Getting your business ready for GDPR

A guide to getting your business or organisation ready for General Data Protection Regulation (GDPR), a new European Union regulation strengthening data protection for European citizens.

34SP.com

DISCLAIMER

This guide pertains to EU data protection law in the United Kingdom.

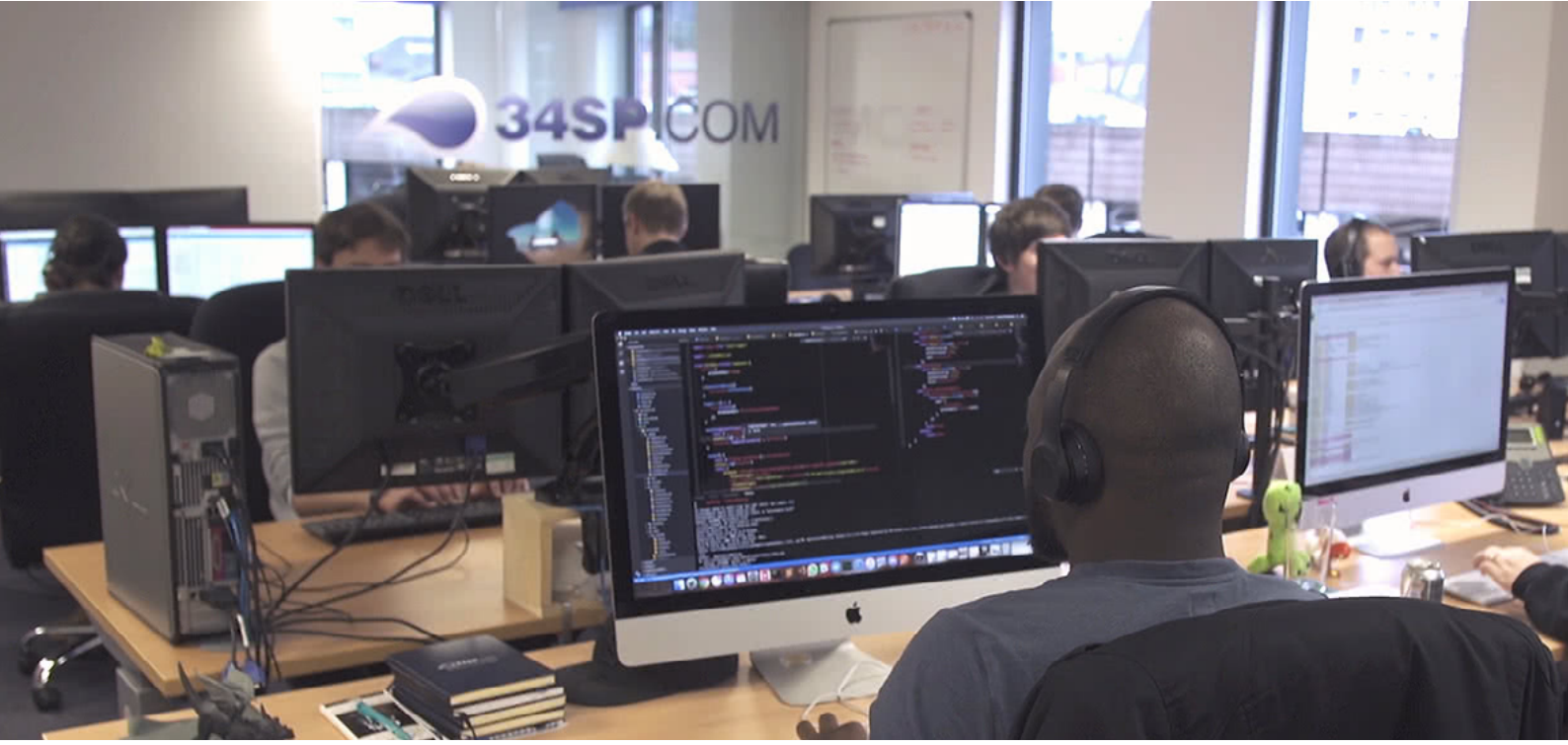
The data protection authority in the UK is the Information Commissioner's Office (ICO) at https://ico.org.uk. In the lead up to 25 May 2018 the ICO is publishing helpful, plain-English guidance on many aspects of GDPR compliance. Bookmark their page at https://ico.org.uk/for-organisations/data-protection-reform/ and visit it often.

The ICO also offers free, constructive, non-adversarial advisory visits. ICO staff will visit your premises, speak with you and your staff, and identify areas for improvement. You can request a visit at https://ico.org.uk/for-organisations/resources-and-support/advisory-visits/.

All guidance and URLs provided in this document are current as of February 2018 and are subject to change.

The information provided in this paper is not legal advice and its guidance is offered without prejudice.

Getting your business ready for GDPR



We're ready. Are you?

At 34SP.com we've been getting ready for the General Data Protection Regulation (GDPR). It's a new set of privacy and data protection rules which replaces the existing regime - all the way from the 1990s! - which we've known in the UK as the Data Protection Act.

GDPR applies to all businesses, organisations, sectors, and situations, whether you're a one-man band, a charity, or a growing corporation. And it's here to stay even after Brexit.

While we admit to being terrified at the start, we were amazed to find that GDPR's requirements are simple, common-sense, and ultimately very healthy. Working towards our compliance processes has already helped us to become a better business. That journey led us to commission this guide to help you, and your businesses, understand what you'll need to do to adjust to the new rules.

While this guide is not legal advice and should not be taken as such, we do hope it will help you feel more confident about what you need to know and what you need to do.

Principles of data protection

Data protection

Before we take a deep dive into what GDPR means for you, let's first take a look at what we mean when we talk about data protection.

In Europe, we have a cultural tradition of respecting privacy as a fundamental human right. That right is protected in law. European privacy laws have been enacted in the UK through domestic legislation, and to some extent, will continue to be so after Brexit.

There are three definitions you need to know about data protection.

GDPR, and the EU's principles of data protection and privacy in general, pertain to **personal data**. For our purposes, this means "any information relating to an identified or identifiable natural person."

Personal data can be one piece of information or multiple data points combined to create a record. It can be a contact form enquiry, a customer account, or an employee record. It can be a large file or a single data string.

Beyond personal data we also have **sensitive personal data**, which is defined as any information concerning an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health data
- Sex life or sexual orientation
- Past or spent criminal convictions

Sensitive personal data requires stricter protection, and the loss or breaches of such data has stricter consequences. (Quite right, too.)

Personal data is used by **data controllers** and **data processors**.

The **data controller** is a person or an entity, such as you or your business, which decides what data is processed, how it is processed, and whom it is shared with. ("Processed" simply means "used".)

The **data processor** is any person other than an employee of the data controller who processes the data on behalf of the data controller.

In your business, you may be a data controller, you may be a data processor, and you may be both. You may handle personal data you collect in your business, and you may handle personal data passed to you by a client or partner.

All of that personal data, regardless of source or purpose, must be protected to the same standards.

The existing rules

The original EU data protection framework, which dates all the way back to 1995, established that personal data must be;

- Processed in a manner which is fair and lawful;
- Used only for the manner in which it was intended to be used;
- Processed in a manner which is adequate, relevant, and not excessive;
- Accurate and kept up to date;
- Not kept for longer than its intended purpose;
- Processed in accordance with the rights of the people the data is about;
- Protected by technical and organisational security measures;
- Not transferred to third countries outside the EU which do not guarantee an adequate measure of data protection.

All of these existing principles stay under GDPR. What GDPR adds is new definitions and requirements to reflect changes in technology which simply didn't exist in the dialup era.

The new rules

First, GDPR **expands the definition of personal data** from the 1995 standard to include an individual's:

- Genetic data
- Biometric data
- Location data
- Online identifiers

Online identifiers means any personally identifiable information generated through interactions with a site, app, wearable, or online service which could identify the individual. Your web site will likely generate quite a few online identifiers.

GDPR introduces a new category of data, called pseudonymous data. This means that the personally identifying data is stripped away, and is held separately and securely, from the processed data. This is useful for groups working with a lot of research information or "big data".

Second, GDPR refreshes the requirements regarding privacy policies, data breaches, consent, and data about children, all of which we'll now explore.

And third, one of the main principles of GDPR is document it or it didn't happen. Document your processes, document your inventories, and document your discussions. In the event of a customer concern or a data breach, data protection regulators (such as the UK's ICO) can ask you for a copy of your documentation.

A note on Brexit

You may be wondering what will happen to your business's data protection obligations after the UK leaves the European Union.

The UK government has confirmed that the UK will adopt GDPR and go into it regardless of Brexit. After all, GDPR is extraterritorial. Compliance with its rules is the cost of doing business with European customers.

GDPR has already replaced the Data Protection Act within UK law and it is that, not the 1998 standard, which you should be working to achieve in your business.
GDPR will remain the UK's data protection law for at least several years after the UK has left from the European Union. This will come in the form of the Data Protection Bill, which as of this writing is working its way through Parliament.

European data protection standards require equivalency from non-EU third countries. This means that if you intend to continue doing business in Europe, you must continue to conform to the GDPR standard regardless of any post-EU data protection law that may replace GDPR in the years to come.

Put simply, you should work towards GDPR compliance as if Brexit will never happen and then stay in GDPR as if Brexit never will.

Get to know GDPR

Know what data you hold

The most basic step involved in GDPR compliance is awareness. Awareness means two things.

First, it means being aware of what GDPR is and what it will mean for you. You're reading this guide, so you've already taken the first step! Second, awareness means knowing what data your business holds, why you collect it, where it is stored, and who you share it with.

Take some time to really think about this. Conduct an audit of all the of the data collecting and processing activities you carry out in your business. That means online with your web sites and apps, in the front end with your contact forms and social sharing, and in the back end with your web site's database too. It means offline with paper forms, client records, or fulfillment information. And it means your archives too: server backups, zip drives, and even paper storage.

If your organisation's data collection and processing is regular (meaning it is a core part of your business), or if it includes sensitive personal data, or if that data you hold could threaten what are known as "people's rights and freedoms", your audit should include a full record of all your data collection and processing activities. These include:

- The purposes for which you are collecting and/or processing personal data;
- A description of the categories of individuals you are processing data about;
- A description of the categories of data you are processing;
- A description of the recipients of personal data you are transferring out of your organisation;
- A description of international (non-EU) transfers of personal data, including what safeguards are in place;
- Any data protection impact assessments you have carried out;
- A description of your data retention procedures, such as where data is stored, how long each category of data is kept, when data is deleted, and how deletion is verified;
- A description of your organisational security measures you have taken, including staff training and HR documentation; and
- A record of the policies you have put in place to deal with a data breach, including internal reporting mechanisms and contact structures.

Know about individual rights

Your GDPR journey should also include informing yourself about people's individual rights.

Under the existing EU data protection framework, data subjects have always had certain rights over your possession and use of the data you hold about them. These rights have been refreshed and enhanced for GDPR.

These rights include:

- The right to be **informed** about what you are doing with people's data, specifically through privacy notices;
- The right of users to **access** their data, which we will discuss next;
- The right to **rectification**, which quite simply means the right to correct any incorrect data you are holding;
- The right to **erasure**, commonly known as the "right to be forgotten", meaning the right to have certain kinds of data deleted under certain circumstances;
- The right to **restrict processing**, meaning the right for a user to ask you to stop using their data in certain ways;
- The right to **data portability**, which means the user's right to download the data they hold about you and upload it to a different service provider;
- The right to **object**, meaning a user's right to object to your uses of their data; and
- Rights in relation to **automated decision making and profiling**, which largely pertains to data used for the purposes of advertising, marketing, and behavioral analysis.

A data subject can invoke any one of these rights at any time.

Know about subject access requests

So how would a data subject invoke their individual rights?

One way that your customers and clients can do that is to file a subject access request (SAR).

This is a request made by someone whose data you hold or process, submitted in any format, for you to provide them with;

- Confirmation that you are processing their data;
- A copy of the personal data that you hold on them;
- Any other information you have in your possession about the subject, such as details of the data you have passed to third parties.

You'll need to detail your SAR process in your privacy notices, which we will discuss later.

SARs have time limits. In most cases, your organisation will need to reply to a SAR within one month. So, make sure they don't get lost.

Know about consent and legal basis

This is one of the most important aspects of GDPR. Pay attention at the back!

In most cases, all the data collection and processing you perform must be done with the consent of the people that data is about. If consent is not the basis, your use of data must be grounded in a *legal justification*.

That means that you cannot just collect and use people's data. You need a justifiable reason to do so. The ways you capture data from your users - whether that is through an active customer relationship or a passive web site visit - must be clear, documented, and verifiable. Your consent processes must be:

- **Active**: consent must freely given, specific, and unambiguous;
- Active consent must also be **positive**, meaning you have not presumed consent from a pre-ticked box, inactivity, or not selecting any option;
- Privacy must be presented as **granular** multiple choices, and not as a black-and-white, either-or choice;
- **Unbundled**: users cannot be forced to grant consent for one thing in order to receive another;
- **Named**: the user must be made aware of all specific third parties who will be receiving their data and why they will be receiving it through your privacy notice;
- **No imbalance in the relationship**: consent must not create an unfair relationship between the user and the data processor (such as an employer-employee relationship);
- **Verifiable and documented**: you must be able to prove who gave their consent, how consent was given, what information they were given, what they agreed to, when they consented, and whether the user has withdrawn their consent.

If your user of user data is not grounded in active consent, you must be able to justify your collection and processing of data in a **legal basis,** specifically that it is:

- Necessary for the performance of a contract;
- Necessary to comply with a legal obligation;
- Necessary to protect the person's vital interests (for example, providing emergency medical help);
- Necessary for the performance of a task in the public interest or in the exercise of official authority;
- Necessary for the purposes of the "legitimate interests" pursued by the controller or third party.

Your documentation must indicate:

- Who gave consent;
- How consent was given;
- What information they were given, and what they agreed to;
- When they consented (ideally a timestamped record); and
- Whether or not the user has withdrawn their consent.

A data subject may withdraw their consent for any reason at any time, and they do not have to provide you with a reason for doing so.

Know about Privacy by Design

Across all of your business's products and services, GDPR requires privacy and data protection to be built in as standard. If you are just starting your business, you are perfectly placed to get this right from the start.

Under GDPR, your customers and visitors should be able to expect enjoy optimal privacy as the default. Privacy can no longer be added on as an afterthought or, worse, made contingent on your customers activating a series of choices.

You should work to design your online and offline products and services around the Privacy by Design (PbD) framework. This is a series of principles which hold that:

- Privacy must be **proactive**, not **reactive**, and must anticipate privacy issues before they reach the user. Privacy must also be **preventative**, not **remedial**.
- Privacy must be the **default setting**. The user should not have to take actions to secure their privacy, and consent for data sharing should not be assumed.
- Privacy must be **embedded into design**. Privacy is a core function of the product or service, not an add-on.
- Privacy must be **positive sum** and should **avoid dichotomies**. For example, PbD sees an achievable balance between privacy and security, not a zero-sum game of privacy or security.
- Privacy must offer **end-to-end lifecycle protection** of user data. This means engaging in proper data minimisation, retention, and deletion processes.
- Privacy standards must be **visible**, **transparent**, **open**, **documented**, and i**ndependently verifiable**.
- Privacy must be **user-centric**. This means giving users granular privacy options, maximised privacy defaults, detailed privacy information notices, user-friendly options, and clear notification of changes.

Think of all the examples you've seen of services, sites, and apps that definitely did not have Privacy by Design. Learn from those mistakes and use PbD to rise above them.

What you need to do

Get everyone on board

Now that you've familiarised yourself with what you need to know, let's talk about how to apply GDPR to what you do.

This first part isn't technical. You should devise a GDPR awareness and implementation plan for everyone on your team, ranging from senior management to temporary staff. Make sure everyone understands what GDPR continues from the old Data Protection Act and what is new.

Remember that GDPR isn't a checklist or a one-off task. It's about your ongoing everyday business processes, whether they're about people and administration or data and tech. So everyone in your organisation, from your receptionist to IT to marketing all the way up to your directors, needs to be aware of how the rules are changing and what this will mean for the ways you work.

You'll need to speak with your contractors, partners, and third-party suppliers about their own GDPR plans as well, particularly if your business relationship involves the regular exchange of data. If a service you rely on isn't willing to get on board with GDPR, that can rebound onto you in the event of a privacy concern of a data breach - so it may well be time to find a new supplier.

Conduct Privacy Impact Assessments

If GDPR is about preventing problems from happening in the first place, there's no better way to do that than conducting a Privacy Impact Assessment, or PIA.

A PIA is the discussion your organisation holds about the privacy risks and protections inherent within a data-intensive project. You should conduct a PIA before any actual work is done, and if you have data intensive projects on the go already, it couldn't hurt to hold one retrospectively.

The PIA is where you document the difficult questions about your uses, sharing, and retention of data which, if done right, can prevent privacy complaints or data breaches from happening in the first place.

Good data protection practice encourages businesses to develop PIA templates which are unique to an organisation's individual needs, and you should develop one for your own data-intensive projects. At the least, your PIA template should include:

- A description of the data processing you are carrying out, including the legal basis for data processing;
- An evaluation of the necessity of the data processing;
- An evaluation of the proportionality of the data processing;
- A risk assessment regarding the data subjects;
- What measures you are putting in place to mitigate risk; and
- What security precautions you have taken.

Earlier we discussed the need to document your GDPR compliance. PIAs are critical to this. In the event of a data breach or a public concern, a data protection regulator such as the ICO can request a copy of your PIA.

Publicise your privacy notices

GDPR requires you to be much more public and transparent about the ways you use data. This will come in the form of privacy notices. GDPR-compliant privacy notices replace the privacy policies we all love to hate.

Your privacy notices must be clear, simple, written in plain English, and broken up into distinct sections and paragraphs. No more nonsense legalese babble hidden in the footer! In your notices, you must be crystal clear about what data you are collecting, how you are processing it, how that data is used, who you are sharing the data with, and what your users' rights are.

Privacy notices must give the users of your services real choices and options. Those options should be granular: privacy, as we have discussed, is not an either-or choice. So here's the place to put your privacy options and settings, such as the ability to opt-in or out, switch features on or off, or disconnect social sharing.

Your privacy notices should also clarify things like:

- If your collection and processing is not based on consent, what lawful basis applies;
- List all the third party partners and services providers with whom you share data, and note what that data is and how it is used. You must actually name them, and link to their privacy policies; the old chestnut of "we may share your data with carefully selected third parties" won't cut it under GDPR.
- You must inform users about their rights, including who to contact for a subject access request, and how they can complain to ICO if they feel you are not honouring their data;
- You must provide clear contact details for your company, your point of contact for subject access requests, and your data protection officer, if applicable.

Prepare for data breaches

Nobody wants their organisation to become the latest horror story about a preventable breach. So GDPR requires you to do everything possible to prevent data breaches from happening, and also to prepare for data breaches in advance.

You'll need to audit your technical systems for issues that could open the door to a data breach, whether that is unpatched software, poor antivirus software, or even ex-employees' accounts remaining active on systems.

Data breach preparation also means looking at what human aspects of your operations could contribute to a preventable disaster. Are new staff given data protection training in their inductions? Does everyone share one admin password? Can staff raise a concern without being punished for trying to cause trouble?

Under GDPR, certain kinds of data breaches must be reported to the ICO within 72 hours of discovery. In the event of a data breach, the ICO will want to see the following information:

- What kind of data was breached, how many individuals were affected, and how many data records were involved;
- How you were alerted to the breach, and by whom;
- Who is responsible for the breach, and how it happened;
- What consequences are happening;
- How you are putting things right;
- Who in your company is taking the lead on the investigation.

Could you pull all of this information together in real time? Run a drill to find out.

Decide whether you need a DPO

While privacy is everyone's job, GDPR introduces the responsibility for good data protection practice as an actual job. If your work involves large-scale processing of personal data, the data protection officer, or DPO, is a named individual who will carry formal responsibility for your organisation's data protection compliance.

Not all businesses will be required to appoint a DPO. You are welcome, however, to name one on a voluntary basis. This can be an add-on to an existing role, a part-time position, or even an external contractor. What better way to keep good privacy practice part of your everyday operations? Think of the DPO as the good cop who will keep your data protection processes on track, but also as the bad cop who will pull everyone's socks up from time to time.

If you do decide to name a DPO, there are certain rights and protections they must be given. The role has to be adequately resourced with whatever they need to do the job. Where applicable, they should regularly report to your directors. The DPO role also has to be protected. The DPO cannot be fired for raising concerns or asking uncomfortable questions, nor can they be told to ignore a problem.

Think about international transfers

Finally, GDPR requires you to be attentive to the data that you send outside the EU and its data protection framework. That means the data you actively send to partners and suppliers as well as the passive data transmitted to web hosts, cloud storage, and SAAS applications.

Personal data cannot be transferred outside of the EU to third countries unless that country ensures an equal and adequate level of data protection. So you need to ensure that your non-EU partners and service providers are protecting the data you send them in accordance with GDPR. And, yes, you'll need to get this down in your contracts and service-level agreements.

The most well-known framework for international data transfers is Privacy Shield, which applies to US companies doing business with European data. Take care to ensure that your US-based partners and third party service providers are Privacy Shield compliant.

You'll need to indicate in your privacy notices that data is being transferred outside the EU, and list all specific parties who receive that data as well as what they do with it. If you work across European borders, your privacy notices must also state your main country of establishment and your lead supervisory authority, in other words, the national data protection regulator who would handle a concern.

Where to begin?

Now that you're familiar with what you need to know and what you need to do to get to grips with GDPR, we suggest you begin your GDPR journey with the following steps:

- Use the ICO's resources to learn more https://ico.org.uk/for-organisations/data-protection-reform/
- Create a staff awareness plan
- Audit the data you hold
- Carry out a Privacy Impact Assessment for new projects, and run one retroactively on older ones
- Review your consent and legal bases for processing data
- Create GDPR-compliant privacy notices
- Implement PbD into your workflows for all future projects
- Review your Subject Access Request process
- Review your data breach process
- Review your technical security standards
- Review your human security standards
- Review contracts with third parties and suppliers
- Decide whether you need to appoint a Data Protection Officer
- Review your international data transfers
- Share this guide with your colleagues!

Let us know how you're getting on!