing automation system. Somebody in sales then follows up my enquiry via email, records my interest in a management package like Salesforce.com, exports my details to a spreadsheet for the sales report ... you get the picture. When your data owners are describing the personal data they are processing, always think about how that data is getting into - and out of - your intended system.

Check formats & consents

Check your formats

You may have personal data held in different ways – perhaps in spreadsheets, Dropbox accounts, in email folders or in a secure database or business app. Even so, your data will develop a life of its own. As mentioned above, it may start life in a well-structured database but will end up being exported into a spreadsheet, combined with other data, emailed to a supplier and so forth. We say: identify what data is where and ensure that you are comfortable that these methods of storage and the way you secure the data isn't exposing the data subject – and your organisation – to uncomfortable levels of risk.

Check your consents

There are confusing messages out there about consent and personal data. The truth is that GDPR does not require blanket and mandatory consent for processing personal data: just those occasions where you don't have another legal basis for holding the data or if the standards say you must because there's a legal need. What follows is not an exhaustive list but broadly speaking, you don't need to rely on consent in the following circumstances:

- If a law requires you to process personal data – such as the record of incidents under the Health and Safety Act
- You are a public authority processing the data in the public interest – for instance, recording driver details in a speeding vehicle
- You have a contract with the individual that you would not be able to fulfil without processing the data – for instance, you can't provide health insurance to this individual without processing their data

Check consents continued

- The individual has asked you to take steps to enter a contract - such as requesting a quote for broadband service - which involves the processing of this data

- Someone's life or safety will be in danger if you don't process this data – for instance, not recording they have a peanut allergy for a forthcoming event means you will otherwise put them at risk

- You have a legitimate interest in processing the data that doesn't conflict with the individual's rights. However, do be careful about relying on the legitimate interest argument as you can expect the authorities to side with the individual if there is any doubt.

You should only be using this position if you can demonstrate it isn't interfering with the individual's rights and that it would otherwise be impractical to gain consent. The Information Commissioner's Office (ICO) has some good further guidance on using legitimate interest here:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

A handy rule of thumb is that if you can't meet any of these standards then you should be seeking consent to process an individual's personal data.

Easier said than done!

“Easier said than done”, you might say?

A fair point, well made. Data record checking is a forensic job and the more personal data you hold, the more of a time-consuming and potentially expensive chore it becomes – especially if the type and location of that data are unreliable, inconsistent or worst case, unknown.

Actually, that’s no longer true at all; the received wisdom is now obsolete.

There is one other easy win you can score that relates back to knowing what data you have and where it resides – achieved by deploying the right technology leverage to the problem. Exonar’s platform provides a top-down view of all the personal data you hold via a GDPR Dashboard.

The platform continuously indexes your data and uses machine learning to figure out the types of personal data contained – plus it lets you locate any of it instantly (and lots more besides). It’ll make your personal data management far simpler, but also give you the all-important view – and control - of that data quickly. This is the key to unlocking the GDPR door: knowing what you have and where it resides. It’s just another easy win ...

Simplifying GDPR - Part 2:
Get the team signed up and on the pitch.
Available to download now!

Can we help you?

Welcome to Exonar: if you need a helping hand ensuring your GDPR projects are heading in the right direction, then get in touch today.

Exonar's platform helps you map and understand your personal data: instantly, simply and at scale. We deliver specialist solutions compliant with the principles of GDPR that enable you to find, understand and protect productive, valuable and sensitive personal information.

Click: exonar.com

Email: tellmemore@exonar.com

Follow us: Twitter

Check us out: LinkedIn

Demo or free trial?