




Simplifying GDPR

Part 3: Data Mapping & Inventory



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

Welcome to Simplifying GDPR from Exonar:

What can you look forward to in Part 3?

Private sector, public sector or third sector, GDPR applies to all of us and the personal data we hold. We're explaining how to ensure GDPR compliance – 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

Read Part 1: exo.nr/GDPRPt1

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

Read Part 2: exo.nr/GDPRPt2



You are here ▼

Part 3: Data mapping and inventory

How to build that clear picture of the personal data you hold quickly - using the right technology strategy. GDPR is now the law so 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: as you have established the legal basis for processing data ensure that you only capture and keep the information you really need, establish clear rules and monitor who has data access and embed an effective cyber security strategy. Oh, and training – it's all about the people!

What is 'personal data'? ▼

What does 'personal data' actually mean?

Before you start work on the nuts and bolts of data mapping, let's pause briefly and establish a helpful absolute: what exactly constitutes 'personal data' under GDPR? Time for a handy definition.

"'Personal data' means any information relating to an identified or identifiable natural person ('data subject') ... an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".
GDPR, Article 4

Well; it's not Shakespeare, but it's a clear, logical and succinct catch-all with no nasty surprises. Remember, GDPR doesn't just cover your customer data, it also applies to personal data for your employees, suppliers and commercial partners. The terms of GDPR are technology-neutral so it's not just about your digitally-held personal data but about any recorded audio, CCTV video and paper records (like HR, medical files or client information) you might hold too.

Again, no serious bear traps there – audio and video are just another type of data file anyway and paper records are much less prevalent than in days of old.

There are actually two categories of personal data under the GDPR so let's distil the definition down a little further ...



Special categories of personal data



There's PERSONAL DATA ...

The Information Commissioner's Office (ICO) observes that life under GDPR reflects how changes in technology have altered the way organisations collect, categorise, use and store personal information. This regular personal data will usually feature any combination of the following criteria ...

- A name or details like age, gender, DOB, address, postcode, mobile, landline and email).
- An ID, reference or membership number that relates to a precise individual.
- Location data.
- Any type of online code that can be related to a specific person.

... and then there are SPECIAL CATEGORIES OF PERSONAL DATA



This information category covers more personal details handled by specific types of organisations in specialist circumstances: information that if lost, stolen or leaked can have a serious impact on the data subjects affected. Categories include: genetic, biometric and medical data, financial, security and cultural information along with criminal records and data relating to religious and political beliefs, trade union membership, sexual orientation or even philosophical

affiliations. It's worth adding that under Article 9, GDPR provides scope to add more conditions to this category and that means variations may emerge between countries over time.

The true picture is that personal data is rather like an onion: it has many different layers. Identifying, managing and controlling these layers manually could well reduce you to tears – and that's why you need the help of an intelligent software platform like Exonar.

What does personal data look like?



What does personal data look like in real life?

For most organisations, the personal data they hold usually includes some combination of the many varied data groups shown here. Some of it will be classed as personal data (standard) and some of it will be sensitive personal data (special). Quick tip: always split the standard from the special and treat each accordingly.



- **General profile:** name, address, email, phone, DOB, relationship status, income bracket, dependents, banking details.



- **Appearance:** hair colour, eye colour, shoe size, height, weight, physical characteristics.



- **Workplace employee:** working hours, salary/wage, payroll, employment contracts, passwords, sick leave records, education, professional accreditations, CVs, testimonials/references, disciplinary records, HR assessments, tax codes, national insurance numbers, immigration/visa data, banking details and even passport numbers.



- **Workplace customer:** typically the customer profile data you hold in your CRM or equivalent systems.



- **Education:** personal details, exam or test grades, attendance and disciplinary records.



- **Private:** photos, videos, political opinions, cultural characteristics, IP addresses, browser cookies and geo-tracking data.



- **Health:** medical history, medication, GP details, genetic/biometric data and general fitness.

Some of it will be structured data – for instance held in a relational database or in a data vault. Some of it will be unstructured data – perhaps held on your email servers, in HR files or in collaborative working applications like Office365 or GoogleSheets.

Employers always handle, manage and store personal data – and we can confirm that this is definitely the case! We – you – collect

and use all the workplace information types detailed above, plus a varying range of profile data on the audiences our respective organisations serve.

Data litter



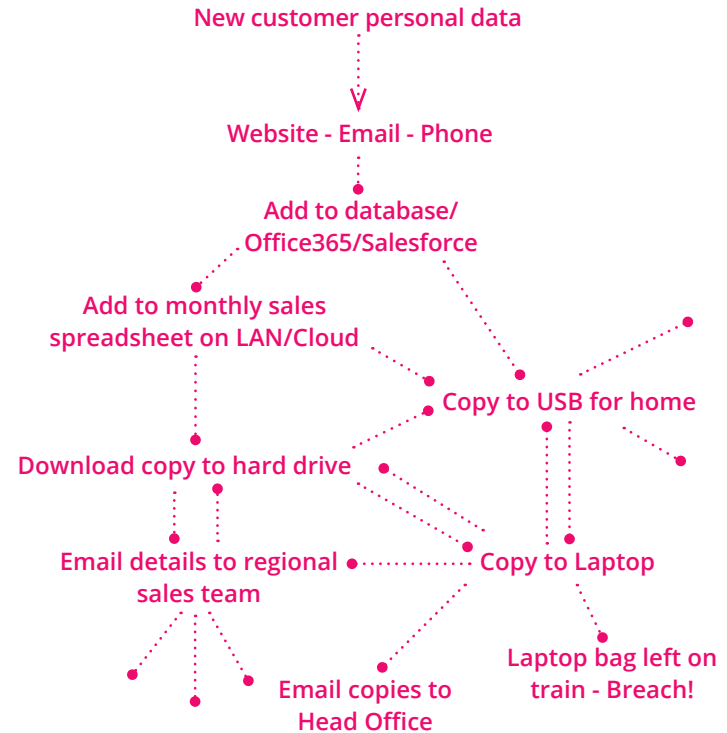
A quick word on 'data litter'

Some wag once quipped that “the road to hell is paved with well-intentioned exports”. We’ve all done it: downloaded files to our local drives, cc’d in loads of people when sharing spreadsheets and dropped work stuff onto USB data sticks. Data can get messy very quickly – and then multiply like rabbits. This unstructured information litter is what criminals, hackers and even unhappy employees look for; all that potentially sensitive stuff floating around your systems that they can steal or otherwise use to your disadvantage.

The reality is that data is rarely tidy unless you’re absolutely on top of your data game. The graphic below demonstrates how typically easy it is for a humble personal data file to develop a flamboyantly chaotic life of its own with very little encouragement



A phrase we regularly hear is “you won’t find any personal data or passwords in there.” But hey presto! That’s often what we find ...



Data governance under the all-important Article 30

In most cases, being GDPR compliant means fixing things but first you need to define what 'fixed' looks like, do you know what end state you desire? Regardless of the state your personal data is in, you need an information governance policy that is compliant and that sets clear rules for the way you handle personal data from this point forward. Think of it as the architect's drawing – it embodies the vision and always precedes the moment the builders break turf.

Having that sound policy plus a well-organised strategy for data mapping and inventory are key planks of compliance.



This is Article 30 of GDPR: it requires you to manage and maintain detailed records covering the personal data you process or use - and also how you do it. Ask yourself the following questions: they'll help you fine tune governance and keep minds focused as the implementation team starts to get its hands dirty ...

- Why are you using the data (what is your legal basis)?
- What are your categories of data subject and what actual personal data do you hold?
- What personal data are you exporting, to whom and where?
- How long do you store personal data and where is it held?
- Are you transferring personal data across geographical borders and if so, where?
- How do your data protection impact assessments mitigate risk to 'standard' and 'special' personal data?
- What is your information security strategy to prevent loss, theft or leak?



Some good rules of thumb

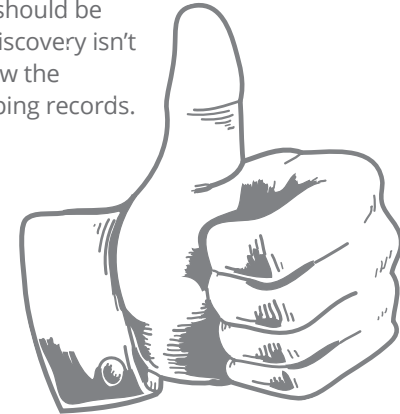
Two simple data mapping rules of thumb are 1) “good enough is good enough” and 2) “don’t get hung up on individual files”. Why? Because like a good hotel concierge, effective automated remediation will take care of the details.

- You could undertake the mapping manually but we really wouldn’t advise it – not only does it take time, resource and money, it will also be soul-destroying for the implementation team and it is inaccurate, relying on what is known by the team.
- Automation is your key. By plugging Exonar into your network, you’ll be able to discover in near real-time what personal data you have – from confidential documents, duplicate files and employment contracts to encryption keys, personal data and passwords... whatever you need to find.
- Good automation using machine learning and artificial intelligence also makes remediation a relative cinch.

You may be unsure about what data you are collecting, how you are handling it, who has access and how you are sharing it. Don’t panic: knowing that initial shape of your information is what the data mapping and inventory process is all about, giving you a starting point (where you are today) and that final destination (compliance!)

Time for the implementation team to start the serious leg-work. You know how to define the personal data you hold; you know what sort of personal data you should be handling (even if the reality of discovery isn’t initially compliant); and you know the Article 30 requirements for keeping records.

Now we can get cracking!



Let’s get mapping!



Let's map your data and build the inventory!

The implementation team we described back in Part 2 is working like a well-oiled machine. Representing each relevant part of your organisation, it is sharing knowledge about the current nature of the personal data you hold, building the governance picture you need to help achieve compliance. Remember...

- **Goals and governance:** always set your desired end state first.
- **Survey and data mapping:** discover your actual current state using the right automated software platform.
- **Remediation and fixes:** compliantly close the gap between the two.

Let's take a step-by-step look at the scope of thorough data mapping...



Step 1: understand how personal data currently flows into, through and out of your organisation

- Is it moving from one country to another, inside the EU to outside or vice versa? To be honest, this only really affects larger international corporates with widely distributed operations. (If you are strictly UK-centric and use UK-based cloud provision, life just got less complex).
- Is your data cloud based? If so, where is your chosen supplier and their infrastructure located?
- Is personal information being handled by third party suppliers, partners or contractors? If it only resides within your organisation, then controlling that data is simpler.

Identify, document and describe



Step 2: identify the personal data you have

- Is your data standard or special – or a blend of both? Is it general profile data – customers for example? Workplace and employer/employee-related? Or location data? For example, a cosmetics company selling online will likely have a lot of physical appearance data about its customers.
- **Formats:** are you holding personal data on paper, electronically, as audio, on video, in a database, in a spreadsheet or similar - perhaps in individual work email accounts? At this stage it doesn't matter if you're surprised by what you find – you get to fix it all later!
- **Collection:** is it coming in via website, by email, post, phone or across the social media platforms you operate? If you then share it with third parties, who are they, where are they, what do they use it for and how do they store it? Is it shared within your organisation creating multiple copies?
- **Responsibility:** who has access to the data and where does the personal data buck stop? They may be on the implementation team – perhaps not – so it's always a good idea to bottom this one out soonest.

Step 3: document and describe the flow processes

- Analyse the lifecycle of the information: establish how it is used day-to-day and whether or not there are uses (or types) you didn't know about.
- Establish exactly what types of information you need for the job in hand (you may be able to delete loads and also streamline what you collect).
- Compare and contrast the personal data you use today against what you will likely need in the future.
- Assess the information security measures you have in place to prevent data compromise.

As you can see, there's quite a bit of logical ground to cover and this is where intelligent automation comes into its own. The technology is out there (well, right here actually!) and in truth, you wouldn't want to approach data mapping and remediation without the correct software solution. The right tools for the job and all that.

Why map your data?



What does data mapping achieve?

A huge amount - it gives you a clear picture of your personal data: where it has come from, what you are doing with it and where it is going. It's the breakthrough moment that has just put you another goal up. Let's explore why 20/20 data vision is a terrific and easily achievable thing. You can ...

- Establish where you have got it right (under GDPR) and where you need to make corrections or adjustments.
 - Understand the personal data you have, define what you actually need and set future personal data formats.
 - Begin taking basic remedial actions – de-duping databases, correcting data categories and deleting old or obsolete data.
 - Begin preparing your data protection impact assessments (DPIAs) that establish relative risk for the personal data you hold.
 - Begin preparing your data retention and record-keeping policies/systems.
- Start designing systems and processes supporting data subject rights for areas like subject access requests, rectification, erasure and portability.
 - Evaluate your existing information security and data access measures and see what you need to change or strengthen.
 - Develop any necessary third party personal data handling safeguards.
 - Prepare a breach notification plan (the aim of course is never to need it!).
 - Assess your current position against your legal obligations under GDPR – in effect generating your fix list/compliance priorities.



The joy of remediation



The Joy of ... Remediation

You now know where you actually are - compared to where you need to be for compliance. You can now remediate the personal data you hold with a clear picture of the gaps.



Based on what you have discovered with data mapping, you can now establish improved procedures for data collection so the way you handle or process personal data day-to-day matches the rules you laid down in the data governance policy.



Start the tidying-up process for non-compliant data.



The secret to fast and accurate remediation is automation. The Exonar platform helps you achieve successful compliance, data subject access request processing, information security and governance, efficient risk management and document retention.

You are now productively overlaying reality onto the practical needs of compliance. You may find yourselves pretty close – perhaps not. If you've done the savvy thing and automated both discovery and fix phases with a solution like Exonar, then you'll be properly on track regardless. (However, if you need some help, please do get in touch!)



[Back to your privacy manifesto](#)



Time to revisit your Privacy Manifesto

Remember the Privacy Manifesto in Part 1? ([View it here](#)). As you navigate the data mapping and inventory process, it will become increasingly clear how well your methods of handling personal data under GDPR is going. That's why now is a good time to re-read that manifesto and ask yourself "are we making progress?"

- Do we understand what personal data we are processing and why?
- Do we have an effective data guardianship mechanism in place?
- Do we know which third parties are involved and what they are doing with that data?
- Have we got our approach to consent right?
- Are our information security processes on the right track?
- Do we know where the risk pressure points are?
- Is our strategy for handling data subject rights and access requests sufficiently robust?
- Do we have the right strategy in place to react quickly and effectively to a breach of any kind?

If you can answer 'yes' to the majority of these questions at this juncture, then your direction of travel is pretty good. In fact, it's a sensible idea to undertake this sense-check with the whole team regularly to keep on top of governance under GDPR. It gives you a chance to fine-tune and re-prioritise your actions smoothly.



The hard way or the Exonar way



There's data mapping the Hard Way ...

You may have read in the press about firms that have taken one look at their existing customer data, sighed a collective "oh dear" - and deleted everything to start afresh. Well that's one way to do it: the nuclear option. Yes, data mapping and inventory management can be a bit of a chore, but only if you lack the right human approach with the right technology solutions in place. As we have observed, doing it manually is a fool's errand - as is trying to make do by using existing software tools that may (or not) be able to complete the task, even at a price.



You could probably benefit from automated assistance if your organisation has been making disconcerting discoveries such as ...

- Not knowing what sort of personal data you hold.
- That data cannot be found easily.
- That storage protocols are ad hoc and accountability is vague.
- Or that data usage is inconsistent and information security possibly poor or non-existent.

... and there's data mapping the Exonar Way

While it's a strong team and thorough governance that makes for sound personal data handling, it's the technology platform behind the scenes that sets the tone and holds the compliance tune - one that connects quickly and simply with your existing systems to deliver the visibility of personal data you need.

GDPR is only one aspect of how you manage your data generally. Yes, you need to ensure compliance now, but in the long run, you need to establish clear, wieldy and real-time control over that data for the years to come. This is the real lesson of GDPR: it is merely the means, not the end in itself. At Exonar we have developed the ideal solution to support that long term end.

Don't just take our word for it!



Don't just listen to us ...

... listen to **Rowenna Fielding** - the self-confessed data protection nerd and leading UK information security blogger Miss Info Geek.



"Life under GDPR gives your data subjects far-reaching access and control rights to the information you hold on them. Be in no doubt that as awareness of those rights grow, the volume of requests that you must process regardless - and free-of-charge too - will multiply. Perhaps exponentially.

The more personal data you handle means more opportunity for error; the more data handling processes you need means greater chances for one of those moving parts to fail. The speed, accuracy and efficiency with which you map and control the personal data you handle is critical to compliance under GDPR; as is how you automate the management of subject requests in a timely, responsive and cost-effective way. Remember, robust compliance here will increase the intangible asset value of the data you hold and the value of your business more generally".



Now push on to the final whistle

The data mapping and inventory process is where all your initial planning comes to fruition. You get to match expectation to reality, see what data you really have and develop a clear idea of what it will take to move you towards compliance under GDPR. This will include satisfying the range of personal data management criteria and objectives that your planning has identified thus far.



At this point you may be well on the way to achieving compliance - or possibly realising that there is still much to do. Either way, data mapping gives you the visibility across personal data you need to act in a proportionate way. With the right tools for the job, it's really not that complicated.

We have the technology – and we can help you!



**Simplifying GDPR - Part 4:
Give yourself an easy life under
GDPR. Coming soon.**



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](https://www.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](https://www.sarlution.com)



Demo or free trial?





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

For a demo or free trial visit
exonar.com