GDPR:

ARE YOU PREPARED?

FIND OUT WHAT YOU SHOULD BE THINKING ABOUT WHEN IT COMES TO GDPR COMPLIANCE FOR YOUR BUSINESS

BAKERLAW
SOLICITORS®

BAKERLAW
SOLICITORS®

CONTENTS

BAKERLAW
SOLICITORS®

WHAT IS THE GDPR?

On 25th May 2016 the General Data Protection Regulation (GDPR) was passed into EU law. Exactly two years later, the deadline for compliance with and enforcement of the regulation will arrive. Put simply, the GDPR is a step towards the greater harmonisation of data protection law throughout the EU in a society which is increasingly dependent upon the amalgamation and fluidity of data.

Prior to the GDPR, the main source of legislation governing data protection law was the Data Protection Act 1998 (DPA), which implemented the EU Data Protection Directive. It is important to note that as a regulation, the GDPR is directly effective in EU Member States, meaning that no national legislation is required to implement it. Notwithstanding the UK's withdrawal from the EU in March 2019, the standards codified in the GDPR will continue to apply in the UK. This will, after all, be necessary to facilitate the free movement of personal data between the UK and EU regarding any future trade relationship.

WHY SHOULD I CARE?

Under the current DPA, the Information Commissioner's Office (ICO) has the power to impose fines of up to £500,000 in the event of a breach. The ICO has not shied away from exercising the full extent of its power as a punitive force and as a deterrent. To take but one example, in 2016 the telecom group TalkTalk was fined £400,000 for its inadequate protection of its customers' data. Under the GDPR, the ICO will have the power to impose fines of up to €20m or 4% of global annual turnover of the undertaking – whichever is the higher of the two.

As businesses have already been given a two year grace period to align their business practices with the new regulations, we should not expect any leniency from the ICO beyond the 25th May 2018, the date on which businesses are to be compliant with the GDPR.

Irrespective of these punitive measures, the safeguarding of customer data is now seen as good business practice and consumers are increasingly concerned about how their information is being protected. This increased awareness therefore presents a unique opportunity for businesses to set themselves apart from their competition.

WHO DOES IT APPLY TO?

The GDPR is intended to regulate the ways in which those who hold personal data can store and use it. The current DPA only imposes obligations on 'data controllers', however the GDPR extends the scope of these obligations to include 'data processors'.

- Data controller: *determines the purpose and means of processing personal data.*
- Data processor: *responsible for processing personal data on behalf of the data controller.*

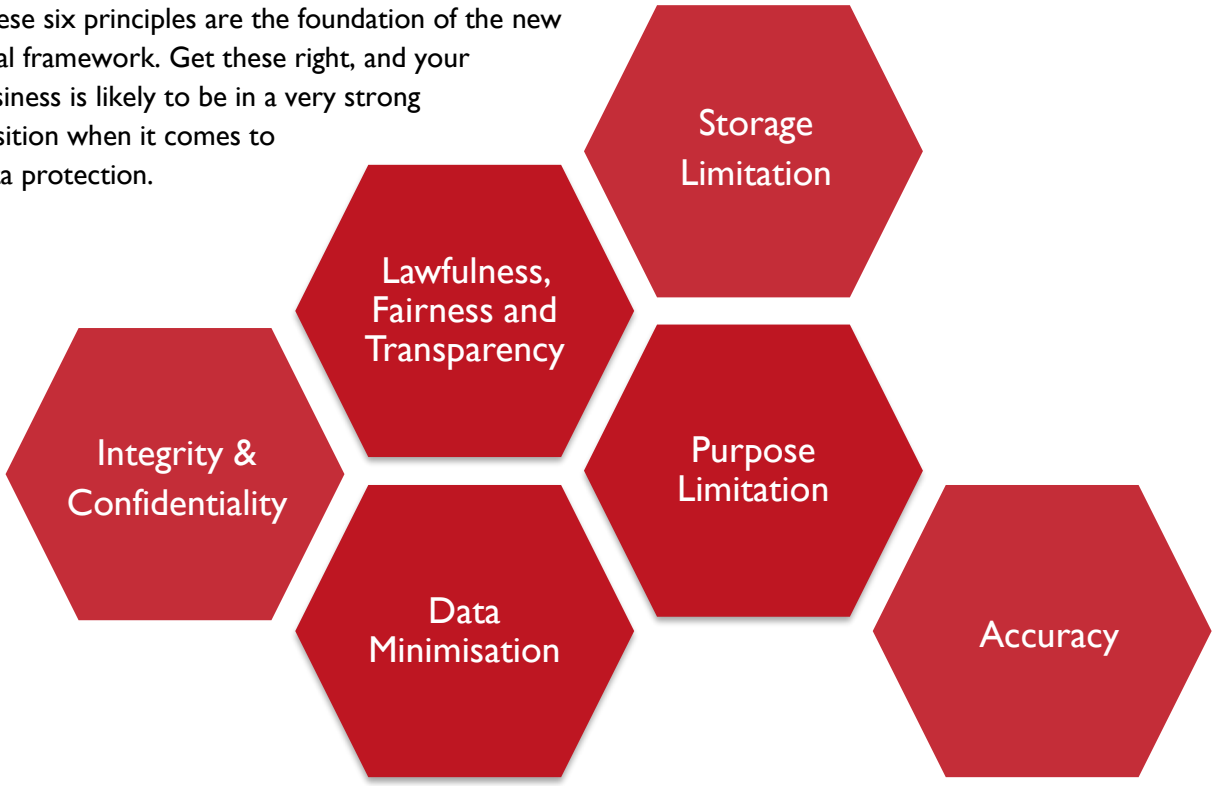
WHAT DOES IT APPLY TO?

The term 'personal data' has been expanded upon, broadening the scope of the regulation. Importantly, the data controller or processor need not operate in the EU for the GDPR to be applicable; the regulations apply to the personal data of those individuals located in the EU.

- Personal Data: *any information relating to a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, number, location data, online identifier, or to the specific physical, physiological, genetic, mental, economic, cultural or societal identity of that natural person.*

THE SIX PRINCIPLES OF THE GDPR

These six principles are the foundation of the new legal framework. Get these right, and your business is likely to be in a very strong position when it comes to data protection.



1. **LAWFULNESS, FAIRNESS AND TRANSPARENCY:** personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
2. **PURPOSE LIMITATION:** personal data must be collected for a specified purpose in accordance with a legitimate basis on which to process that data. It must not be processed in such a way which exceeds or is contrary to that purpose.
3. **DATA MINIMISATION:** data processors should only keep data to the extent that it is necessary to do so – any excess data that is not relevant for the specific purpose should be deleted.
4. **ACCURACY:** every reasonable step must be taken to ensure that personal data is accurate, current and still necessary for the processing purpose.
5. **STORAGE LIMITATION:** processes should be put in place which facilitate the identification of data subjects whose data is no longer necessary for the purpose for which it was processed.
6. **INTEGRITY AND CONFIDENTIALITY:** personal data must be processed in a manner which ensures that it is appropriately protected.

ACCOUNTABILITY

Arguably, one of the most significant changes implemented by the GDPR that businesses should be aware of is the explicit accountability on the part of the data controller:

"The controller shall be responsible for, and be able to demonstrate compliance with [the six principles]".

It is no longer sufficient to comply with data protection law – there is now an evidential burden on data controllers to be able to positively demonstrate that they do as a matter of fact comply. Because of this, documenting processing procedures and making detailed records of activity surrounding personal data is more important than ever before.

Businesses should implement technical and organisational measures which ensure and illustrate that they are GDPR compliant. When considering internal policies and procedures, bear in mind the six principles of GDPR and how you are demonstrating these. For example, ensuring frequent reviews of the relevance of data you hold in relation to the prescribed lawful basis and prescribed purpose is indicative of an awareness of the principle of data minimisation.

YOU SHOULD BE ABLE TO DEMONSTRATE...

- What data you are holding, where you obtained it from and where it is being stored.
- Who has access to it.
- The lawful basis on which you are justifying its retention and processing. If this requires positive action on behalf of the data subject (e.g. consent) you should hold proof of how you obtained their consent and what they consented to.

DOES MY BUSINESS NEED A DATA PROTECTION OFFICER?

You are under a duty to appoint an independent individual to be your data protection officer who will monitor your internal compliance, if:

- Your core activities require large scale, regular and systematic monitoring of individuals;
- Your core activities require large scale processing of special categories of data (*see Art. 9.1 GDPR*) or data relating to criminal convictions or offences; or
- You are a public authority.

LAWFUL PROCESSING OF DATA

The requirement for a lawful basis as a prerequisite to processing personal data is not new – the same was required under the DPA. The most significant change under the GDPR is the emphasis on the accountability of the data controller and transparency of the lawful basis for processing.

It is a common misconception that data controllers are required to obtain specific consent to enable them to retain personal data. There are in fact six distinct lawful bases, of which, consent is just one. A data controller must be able to justify the retention of personal data under one of these. The justification must have been determined and recorded *before* the data processing takes place. If this is not the case, the data controller will be in breach of the first principle of the GDPR: that the processing be *lawful*.

It is important to recognise that there is no one-size-fits-all approach. The lawful bases are contextually dependent and if the circumstances surrounding the processing and use of particular data changes, the basis should be reassessed for appropriateness. If the data controller does not identify the correct basis from the start, the processing will be in breach of the regulations and a data controller is not entitled to change the basis under which data is processed at will.

EXISTING PROCESSING:

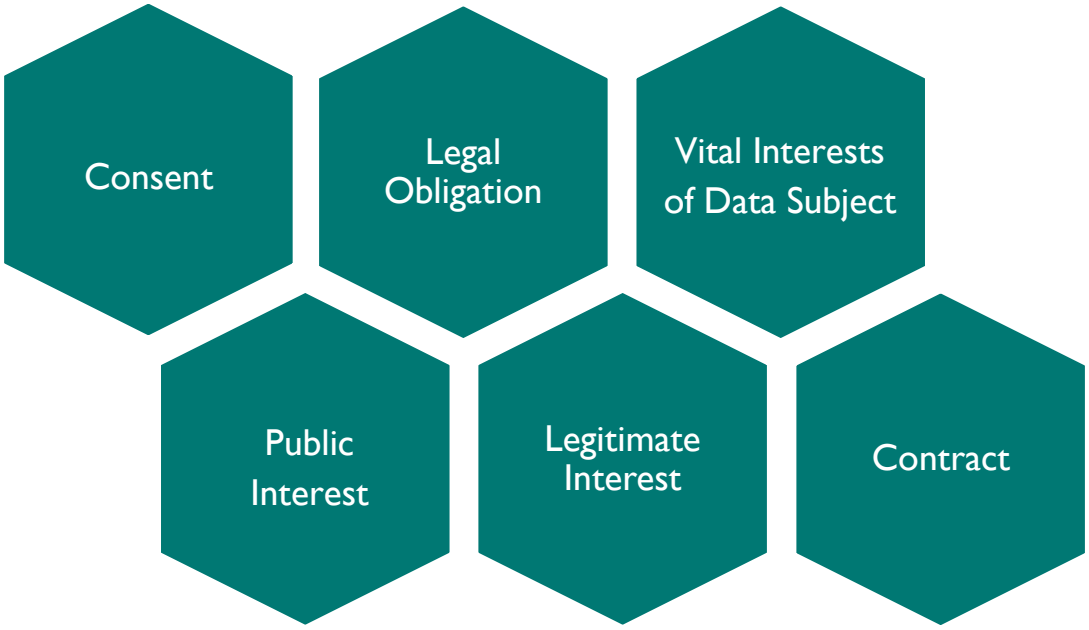
- Review ongoing data processing and determine whether or not it can be justified under one of the lawful bases.
- If it can, the basis which is being used to justify the particular processing should be documented.
- You must retrospectively inform the data subject of the basis on which you are holding their data before 25th May 2018.

NEW PROCESSING:

- Processing of new data should not take place unless and until it has been established that there is a suitable basis on which to justify it.
- If and when this has been established, once again, this should be documented.
- Inform new data subjects of the basis on which you are holding their personal data.

THINGS TO CONSIDER WHEN SELECTING A LAWFUL BASIS:

- What are you trying to achieve? As a data processor you need to justify your processing in pursuit of a purpose; be clear on what this is.
- Is your processing proportionate and necessary to achieve your purpose? It need not be *absolutely* essential, however there should not be a less intrusive way of achieving the same outcome by reasonable means.
- The basis on which the processing of data is justified will influence the rights of the data subject, e.g. the right to erasure (to have one's data removed) does not apply to processing justified on the basis of a legal obligation or performance of a public task.
- There is a requirement under the GDPR that personal data is processed transparently. In practice, this means that as a data controller you must be open and honest about the ways in which you process and use personal data. The bases on which you are processing data should be detailed in your privacy policy – if it is not already, this needs to be updated before 25th May 2018.
- The principle of accountability highlights the importance of making a record of the basis under which you are processing personal data and the justifications for using that basis.



CONSENT CHECKLIST:

There are many situations in which consent will be wholly inappropriate to use as a lawful basis for processing personal data. However, due to the frequency with which consent is misunderstood in the context of the GDPR, the below checklist should help identify areas of your business practices and procedures which may need to be addressed insofar as it is appropriate to use consent as the lawful basis for processing personal data.

ASKING FOR CONSENT

- ✓ Check that a consent request is the most appropriate lawful basis for processing the data.
- ✓ Ensure the request for consent is prominent and separate from any terms and conditions.
- ✓ People have been positively asked to opt-in.
- ✓ Pre-ticked boxes or any other type of default consent have been removed.
- ✓ Clear and plain language has been used when asking for consent.
- ✓ You have clearly explained what the data is and what you are going to do with it.
- ✓ Various options have been given regarding consent for different purposes and processing.
- ✓ You have identified anyone relying on the consent (including any third-party controllers).
- ✓ Individuals have been informed that they can withdraw their consent.
- ✓ Any non-consenting individual must not suffer any detriment.
- ✓ Ensure that consent is not a precondition of a service.
- ✓ Where any online services are offered directly to children, consent is only being sought if age-verification measures (and parental-consent measures for younger children) are in place.

RECORDING CONSENT

- ✓ Records of when and how consent has been obtained from the individual are being kept along with a record of exactly what the individuals were told at the time.

MANAGING CONSENT

- ✓ Consents are regularly reviewed to check that the relationship, the processing and the purposes have not changed.
- ✓ Processes are in place to refresh consent at appropriate intervals, including any parental consents.
- ✓ Privacy dashboards or other preference-management tools are considered as a matter of good practice.
- ✓ It is easy for individuals to withdraw their consent at any time, and it is clear how to do so in your literature.
- ✓ Withdrawals of consent are acted on promptly.
- ✓ Individuals who wish to withdraw consent are not penalised.

EMPLOYEES AND HR

The GDPR applies to all personal data – not just that of clients and customers of your business. This means that employers not only need to consider how they handle the personal data of data subjects outside the business, but also need to review their internal policies and procedures which dictate the processing of the personal data of their employees.

The circumstances in which it will be possible and appropriate to rely upon consent as a lawful basis for processing the personal data of employees will be extremely limited. Consent must be freely given, and because of the imbalance of power inherent in the employee/employer relationship, it is highly questionable that an employee could be regarded as having a genuinely free choice with no adverse consequences. What happens if the employee declines to consent, or opts-out?

In the vast majority of cases it is arguable that the processing of an employee's personal data will be necessary in order to carry out their employment contract, however this must of course be balanced against exactly what data the employer holds.

As with the personal data you hold on data subjects outside your business, you need to identify precisely what data you hold, source the origins of this data, be able to explain how you use this data and know whether or not this data is transferred to third-parties. If employees' personal data is transferred to third-parties (for example, a payroll provider), you must ensure you have the appropriate contractual protection in place, especially if the personal data crosses international borders. Employees must be informed of how and on what basis their personal data is being processed and provided with a privacy policy which contains the requisite details. The same goes for the personal data of prospective employees during the course of a recruitment process – you must inform applicants that you are holding their personal data and provide them with a privacy policy detailing the basis on which you are able to justify the processing of their data. Processes should be in place for the review of employees' personal data; when the processing of any personal data no longer becomes justifiable under a legal basis, the data must be deleted immediately.

DATA SUBJECT ACCESS REQUESTS

Further to the principle of transparency under the GDPR, data subjects have the right to obtain from the data controller:

- Confirmation that their data is being processed;
- Access to their personal data; and
- Supplementary information.

This must be free of charge to the subject of the access request (unless manifestly unfounded, excessive or repetitive).

The data controller must comply with their obligations without undue delay, and at the latest within one month.

DATA BREACHES

It is dangerous to assume that the safeguards you have in place protecting your data are impenetrable. To equip your business for effective breach response, the first step is ensuring that your employees understand what constitutes a data breach and implementing a robust system for detecting breaches.

WHAT IS A DATA BREACH?

The definition of a breach is far wider than simply a loss of personal data:

'A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.'

EXAMPLES:

- Access by an unauthorised third-party.
- Sending personal data to an unintended recipient.
- Devices containing personal data being lost or stolen.
- Unauthorised alteration of personal data.

HOW TO PREPARE:

- Have a process in place for reporting and investigating personal data breaches in a time efficient manner. These should also determine the level of risk a data subject's personal data could be subject to.
- Construct a detailed plan regarding how you will respond to a data breach, involving the designation of key responsibilities.

WHAT YOU SHOULD DO IN THE EVENT OF A DATA BREACH:

- Under the GDPR, businesses are under an obligation to report personal data breaches within 72 hours of the breach coming to their attention, where feasible. The breach should be reported to the relevant supervisory authority. In the UK this is the Information Commissioner's Office (ICO), but if the affected data subject is elsewhere in the EU a different authority may have jurisdiction.
- The data subjects whose personal data is subject to the breach in question must also be informed without undue delay when there is a high risk that the breach will adversely affecting the individual's rights and freedoms.
- Make a record of any personal data breach.

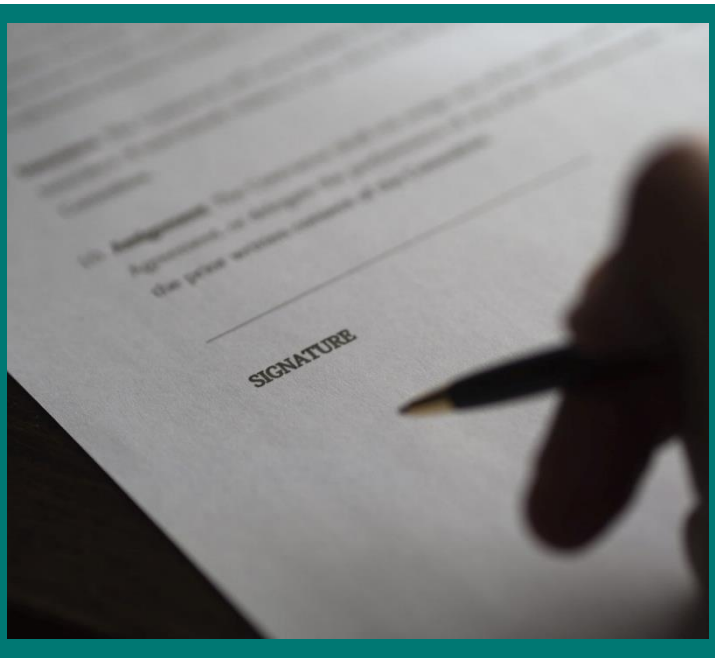
STEPS BUSINESSES SHOULD BE TAKING

- Ensure that you have sufficient staff and resources to discharge your obligations under the GDPR.
- Appoint a Data Protection Officer, if necessary, who is sufficiently qualified to advise your business on its obligations.
- The GDPR requires that data controllers implement appropriate technical and organisational measures. This means that you must be thinking about data protection when you are designing your business's various procedures and processes. SMEs can take some comfort in the fact that the term 'appropriate' permits a degree of flexibility. In other words, small businesses who hold less data on a smaller number of individuals will not be held to the same standards as a multinational corporation holding millions of people's personal data.
- Data protection impact assessments are a way for data controllers to proactively identify the likely risks involved in the processing of personal data using new technologies and to most effectively comply with their obligations under the GDPR.
- The fines imposed by the ICO are done so at their discretion and are punitive and fault based. Therefore, the greater lengths your business goes to in an effort to safeguard the personal data you hold (e.g. encrypting data), the less culpable you may be deemed in the event of a breach.
- Perhaps most importantly, record everything! If you do not, regardless of whether or not you have been complying with your core obligations, the fact that you are unable to demonstrate this will mean that you are in breach of the GDPR.

CONTRACTS:

If you are a data controller and you use a data processor, the GDPR states that you must have a written contract in place providing sufficient guarantees and which specifically determines:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.



WHERE TO LOOK FOR ADVICE

The complexity of the new regulations can leave SMEs with limited time and resources feeling overwhelmed by information and unsure how to prioritise their various obligations and implement them into their businesses.

Despite recent publicity and the fact that smaller businesses may risk insolvency if found liable for a fine, a recent survey concluded that 55% of SMEs are still not familiar with the GDPR.

At BakerLaw, we understand the various challenges that SMEs can be subject to. Our commercial team has a host of experience working with SMEs to help develop and grow their businesses.

If you would like to learn more about the GDPR and talk with one of BakerLaw's GDPR specialists about how we could assist your business, please do not hesitate to get in touch:

Danielle Collett-Bruce
Company & Commercial

Solicitor
danielle.collett-bruce@baker-law.co.uk
01252 931116

Emily Yeardley
Employment

Associate Solicitor
emily.yeardley@baker-law.co.uk
01252 730765

David Deakin
Commercial and Intellectual Property

Consultant Solicitor
david.deakin@baker-law.co.uk
01252 931272

BAKERLAW
SOLICITORS®

This guide is not a definitive statement of the law. It is designed as a free update on the law at the time of publishing. It is not a substitute for legal advice on specific facts and circumstances. BakerLaw LLP and/or the writer accepts no liability or responsibility for reliance on this guide and recommends that you seek independent legal advice on your specific circumstances prior to taking any steps.

FARNHAM OFFICE

Gostrey House
Union Road
Farnham
Surrey
GU9 7PT

LONDON OFFICE

Eldon Chambers
Falcon Court
30-32 Fleet Street
London
EC4Y 1AA