Gaby Hardwicke SOLICITORS

Briefing Note: Data Protection

Introduction

This Briefing Note highlights some of the key legal obligations your business should consider when dealing with Personal Data about Customers, Suppliers and Employees in the ordinary course of business, as well as some key areas that have been affected by the changes to data protection legislation since the introduction of the General Data Protection Regulation (GDPR) in 2018.

This briefing Note should not be relied upon as legal advice and you should contact us for advice on your specific circumstances.

Briefing Note
Reviewed September 2025

Summary:
An overview of the key legal obligations your business should consider when dealing with Personal Data about Customers, Suppliers and Employees in the ordinary course of business.

For detailed advice on all data protection matters please contact:

Mark Williams
Corporate Partner
mark.williams@gabyhardwicke.co.uk

01323 435900

William Baker
Associate Solicitor
william.baker@gabyhardwicke.co.uk

01323 435900

Background

The key legislation impacting on personal data in the UK is the Data Protection Act 2018 (**the Act**), which gave effect to the GDPR. Post-Brexit, the UK has retained, for the most part, the provisions of the GDPR. The relatively subtle modifications have caused the retained-law version of the GDPR to be referred to as **UK GDPR**. However, the underlying principles are broadly the same.

As well as clarifying and codifying key principles of protecting personal data, the Act also introduced new obligations on organisations processing Personal Data as well as substantial fining powers for the Information Commissioner's Office (**ICO**) for breaches of these obligations.

Personal Data

Personal Data is defined as being any information relating to an identified or identifiable natural person. If a natural person (i.e. a living human individual) can be identified, whether directly, or indirectly, it is likely that that information is classed as 'Personal Data' for the purposes of the Act. This will include obvious examples, such as names, addresses and contact details, but also less common examples, such as IP addresses if they can be used to identify a Data Subject.

In addition to this general class of Personal Data, there is also what is called 'Special Categories of Personal Data'. These 'Special Categories' require additional levels of protection as they are considered to be sensitive in nature. They include:

- Race;
- Ethnic origin;
- Political opinions;
- Religious of philosophical beliefs;
- Trade Union membership;
- Genetic data;
- Biometric data;
- Health data;
- Sex life; or
- Sexual orientation.

Sometimes, you may see reference to criminal convictions and offences lumped in with these Special Categories as they are also subject to higher (although, separate) levels of protection.

Briefing Note: Data Protection

Personal Data that is anonymised (to the extent that it can no longer identify a Data Subject) is excluded from the scope of the Act, but Personal Data that is only pseudonymised (data that on its own does not identify a Data Subject, but when used with additional information can identify a Data Subject) may still be caught by the Act. It is therefore important that if Personal Data is only pseudonymised, that any additional information is stored safely and securely to avoid any risks of unlocking the Personal Data.

Collecting and Processing Personal Data

In the broadest terms, 'processing' is the term used to describe when an organisation takes any action with someone's Personal Data. This often includes storing or otherwise using that Personal Data (whether in the course of selling goods or services, or storing a name on a mailing list) and will continue until that Personal Data is destroyed.

It is therefore clear that almost every organisation will process some kind of Personal Data in their course of business.

Controllers and Processors

The Act differentiates between a 'Data Controller' and a 'Data Processor'.

'Data Controllers' will typically be an organisation that decides to collect or process Personal Data and will decide what the purpose or outcome of that processing should be. 'Data Processors' on the other hand are typically told by a Data Controller what to do with Personal Data. This does not mean that a Data Processor cannot also act as a Data Controller. If the Data Processor acts without the instruction of the Data Controller in such a way that it determines the means and purpose of the processing, it will be considered to be acting as a Data Controller in respect of that set of Personal Data. It is therefore possible to be both a Data Controller and a Data Processor in respect of the same set of Personal Data depending on the nature of the processing.

It is important to note that employees of a Data Controller are not Data Processors, but are agents of the Data Controller. This will mean that a breach of any obligations under the Act by an employee will be construed as a breach by the employer as Data Controller.

Whilst a Data Controller will ultimately be responsible for the highest level of compliance with the Act (including being responsible for paying the data protection fee), Data Processors can also be held responsible for breaches of certain obligations. This distinction is therefore important in terms of liabilities under the Act and should be accurately recorded in a Data Processing Agreement, or as part of a general contract.

In some situations, it is possible for two or more parties to be 'Joint-Controllers'. These arrangements are often complex in that they will involve a great deal of commonality, with agreement needed in respect of a common objective, the same purpose(s) etc. In these situations, it is important that any liabilities are adequately set out in a Data Processing Agreement as each individual Data Controller may have an action brought against them for failing to comply with any obligations under the Act.

Principles

The Act requires organisations that process Personal Data to process that Personal Data in accordance with the following principles:

- **Lawfulness, fairness and transparency**
    - Ensuring that you have a valid legal basis for processing the Personal Data and not doing anything to otherwise breach any other laws. You also need to use the Personal Data in a

way that is fair, including ensuring that you are open and honest with Data Subjects about how you will use their Personal Data.

- **Purpose limitation**
    - Being clear about your purposes for processing and not processing the same data for different purposes without the consent of the Data Subject, or identifying a clear function or obligation set out in law.
- **Data minimisation**
    - Only processing Personal Data that is necessary and related to your stated purpose.
- **Accuracy**
    - Taking steps to ensure that the Personal Data you process is accurate and not misleading. If you subsequently find out that any Personal Data you hold is incorrect, you must take reasonable steps to correct it.
- **Storage limitation**
    - Ensuring that you do not store any Personal Data for longer than is required (either for its purpose or for any legal or regulatory reason).
- **Integrity and confidentiality (security)**
    - Ensuring that you have in place appropriate technological and organisational measures in respect of the storage and use of Personal Data. In short, this requires that you conduct risk assessments and ensure that the Personal Data is stored securely.
- **Accountability**
    - Taking responsibility for your processing of Personal Data.

These seven principles underpin the entirety of the Act and, whilst they themselves are somewhat abstract, their application can be seen when you start processing Personal Data.

Legal Basis

There are six lawful bases for processing Personal Data. Organisations must have a valid lawful basis in order to process Personal Data, and you will need to ensure that, even with a valid legal basis, the processing is 'necessary' in order to ensure compliance with the Act.

The legal bases are:

- **Consent**
    - The Data Subject has given clear consent for the processing to take place. It is worth noting that this consent can be withdrawn by the Data Subject and therefore this legal basis is typically not used except in cases where no other basis exists.
- **Contract**
    - It is necessary to process Personal Data for the performance of a contract with the Data Subject (for example, the provision of on-going financial services).
- **Legal Obligation**
    - It is necessary to process Personal Data in order to comply with the law (not the performance of a legally binding contract).
- **Vital Interests**

    - The processing is necessary to protect someone's life.
- **Public Task**
    - It is necessary to process Personal Data for you to perform a task as part of your official functions or in the public interest (this will most often be seen in public authorities who are required by law to conduct a specific function, such as the collection of Council Tax).
- **Legitimate Interests**
    - It is necessary to process Personal Data for the legitimate interests of an organisation (whether you or a third party) unless there is a good reason to protect a Data Subject's rights which overrides those interests. This often applies in situations where the scope of processing is minimal. Organisations should conduct a 'Legitimate Interests Assessment' to demonstrate compliance with the Act.

Identifying which legal basis (or bases) you use will be important at the outset as it is difficult to 'swap' purposes at a later date. Whilst you can 'add' purposes, again these are issues that you should consider at the start of the process, and these should be recorded by your organisation to demonstrate your consideration of the application of the Act on your processing.

It is also important to consider which basis (or bases) you are relying on as it may have an impact on the individuals' rights under the Act.

Practical Steps

Organisational procedures

Identifying and recording appropriate procedures to have in place will often be one of the first steps an organisation will take after determining the scope of their processing. The exact nature of these procedures will depend on the scope, volume and nature of the processing. Some key considerations will include ensuring that any Personal Data held is held securely (irrespective of whether it is stored on a computer or in physical form), codifying who has access to the Personal Data and ensuring that any access to the Personal Data is consistent with the purpose for which the Personal Data is held.

Contracts

Whether you are a Data Controller or a Data Processor, having the relationship properly identified and codified in some form of agreement will be a very important step to take. Most commonly, parties will enter into Data Processing Agreements that set out the specific details of what the Data Processor will do on behalf of the Data Controller, as well as detailing any issues with regards to indemnities (the promise to pay costs in respect of a breach of a term of the agreement). It will also clarify certain responsibilities with regards to Data Subjects' rights (i.e., who the Data Subject must approach in the event of a breach, and what, if any assistance one party should give to the other).
If you are a Data Controller and looking to share Personal Data (rather than have another party simply process that Personal Data), a Data Sharing Agreement will be required. Unlike Data Processing relationships, a Data Sharing arrangement requires that the parties identify a separate legal basis for sharing that Personal Data.

Privacy Policies

However you collect or otherwise process Personal Data, you will want to ensure that this is adequately set out in a Privacy Policy. A Privacy Policy is a short document that sets out who you are, what Personal Data you are collecting, how you collect it, what you do with it and who you share it with. It also sets out the statutory rights that Data Subjects have in respect of the organisation collecting their Personal Data.

Briefing Note: Data Protection

Some organisations may only require one Privacy Policy. However, often times, larger trading companies will require multiple Privacy Policies. It is not unusual for companies to have separate Privacy Policies in respect of employees, customers and use of the organisation's website.

The benefit of separating Privacy Policies in this way is that it often makes things clearer for whoever is reading the Privacy Policy. For example, the purpose, basis and method of an organisation collecting the Personal Data of its employees will be separate from that same organisation's reasons for collecting the Personal Data of its customers. As a result, a customer may not be able to ascertain what Personal Data the organisation holds on them if the Privacy Policy is unnecessarily convoluted.

Employment

You will need to ensure that your organisation has in place a well-drafted Privacy Notice. Employees and workers will need to be informed about their data privacy, at the point of data collection or when requested in accordance with the GDPR.

Personal Data must be processed lawfully, fairly and in a transparent manner. It is best practice to have employees acknowledge receipt of the Privacy Notice at the commencement of their employment and that its contents have been understood. In summary, it will inform the employee how the organisation will use and share their Personal Data as well as their rights in certain circumstances, including how to request disclosure of their Personal Data and if necessary, placing restrictions on the extent to which it is processed.

Individuals' Rights

Ensuring that Data Subjects can quickly and easily exercise their statutory rights is one the key focuses of the Act. The Act provides for the following rights:

- the right to access personal data held about them (subject access request);
- the right to be informed about how and why their data is used;
- the rights to have their data rectified, erased or restricted;
- the right to object;
- the right to portability of their data; and
- the right not to be subject to a decision based solely on automated processing.

You will need to ensure that you have procedures in place for Data Subjects to exercise these rights. Often this will be through ensuring that your Data Protection Officer (DPO) or person in charge of Data Protection at your organisation has their email address or other contact details available to Data Subjects.

Unlike under previous Data Protection laws, organisations are not permitted to charge a Data Subject in the course of them exercising their rights under the Act, unless such exercise is determined to be 'vexatious'. Even in such cases, only a 'reasonable' fee may be charged.

DPO's

Certain organisations (for example, public authorities) are by law required to have a DPO in place. For most businesses, this won't be mandatory, but having an employee in place to deal with ensuring your organisation's compliance with the Act is often advisable, especially if your organisation is regularly processing Personal Data, or has an international element to its processing.

Briefing Note: Data Protection

Data Protection Impact Assessments

In certain cases where there is likely to be a high risk to individuals in relation to the processing, organisations must conduct a Data Protection Impact Assessment (DPIA), This is a process by which organisations can identify the scope of the processing, the measures put in place, the risks to individuals and any measures that could be taken to mitigate these risks. If, as a result of this process, you cannot identify a way to mitigate the risk, you must speak to the ICO before conducting the processing.
Whilst conducting a DPIA is only mandatory in situations where there is likely be a high risk of harm, it does not mean that DPIA's aren't useful in other areas. Organisations who process a high volume of Personal Data may benefit from undertaking DPIA's to see whether there are any issues with their own internal processes. If you are engaging a new Data Processor for Special Categories of Personal Data, it may be that a DPIA is undertaken to ensure that you have in place adequate security measures to prevent damage to that Personal Data in transit.
Other than in routine processing, conducting a DPIA can often have merits as it will involve you taking stock of what processes you have in place and what improvements can be made to ensure that you are complying with the terms of the Act.

Personal Data and the Internet

If you operate a website, there will be even more scope for the collection of Personal Data, whether you intend to or not.
Oftentimes, websites will 'track' users for analytical purposes throughout the website. This uses small text files called 'Cookies'. Whilst Cookies are designed primarily to monitor functionality of the website and provide analytical feedback, they will often track user's IP addresses, which potentially falls under the scope of Personal Data.
Some websites also require that individuals give Personal Data expressly, either to sign up to a mailing list or to gain access to certain members-only sections of the website. If you sell goods or services on your website, financial information (such as banking and address data) will need to be processed in order to take payment.

It is therefore important that all websites consider the need for Privacy Policies. Those websites that potentially handle Special Categories of Personal Data will also want to ensure that regular DPIA's are undertaken and risks continually assessed and mitigated against, whether through developments in website security infrastructure, or a review of what Personal Data is actually required.

Breaches

Breaches of the Act can result in significant financial fines. The most serious breaches are (at the date of this Briefing Note) capped at £17.5million or 4% of a business's annual global turnover, whichever is higher. There is also the reputational damage that comes with large-scale breaches.
Having internal (and, where appropriate, contractual) procedures to deal swiftly with a Personal Data breach will be important. This is often where it is most useful to have a DPO.
The ICO website also has helpful guidance on when you need to report a Personal Data breach, including a reporting portal.

Enquiries about Personal Data

Depending on the size and scope of the processing, organisations will have different sets of requirements placed on them. However, compliance with the Act at all levels is important. Here at Gaby Hardwicke our specialist corporate and commercial lawyers can help you at all stages of your business, from incorporation to sale, to ensure that you are compliant with the Act.
If you would like to know more about this topic, or our other legal services, please contact Mark Williams…

Gaby Hardwicke SOLICITORS

Briefing Note: Data Protection

If you would like to know more about this topic or our other legal services, please contact Mark Williams or William Baker on 01323 435900 mark.williams@gabyhardwicke.co.uk william.baker@gabyhardwicke.co.uk

Gaby Hardwicke Solicitors
33 The Avenue
Eastbourne
East Sussex
BN21 3YD

Tel: 01323 435900
info@gabyhardwicke.co.uk
www.gabyhardwicke.co.uk