DIGITAL BOOST

power up your business

GDPR FOR BUSINESSES

Digital Scotland

business gateway

your gateway to business expertise

INTRO

DISCLAIMER

This guidance pertains to EU data protection law through its implementation in the United Kingdom. The data protection authority in the UK, including Scotland, is the Information Commissioner's Office (ICO) at https://www.ico.org.uk

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

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

TABLE OF CONTENTS

1 What is GDPR

2 Who does it apply to

3 Principles of data protection

4 Under 1998 DPA

5 Under 2018 GDPR

6 Know what data you hold

7 Know about individual rights

8 Know about consent and legal basis

9 Know about Privacy by Design

10 What to do to work towards compliance

11 Prepare for data breaches

12 Think about international transfers

13 A note on Brexit

14 Checklists

SECTION 1

WHAT IS GDPR

Data protection law is changing. On 25 May 2018 the EU's General Data Protection Regulation (GDPR), the successor to the Data Protection Act, becomes enforceable across Europe, including the UK.

GDPR is a complete update and overhaul of our existing data protection regime, which - somewhat incredibly - dates from 1995. The modernisation has taken rules designed for the age of floppy disks and brought them bang up to date for the age of the cloud.

For your small business or startup, the new rules will mean a new set of rules to follow about

- The data you collect;
- The ways you use the data;
- The ways you store the data; and
- The ways you share the data.

These new rules apply to your customer-facing tasks as well as your internal processes. They apply online and they apply offline. And, yes, they will apply even after Brexit.

GDPR will be enforced by large fines – up to 20 million euros or 4% of a company's global turnover – for non-compliance.

This guide is intended as a basic overview of the fundamentals of data protection under GDPR. It is not legal advice, nor is it a comprehensive inventory of your new obligations.

It is, however, designed to kickstart your thinking and inspire your compliance journey.

SECTION 2

WHO DOES IT APPLY TO

If you do business domestically or across the continent, GDPR and its requirements apply to you and your work.

Data protection law applies to all personal data about individuals collected or processed in Europe regardless of those individuals' nationality or citizenship. It applies whether the data is on paper or stored electronically.

Data protection law also applies across all sectors, industries, and situations.

There is no minimum size a business must be before the law applies; sole traders must work to the guidelines just the same as large corporations.

In the lead-up to GDPR, many industry groups and trade bodies are developing guidelines for their members which go above and beyond the baseline required by the legislation. If you belong to an organised industry, please check with your industry body.

SECTION 3

PRINCIPLES OF DATA PROTECTION

In Europe, privacy is enshrined as a fundamental human right. This right is protected in law using many instruments, including data protection law.

There are three critical 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**. Personal data, for our purposes, means information about a living individual who could be identified from that data, either on its own or when combined with other information.

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

The **data controller** is a person or an entity, such as your business, who, either alone or jointly or in common with others, determines the purposes for which and the manner in which any personal data are, or are to be, processed. "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. It must all be protected to the same guidelines.

SECTION 4

UNDER 1998 DPA

Data protection law defines personal data as "any information relating to an identified or identifiable natural person." This can be one piece of information or multiple data points combined to create a record.

Beyond personal data there is also **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 rightfully carries stricter punishments.

The 1995 data protection principles 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.

GDPR continues these principles, expands upon them, and adds additional responsibilities. From the 25th May Sensitive Personal Data will be known as Special Category data. This will be data that the GDPR says is more sensitive such as genetic and some biometric data and needs more protection. Personal data relating to criminal allegations or convictions will not be covered by GDPR as there will be specific safeguards for this kind of data.

SECTION 5

UNDER 2018 GDPR

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, whether that is an analytics record, a check-in map, a purchase history, the data from a health tracker, or the information exchanged through a social media login.

GDPR introduces a new category of data, called *pseudonymous data*. Pseudonymisation is "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information." In other words, the personally identifying data is stripped out, and is held separately and securely, from the processed data.

GDPR also imposes stricter requirements regarding privacy policies, data breaches, consent, and data about children, amongst other things.

HOW BUSINESSES ARE IMPACTED

GDPR became law in 2016, but it does not become enforceable until 25 May 2018. This has been designed to give businesses a two-year lead-in time to become fully compliant. It is not an overnight project, nor is it a one-off compliance task, and so you must begin your compliance process as soon as possible.

All businesses and organisations must comply with both the letter and the spirit of the law on data protection and privacy.

In the event of a dispute about your data protection standards or your wider approach to privacy, members of the public should contact your business to raise a complaint and give you the opportunity to deal with it first. They can then raise the matter with the UK's data protection regulator, the ICO, if necessary. If they have received a complaint about your business, the ICO will work with you in a constructive, non-adversarial manner to put things right.

However, the ICO does have a range of options available to them for businesses which fail to come into compliance, refuse to engage in responsible practice, commit clear violations of privacy, or permit data breaches to happen. These options include advisory warnings, formal reprimands (which are public), and orders to suspend activities. For truly egregious violations of privacy and data protection, GDPR permits regulators to impose dissuasive penalty fines which, in some circumstances, can be a measurable percentage of a company's global annual turnover.

Compliance, of course, should not be viewed as a thing businesses must do out of fear of penalties and fines. Compliance is about following best practice, protecting your customers, and giving your business an advantage over competitors who fail to respect their users' privacy.

Let's run through a very basic overview of what you need to know about your data protection obligations under GDPR.

We can divide this into two sections:

UNDERSTANDING HOW YOUR BUSINESS IS IMPACTED

- Know what data you hold
- Know about individual rights
- Know about subject access requests
- Know about consent
- Know about privacy by design

UNDERSTANDING HOW TO BEGIN YOUR COMPLIANCE JOURNEY

- Encourage awareness within your business
- Conduct privacy impact assessments
- Publicise your privacy notices
- Prepare for data breaches
- Decide whether you need a Data Protection Officer
- Think about international data transfers

SECTION 6

KNOW WHAT DATA YOU HOLD

The most basic step involved in GDPR compliance is being constantly aware of what personal data your business holds, why you collect it, where it is stored, and who you share it with.

You should audit all of the data collecting and processing activities you carry out in your business. In the event of a customer concern or a data breach, ICO can require you to produce a copy of your audit.

If your data collection and processing is regular (meaning it is a core part of your business), includes sensitive personal data, or could threaten people's rights and freedoms, your audit should include a full record of all of your data collection and processing activities, including

- 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 what technical security measures you have taken;
- 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.

SECTION 7

KNOW ABOUT INDIVIDUAL RIGHTS

Under European data protection law, individuals retain certain rights over your company's possession and use of the data you hold about them. These rights existed under the previous EU standard but have been greatly enhanced under GDPR.

These rights include:

1. The right to be **informed** about what you are doing with data, specifically through privacy notices, which we will discuss later;
2. The right of users to **access** their data, which we will discuss next;
3. The right to **rectification**, which quite simply means the right to correct any incorrect data you are holding;
4. 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;
5. The right to **restrict processing**, meaning the right for a user to ask you to stop using their data in certain ways;
6. 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;
7. The right to **object**, meaning a user's right to object to your uses of their data; and
8. Rights in relation to automated decision making and profiling, which largely pertains to data used for the purposes of advertising, marketing, and behavioural analysis.

These individual rights are **granular**. GDPR does not permit an all-or-nothing, either-or view of data processing. For example, a customer can object to your sharing their data with third parties for advertising purposes. You cannot require their data to be shared as a prerequisite for being a customer.
Know about subject access requests

One way that your customers and clients can invoke their individual rights is called 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

1. Confirmation that you are processing their data;
2. The processing information itself, which is similar to the information contained in a data processing/privacy notice;
3. A copy of the personal data that you hold on them;
4. Any other information you have in your possession about the subject, such as details of the data you have passed to third parties.

Your SAR process should be clearly explained in your privacy notices, which we will discuss later.

Your business must respond to a subject access request within one month of receipt. Because a subject access request is an invocation of fundamental rights, you cannot charge individuals an administrative fee or surcharge to exercise this right.

SECTION 8

KNOW ABOUT CONSENT AND LEGAL BASIS

In most circumstances, 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. Consent is just one of the lawful bases for processing, but there are alternatives to this. If consent is difficult, you can opt to use an alternative.

The consent mechanisms and legal bases you use to collect and process data must be clear, documented, and verifiable.

Your consent processes must be:

- **Active:** consent is 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 dichotomy;
- **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;
- **No imbalance in the relationship:** consent must not create an unfair relationship between the user and the data processor;
- **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 or not the user has withdrawn their consent.

If not grounded in active consent, you must be able to justify your collection and processing of data in a **legal basis**, of which there are 6, including consent:

- **Contract:** Necessary for the performance of a contract;
- **Legal obligations:** Necessary to comply with a legal obligation;
- **Vital interests:** Necessary to protect the person's life (for example, providing emergency medical help);
- **Public task:** Necessary for the performance of a task in the public interest or in the exercise of official authority, and this task has a clear basis in law;
- **Legitimate interests:** Necessary for the purposes of the "legitimate interests" pursued by the controller or third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

The ICO have an interactive tool that can help you find your correct lawful basis for processing. https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/lawful-basis-interactive-guidance-tool/

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.

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

SECTION 9

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!

Your customers should 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.

Work to design your product and services around the Privacy by Design framework, a series of principles which hold that:

1. Privacy must be **proactive**, not **reactive**, and must anticipate privacy issues before they reach the user. Privacy must also be **preventative**, not **remedial**.
2. 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.
3. Privacy must be **embedded into design**. Privacy is a core function of the product or service, not an add-on.
4. 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.
5. Privacy must offer **end-to-end lifecycle protection** of user data. This means engaging in proper data minimisation, retention, and deletion processes.
6. Privacy standards must be **visible, transparent, open, documented, and independently verifiable**.
7. 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.

SECTION 10

WHAT TO DO TO WORK TOWARDS COMPLIANCE

ENCOURAGE AWARENESS WITHIN YOUR BUSINESS

The most basic step involved in GDPR compliance is awareness. Everyone in your organisation, from your receptionist to your directors, needs to be aware of how the law is changing and what this will mean for the ways you do business. This guide can help, but it is only intended as a start. It is your responsibility to educate yourself on all the aspects of GDPR compliance which will impact your work.

You should devise a GDPR awareness and implementation plan for everyone on your team, ranging from senior management to zero-hours staff. Make sure everyone understands what GDPR continues from the old Data Protection Act and what is new. Allocate appropriate human and technical resources to GDPR implementation both before and after May 2018, and remember that these needs are not a one-off task: they must be incorporated into ongoing processes.

You should speak with your contractors, partners, and third-party suppliers about their own GDPR plans as well, particularly if your business relationship involves the exchange of data.

Please do be aware that in your journey towards compliance, there is a lot of good, accurate, and helpful GDPR advice out there. There is also a lot of marketing hype, scaremongering, and snake oil. Be vigilant about compliance advice which misrepresents, frightens, or threatens.

CONDUCT PRIVACY IMPACT ASSESSMENTS

A key aspect of privacy by design (discussed earlier) is a planning process called a Privacy Impact Assessment, or PIA.

A PIA is a process by which your organisation discusses the privacy risks and protections inherent within a data-intensive project before any actual work is done. Put simply, it is the phase where you sit down and ask 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.

Under GDPR, organisations will need to carry out DPIAs, Data Protection Impact Assessments, where they will be carrying out high risk processing.

PUBLICISE YOUR PRIVACY NOTICES

GDPR requires you to be much more public and transparent about the ways you use data requiring any information about data processing to be given at the time of data collection. The public face of compliance will be your privacy information 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 the user's rights are. This is known as the Right to be Informed and must be carried out in a simple manner with any information given to the user in an easy to access and read way.

Privacy information notices replace the privacy policies that we are used to seeing on web sites and in apps. They also replace the days of privacy statements being drafted by lawyers, for lawyers. The language must be simple and plain in a way that anyone can understand. In fact, if your web site or app is used by children, you are required to present your policy in language that a child can understand.

Your statement is a dialogue with your users. A dialogue, of course, works two ways. Privacy information 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.

Your notices should also clarify things like:

- If your collection and processing is not based on consent, what lawful basis applies;
- You must list all third party partners and services providers with whom you share data, and note what that data is and how it is used;
- You must inform users about their rights, including who to contact for subject access requests, 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.

Design also comes into play here. Privacy information notices should be presented in an attractive way, preferably a table with icons.

Privacy notices should be separated out from general terms and conditions statements.

SECTION 11

PREPARE FOR DATA BREACHES

Data breaches can be disastrous for your customers and for your business as well. The truth of the matter, however, is that data breaches - whether caused by technical or by human factors - are almost always preventable.

GDPR requires you to do everything possible to prevent data breaches from happening, and also to prepare for data breaches in advance. You should audit your technical systems, as well as your human processes, for things that could open the door to a data breach happening.

Preventing data breaches also requires you to take an honest (and, possibly, quite uncomfortable) look at what human aspects of your operations could contribute to a preventable breach. Are new hires being put onto systems without sufficient training? Are systems outdated, insecure, and not backed up? Have you been downloading data from the cloud to local laptops? What about your internal culture: can staff report an issue, either technical or human, which could lead to a data breach, without fear of reprisal?

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.

DECIDE WHETHER YOU NEED A DPO

While data protection is indeed everyone's job, GDPR introduces the responsibility for good data protection practice as an actual job. For organisations which engage in large-scale processing of personal data, the data protection officer, or DPO, is a named individual who will monitor and advise on an organisation's compliance with data protection legislation. It is not the DPO's legal and professional responsibility for data protection compliance; that responsibility lies with the organisation. Under the GDPR, you should appoint a DPO if you are a public authority, or if you carry out certain types of processing activities.

A DPO's name and contact details must be publicly stated in your organisation's privacy notices. Their details must also be supplied to your data protection regulator, as they will be the first point of contact for concerns and queries.

If you do decide to name a DPO, there are certain rights and protections they must have to do their job. They must be informed of all data protection issues in a transparent and timely matter; they must be made available to any user who has a concern over your use of their data; they must maintain secrecy and confidentiality at all times; they must be provided with all the resources necessary to do the job; and they must report directly to, and be in contact with, your highest level of management.

In addition, your DPO cannot be told how to do their job, they cannot be punished or fired for raising questions you might rather not hear, and they cannot be given other tasks or responsibilities which could cause a conflict of interest.

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. What better way to keep good privacy practice part of your everyday operations?

SECTION 12

THINK ABOUT INTERNATIONAL TRANSFERS

If your business trades internationally, you should be aware that under European data protection law, personal data cannot be transferred outside of the EU to third countries unless that country ensures an equal and adequate level of data protection.

To protect data once it leaves you, you must ensure that your non-EU partners and service providers have implemented a data protection system equal and adequate to GDPR for the European data you are sending them. This should be clarified in your contracts and service-level agreements.

To ensure you have a legal basis for non-EU data transfers, you must guarantee that your data is being transferred either under a framework agreement or through specific alternatives. The most well-known framework 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. Alternatives to framework agreements include intra-company transfers and contractual clauses, all of which should be dealt with by a solicitor.

You must 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. Your notices should also provide a means for users to object to their data being transferred outside the EU, keeping in mind that they need not provide a reason for asking you to do so. Individuals can object to their data being transferred internationally if there are no adequacy decisions or appropriate safeguards there to protect it.

If you work across European borders, your privacy notices must state your main country of establishment and your lead supervisory authority, in other words, the national data protection regulator who would handle concerns about your company.

SECTION 13

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**.

GDPR will replace UK law on the 25th May 2018 and it must be read jointly with the Data Protection Act 2018 which should be in force by the 25th May.

GDPR will remain the UK's data protection law for several years after the UK has left from the European Union.

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.

FOR FURTHER INFORMATION

In the lead up to 25th May 2018 the Information Commissioner's Office 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 has a Scotland office which you can learn about at https://www.ico.org.uk/about-the-ico/who-we-are/scotland-office.

The ICO also offers free, constructive, non-adversarial advisory visits. ICO staff will visit your office, 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/

SECTION 14
CHECKLISTS

SHORT CHEAT SHEET

We suggest you begin your GDPR compliance process with the following actions:

- ☐ Use the ICO's self-assessment toolkit to assess where you are on your data protection journey https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment-toolkit/
- ☐ Create a staff awareness plan for GDPR compliance
- ☐ Create an inventory of all the data you hold, both online and offline, internal and external
- ☐ Create privacy information notices for all products and services
- ☐ Decide whether you need to appoint a Data Protection Officer
- ☐ Review your consent processes across all projects
- ☐ Review your Subject Access Request process
- ☐ Review your data breach process
- ☐ Review your technical security standards
- ☐ Review your internal security standards such as staff training, HR documentation, and network access
- ☐ Implement PbD into your workflows for all future projects
- ☐ Decide whether you need to create a PIA template specific to your business's needs
- ☐ Review contracts with any third parties with whom you give or receive data
- ☐ Review your legal basis for sending or receiving data outside the EU
- ☐ Share this guidance with your colleagues

LONGER CHECKLIST TO KICKSTART PROCESSES

Awareness

- ☐ Have you devised a GDPR awareness and implementation plan for all employees, ranging from senior management to line staff?
- ☐ Have you allocated appropriate human and technical resources to GDPR implementation both before and after May 2018?
- ☐ Have you spoken with your contractors and suppliers about their own GDPR implementation plans?

The information you hold

- ☐ Have you conducted an audit of the information you hold online?
- ☐ Have you conducted an audit of the information you hold offline?
- ☐ Does your audit contain record of all processing activities?

Your users' individual rights

- ☐ Are you aware of the rights that individuals have over their data?
- ☐ Do you understand how these rights work in practice?
- ☐ Are you aware the user can invoke any of their rights at any time over any aspect of their data?

Subject access requests

- ☐ Have you created an SAR process?
- ☐ Is your SAR process detailed in your privacy notices?
- ☐ Do you have the technical and staffing capability to respond to subject access requests within 30 days?

Privacy notices

- ☐ Are your privacy notices written in plain English, with no "legalese"?
- ☐ Are your privacy notice broken down into clear sentences and short paragraphs?
- ☐ Do your notices provide a clear and transparent description of what data is collected, how data is processed, how data is used, who data is shared with, and what the user's rights are?

Consent and legal basis

- ☐ Have you determined which aspects of your data collection and processing are grounded in consent, and which aspects are grounded in a legal basis?
- ☐ Have you ensured that your consent processes are active, positive, granular, unbundled, named, do not create an imbalance in a relationship, are verifiable, and are documented?
- ☐ If not grounded in active consent, can you document and prove that your collection and processing of data is grounded in a legal basis?

Information about children

- ☐ Have you documented your processes for data about under-16s?
- ☐ Do children provide their information directly? If so, have you written a privacy notice for children in language they can understand?
- ☐ Are you documenting evidence that you have parental consent for any data processing for under-16s?

Data breaches

- ☐ Do you regularly audit your systems and processes for potential data breach issues?
- ☐ Do you know the criteria for a "high-risk", reportable breach?
- ☐ Have you created a template for GDPR's data breach reporting requirements?

Privacy by design

- ☐ Have you familiarised yourself with the principles of Privacy by Design?
- ☐ Have you reviewed your existing sites, apps, and processes for best PbD practice?
- ☐ Have you developed a Privacy Impact Assessment template unique to your business's needs?

Data Protection Officers

- ☐ Have you determined whether you need a DPO by law?
- ☐ If not required, have you considered appointing a DPO voluntarily?
- ☐ Have you publicised your DPO's details in your privacy notices?

International data transfers

- ☐ Are all of your partners and third party service providers in non-EU countries familiar with the new requirements under GDPR?
- ☐ Are your US-based partners and third party service providers Privacy Shield compliant?
- ☐ Are you including and requiring GDPR compliance in your contracts with partners and service providers?

DIGITALBOOST
power up your business

CONTACT YOUR LOCAL BUSINESS GATEWAY OFFICE

Get expert advice on this and a wide range of topics for free at your local Business Gateway office.

bgateway.com/local-offices