EXONAR

Simplifying GDPR

Part 4: Give yourself an easy life under GDPR

The final episode of our four-part guide to making your life easier under the UK's new data protection laws

Welcome to Simplifying GDPR from Exonar:

what can you look forward to in Part 4?

Private sector, public sector or third sector, GDPR applies to all of us and the personal data we hold. The legislation is now in force and the sky hasn't fallen in! Let us help you align the right technology, people and processes so that GDPR works for you and not vice versa.

Part 1: Introduction and tackling transparency

Read Part 1: **exo.nr/GDPRPt1**

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

Read Part 2: **exo.nr/GDPRPt2**

Part 3: Data mapping and inventory

Read Part 3: **exo.nr/GDPRPt3**

You are here

Part 4: Give yourself a simple life under GDPR – the hallowed turf of compliance!

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 – it's all about the people!

Always think about the information you hold

Always think about the information you hold

As Sinatra once memorably sang: "And now, the end is near …" Your implementation team has now completed most of the hard yards: they've mapped and inventoried the personal data you hold and have started remediating it. Whatever state that personal data was in – including all the digital litter – you're now fixing it all. Nice! Now's the time to run through all those areas you need to keep an eye on that will help you stay compliant and make your life under GDPR easier. Remember, compliance isn't just the immediate destination, it is how you manage your stewardship of personal data from now on – and indefinitely.

- **Only collect the data you need:** you've already defined the type of personal data you need to get the job done and cleaned up what you already have. Unstructured digital litter can build up quickly if unmanaged so always stick to the personal data criteria you have set!

- **Data compliance through good governance:** ensure every part of the organisation collecting, handling, processing, managing and interacting with personal information follows the governance protocols you have established. This is perhaps the single most important long-term task for your data protection officer: a quick sweep up on a regular basis - every quarter or so - will keep you steadily on track.

Housekeeping Tip:

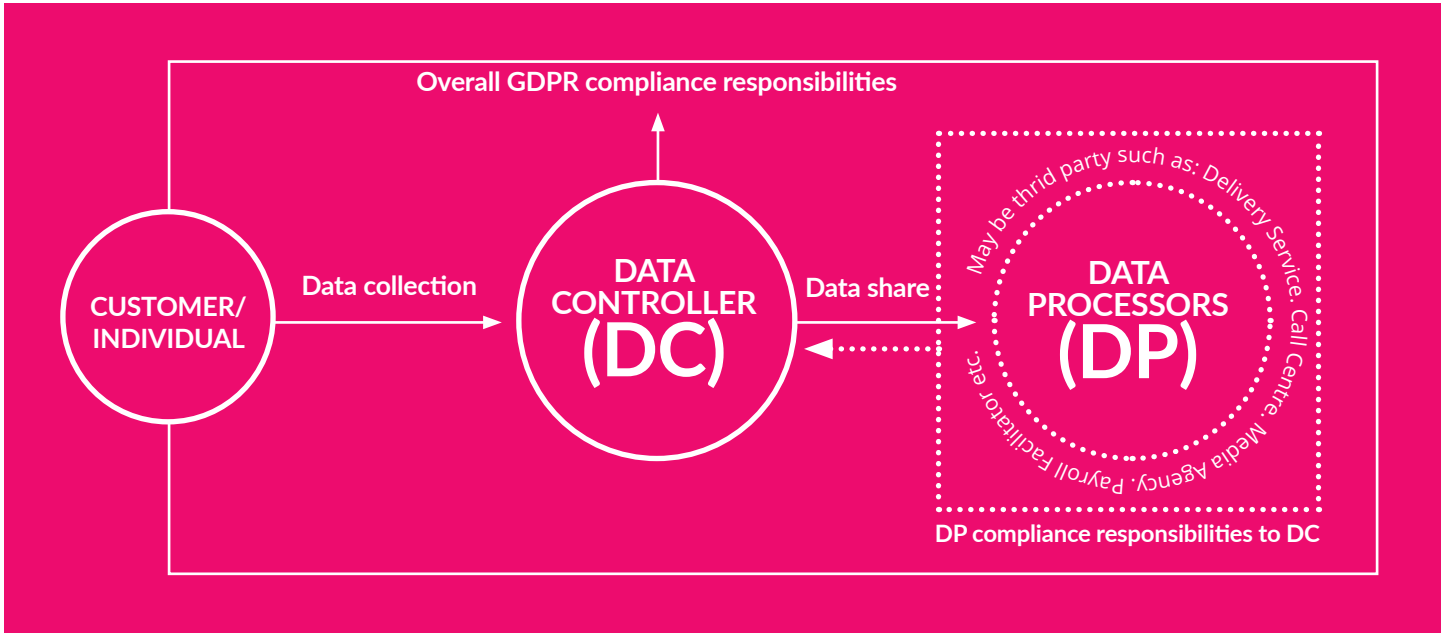
keep Exonar on the inside and the digital litter outside.

Exonar enables you to see, control and remediate personal data in near real-time – all the time.

Always think about your control and processing obligations

Always think about your control and processing obligations

Under GDPR there are data controllers and data processors. You can be one or the other – or you can be both. A quick reminder on the highlights for what each is, what they do and their obligations under GDPR... now take a deep breath!



1. Data Controller(DC) Responsibilities

1. Data Controller (DC) Responsibilities

Data Controller (DC) Responsibilities The DC determines the purpose and means of processing personal data. In other words, the controller decides what personal data is collected and how it is used, shared and stored. Typically this is the organisation ultimately responsible for that personal data.

- **Accountability:** ensures all personal data processing activities are compliant and must be able to demonstrate that compliance through appropriately documented work processes and data handling records.
- **Legality:** applies all appropriate technical and organisational measures that demonstrate compliance. These include things like a documented and clear privacy policy, established lines of responsibility and adherence to the governance strategy.
- **Design and default:** makes sure compliance is embedded in all data processing activities by design and that by default, you process only the minimum amount of personal of data needed to get the job done.
- **Joint controller status:** evenly apportions compliance responsibilities when two entities or more determine how personal data is being used. This could be where two separate departments in the same organisation are making their own decisions about personal data use.
- **Processor appointment:** ensures any third party data processor appointed can guarantee full compliance with GDPR.
- **Records:** manages the upkeep of data processing records that can be made available on request by a data protection authority (DPA) – that's the Information Commissioner's Office in the UK (ICO).
- **Data security:** takes all reasonable measures to ensure the security of personal data. There's lots of latitude here but it basically means applying the organisational, operational and technical measures that protect the personal data you hold from breach, leak or loss. So talk to IT!
- **Breach reporting:** reports any compliance breach to the ICO (via the data protection officer) within 72 hours of discovery and to all affected data subjects without any undue delay.

2. Data Processor (DP) Responsibilities

2. Data Processor (DP) Responsibilities

The DP is responsible for processing personal data - using it day-to-day - on behalf of the controller and is covered by Article 28 of GDPR. This will usually be a third party; an organisation you share the data with for agreed (and compliant) purposes of use. Good examples of a DP might be when HR outsources processing of employee data to a specialist company or marketing passes personal customer data to a digital campaign or ad agency - perhaps to a third party call centre to handle customer responses (see page 7). Alternatively, you as a DC may have several DPs - for instance if you're selling online and use different parcel delivery firms, those delivery firms are all data processors under GDPR. The major responsibilities are as follows ... so take another deep breath!

- **Definition:** processes data for the DC on the authority and instruction of the DC.
- **Guarantees:** must embed and document appropriate organisational and technical measures that are fully and demonstrably compliant, protect data subjects' right and ensure a level of information security that matches the risk to the data involved.
- **Appointment:** must be bound to the DC by a contract itemising the nature, duration and purpose of the data processing task along with the type of personal data to be used, the types of data subjects involved and the legal rights of the DC.
- **Instructions:** can only act on documented instructions from the DC.
- **Confidentiality:** must ensure that all staff processing personal data understand their confidentiality responsibilities – then document it.
- **Client register:** if you're a processor handling DP work for multiple clients, you need to keep a register of what you process and for whom.
- **Sub-processing:** a DP wishing to contract-out to a sub-processor must have the permission of the DC.
- **Assistance:** must support the DC across data subject rights and security plus data protection impact assessments (DPIAs) and data breach duties.
- **Fate of data:** either delete or return all personal data at the end of the processing contract, depending on the DC's preference.
- **Warning:** if a DC's instructions appear to be in breach of regulations, the DP is duty bound to flag it with the DC.

Keep on top of your legal justifications for handling personal data

Keep on top of your legal justifications for handling personal data

Are we handling personal data in a compliant fashion? Under GDPR, this is the key question you need to ask yourself; not just once but continuously. Good governance practice means you should check the way you handle personal data as part of continuous assessment – we suggest a broad review every quarter or so. It'll keep your organisation on top of your compliance obligations and your people's eyes on the ball.

The nutshell perspective: personal data handling and processing must at all times be lawful and fair as well as transparent for your data subjects, readily accessible and easy to understand.

Continued

Your six grounds for legal and compliant personal data processing

If you can satisfy at least one of the following criteria, then you will have a clear legal basis for processing personal data.

- **Consent:** you have your data subjects' agreement to hold, handle and use their personal data.
- **Legitimate interest:** you can demonstrate a balanced and legitimate interest for processing personal data not contrary to the other grounds.
- **Public interest:** you are a public authority or body processing personal data in the pursuit of your legal duties and responsibilities.
- **Contractual necessity:** you are processing personal data in order to enter in to or execute a contract with data subjects.
- **Legal obligation:** the law obliges you to process personal data.
- **Vital interests:** you must be able to process, handle or use personal data in matters of life or death.

Review, maintain and document

Those six grounds are really important and we think it's good practice to overlay them against your actual personal data processing every time you undertake a periodic review of your current compliance status. Should you suffer any sort of breach that could land you in hot water with your personal data audience – or the regulator – then you will need to be able to demonstrate what has taken place. That means making and keeping consistent records about what personal data you process, how, why, what for and when as standard practice so you can easily log, report and explain any breaches.

Third Party data sharing and supply chain risk

Third Party data sharing and supply chain risk

If the personal data you process is handled solely and exclusively in-house and shared with neither man nor third party beast, then it's time for tea and a biscuit. But if you share data with third parties for any reason – and particularly if they then process that data on your behalf – then read on because there's an important issue to explore. We call it 'supply chain risk': the more data cooks you have in the kitchen, the greater the chance of spillage.

Put simply, if you share the personal data you hold with a third party who processes it on your behalf, then you need to ensure that they are doing so compliantly. It's back to the basic relationship between data controller and data processor we touched on earlier when DC and DP are separate entities.

- Most commercial organisations also have a physical supply chain of suppliers and partners that help make the business tick.

- These include delivery firms, HR specialists or accountants, cloud service providers, IT support contractors, manufacturers, marketing agencies, call centres and property maintenance – you name 'em. If in the process of serving your organisation they need to process (your) personal data – say using customer contact or employee details – then they are data processor to your data controller and you must ensure that they prove themselves compliant under GDPR.

We say...

- **Examine your supply chain:** who amongst your outsourcing or partnership network is using your personal data?

- **Expand your contracts:** cover the use of personal data in the contractual arrangements you have to include what is used, what for and why, storage, security, duration and disposal or return at contract's end.

Remember, if it's your personal data then you are the data controller and the supplier is the data processor – in the information supply chain, the buck always stops with your organisation as DC.

Turning your privacy policy into a realistic privacy notice

Turning your privacy policy into a realistic privacy notice

You've already created your privacy policy and chances are, the more personal data you process, the more detailed that policy is in practice. But in the real world, it's likely no consumer who interacts with you will bother to read it and that's why your privacy notice is really important. Under GDPR, you have to make your audience aware of the key privacy facts at the point of consent or personal data collection. Brevity is the name of the game – particularly if you are collecting personal data over the phone or in person. Even if your internal privacy policy is large, the corresponding privacy notice needs to be short, sharp, simple, easily accessible and always in Plain English.

The Information Commissioner's Office says: "being transparent by providing a privacy notice is an important part of fair processing. You can't be fair if you are not being honest and open about who you are and what you are going to do with the personal data you collect". Makes sense.

Your privacy notice: the key ingredients

Remember; the privacy notice accompanies any mechanism you use where you are collecting personal data or gaining consent for that data. Ask yourselves these questions, answer them snappily - and voila! You have a compliant privacy notice that's also a great aide memoire.

- What information are you collecting?
- How are you collecting it and where from?
- Why are you collecting it?
- Who is collecting it on your behalf (e.g. a data processor?)?
- How will you use it?
- Who will you share it with (if at all)?
- How long will you keep it and what mechanism will you use to ensure automatic deletion?
- How will you secure it?
- How will you meet the rights of the data subject under GDPR?

As part of good governance, it's wise to check your privacy notice as part of your periodic personal data review. Things do change (one thing guaranteed isthat legislation always involves mission-creep) so make sure that your privacy notice is current and clear.

Factoid: did you know that if you read all the privacy policies on every web site you visited over a year, you'd spend over 10 days glued to the screen? What a thrill-packed 244 hours!

Always keep in mind the rights of the data subject

Always keep in mind the rights of the data subject

People's awareness of their new personal data rights are ramping up, the key difference that they have significant control over – and access to – the personal data you hold on them. While that awareness is spooling up, it makes sense to embed those rights clearly in the minds of all your people interacting with personal data. Data subject rights requests take several forms and you could be on the receiving end of some, or even all of them, depending on how extensively you are using that information.

We've said it before and will do so again: automating your data subject rights responses will take the pain out of the task and enable you to manage personal data quickly, easily and cost effectively. Our Exonar platform is an easy-to-use solution that performs the job for you. Let's run through those rights ...

- **Right to be informed:** enshrined in your privacy notice at the point of consent or data collection, you need to make it clear about what personal data you are collecting, how it will be used, how long it will be kept and how it will (or won't) be shared.

- **Right of access:** people can now oblige you to provide a copy of the personal data you hold on them – all of it. This is a data subject access request (DSAR) and you have one month to respond. You need to provide that information free of charge and it must be in a clear and easy-to-read format. You can only reject a DSAR if you can show it to be vexatious, i.e. repetitive, excessive, mischievous or unfounded. Some types of business – and some types of brands – are vulnerable to activist attention and can very quickly be made the deliberate target of Twitter 'storm' pressure. Other organisations that just process large amounts of personal data may similarly be in for a deluge of DSARs. Be prepared: automate your DSAR processing now.

- **Right to rectification:** if an individual discovers the data you hold is inaccurate – perhaps via a DSAR - they can demand you correct it and not getting all RoboCop about it, but you have one month to comply else it's a compliance breach.

Continued...

Always keep in mind the rights of the data subject (continued)

- **Right to erasure/be forgotten:** not the successful 1980s pop/dance combo but the right to ask you to erase personal data in certain circumstances. This could be to withdraw consent, the data isn't needed anymore, it was unlawfully processed or no longer meets the legal grounds on which it was collected.

- **Right to restrict processing:** an alternative to erasure, individuals can ask that you restrict the processing of their personal information for reasons of inaccuracy or if they no longer need you to have that information (even if you do).

- **Right to data portability:** this covers the simple transfer of personal data from you to the subject in an easily-read, machine readable format like a Word file or PDF. Think of it as how you physically deliver the result of a DSAR – make your life easy and automate the process.

- **Right to object:** individuals can also object to your processing their personal data even if you're using it compliantly. If you can demonstrate a compellingly legitimate case for continuing to process that data, then you can override the request.

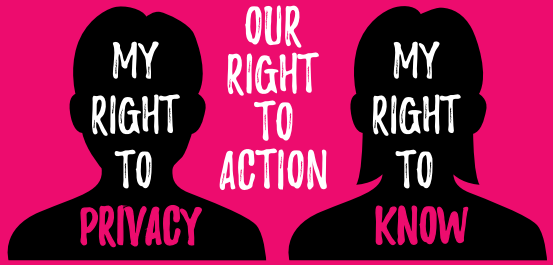
- **Rights relating to automated decision-making and profiling:** this covers personal data processing which is automated - such as profiling that makes assumptions about the individual based on the data held. People can challenge or ask for a review if they think you're not sticking to the rules.

Managing Data Subject Rights

As the rights make clear, you can be challenged on the personal data you hold in a number of ways. How you handle those challenges makes all the differences between at worst being swamped – or expensively inconvenienced - and at best, being able to manage data subject rights quickly, at low cost and in high volume if needs be.

That difference comes down to automation.

Our machine learning data management platform does all the heavy lifting – finding, fixing and managing the personal data you hold to help get you compliant and keep you that way.



Accountability – it's back to good solid governance!

Accountability – it's back to good solid governance!

Having a sound protection policy on paper is one thing, ensuring it is checked, updated and executed correctly, compliantly and consistently across your organisation is another. Remember: the ultimate risks are people being harmed by inaccurate or improper use of personal data – or that information getting into the wrong hands through poor security or inappropriate disclosure. Tactically, it's the responsibility of the data protection officer (DPO) and strategically, responsibility lies with the board. By now the implementation task is broadly complete and it's now the team's job to maintain compliance.

1. Data protection policy and monitoring

Review your performance against the policy every quarter or so and make adjustments accordingly. The DPO should keep a weather eye out for changes in the legislation, adapt the policy to reflect those changes and where relevant, alter and communicate any necessary changes to the day-to-day processes. A sound policy should be good for about three years before needing a thorough check - so best to put a reminder in the diary now.

2. Data breach notification

The legislative switch is still relatively young, but accidental breaches have already hit the news. A breach isn't just about loss, theft or leakage of personal data, so we say...

- Know how to recognise a personal data breach and ensure that the DPO is able to report it to regulator (in the UK the The Information Commissioner's Office (ICO)) within 72 hours.
- If it's a major breach, have a mechanism in place for informing the individuals affected without undue delay.
- Allocate breach management and response to a named person or team and ensure they can escalate that response quickly and efficiently.

Continued

3. Data protection training for controllers and processors

It's almost a no-brainer, but train your DCs (and instruct your DPs if you have them) on how best to follow the data protection policy.

- A skilled DPO can manage this in-house or you may need an external provider.
- Ensure that responsibilities and processes are clear and well understood.
- Embed the data breach procedures so the DPO can react positively and decisively.
- Work with HR to make sure all newbies joining your organisation who will work with personal data are fully inducted into good GDPR governance.

4. The Information Security Policy

This is a wider thing about data security and a good defence strategy will keep all of it as safe as is possible, and not just personal data. Make sure this policy (and its physical implementation) covers key areas like: cloud, web, network, email, devices (especially if you're running a BYO policy!), storage, back-up, remote working and social media. Again, work closely with the IT team so there is consistent understanding and consistent protection.

5. Data Protection Impact Assessments

Also known as a DPIA, it's the information equivalent of a Health and Safety risk analysis. The implementation team and the DPO will have carried these out early-doors anyway but it makes sense to revisit them annually to capture emerging risks - or ones you may have missed first time round. Remember, a DPIA should ...

- Describe the nature, scope, context and type of personal data processing.
- Identify the compliance measures required.
- Consider the likelihood and severity of impact on individuals if there were a breach.
- Identify the level of risk to individuals or groups (particularly for sensitive data).
- Specify the risk mitigation measures you then take.
- If you uncover a high risk personal data situation that processes can't mitigate, then the DPO should get in touch with ICO to discuss it.

Continued

6. Your Data Protection Officer

Most importantly, don't dump everything on your DPO and expect them to just get on with it! Personal data management under GDPR is a more complex beast than working to the old Data Protection Act. Clearly specify the role and its responsibilities but above all, make sure they have the support they need day-to-day – particularly with regard to IT and personal data management systems - and within the senior management team.

7. Where the buck stops

That's with the senior management team – you! First, it's with the board room 'champion' – the key point of contact for the implementation team, the DPO and compliance management. Ultimately, all responsibility for compliance resides in the board room. Ensure that GDPR is a permanent agenda item for top management. The closer an eye you keep on how your organisation processes the personal data you rely on, the better you are able to maintain compliance, contain a breach and help the DPO keep things ship shape.

8. Training and HR

We touched earlier on the importance of training relevant new people when they join your organisation: embed the compliance culture and processes at the point of induction. Ongoing refresher training is important too: the GDPR legislation won't stay static – it'll evolve and that evolution needs to be matched by the people at the sharp end who process the data. The technology you rely on to find, fix, manage and remediate your personal data will also evolve so build Exonar into your personal data training programmes. Working closely with HR, design a training schedule that will keep everyone frosty, on top of process, on top of systems, on top of the tech and on top of compliance.

They think it's all over?

They think it's all over?

Congratulations! You've built the policies and processes, tasked the team, found then fixed your personal data and made clear all the responsibilities needed to ensure compliance under GDPR.

But that's not all of it. Compliance is a journey, not just a destination. You have put in place the foundations and reached base camp, but the maintenance of ensuring you adhere to the regulations is ongoing. Manage your personal data and maintain compliance with the right tools for the job: and we have the technology to help you.

So, make sure you give yourself the best shot and an easy life under GDPR: base compliance around a technology platform that can find, fix and remediate the personal data you process, of whatever type, in whatever format and at any time.

We hope you've found our four guides to GDPR useful – perhaps even made you smile. Most of all, we hope they have helped you see through the recent hoopla to realise there's no substitute for effective processes, run by trained people that are backed by cutting edge and user-friendly technology.

Choose speed, scale and clarity.

Choose Exonar.

Coming next:
All four guides compiled into one handy download

Map and understand your data. Swiftly. Simply. At Scale.

Exonar solves a problem common to all organisations and their information owners, "I just don't know what I've got".

Plug Exonar into your network to instantly discover:

Confidential Documents | Duplicate files | Employment contracts
Encryption keys | Personal data | Passwords ... whatever you need to find.

Achieve successful:

Compliance with regulations such as GDPR | Subject Access Request Processing | Information Security & Governance
Risk Management | Document Retention | Cloud Migration and Governance.

Connect to a range of data sources:

Windows | SharePoint | Exchange | Office 365 | OneDrive
Databases and Business Systems.

Connecting Exonar to your network is simple and our dashboards are easy to use. Once installed, our crawlers will begin to index your data and deliver results on the same day.

If you need a helping hand running your GDPR projects, then get in touch today.

Click: **exonar.com**
Email: **tellmemore@exonar.com**
Follow us: **Twitter**
Check us out: **LinkedIn**

For more information on managing Subject Access Requests, visit our dedicated site at: **SARlution.com**

Demo or free trial?