WE MEAN BUSINESS:

COUNTING DOWN TO THE GENERAL DATA PROTECTION REGULATION

BLAKE MORGAN

CONTENTS

Chairman's view	03
What is the GDPR?	04
What should you be doing now to prepare?	04
Key changes in the GDPR	05
Blake Morgan's data protection and information governance expertise	07
How we can help you prepare for the GDPR	08
A wealth of experience in helping mitigate risk and protecting your data	09
Meet the experts	10

"THE GDPR INCLUDES NEW CONCEPTS SUCH AS THE **'RIGHT TO BE FORGOTTEN'**, THE ACCOUNTABILITY PRINCIPLE AND THE DUTY TO REPORT SECURITY BREACHES, WHICH BUSINESSES NEED TO FULLY UNDERSTAND AND PREPARE THEMSELVES FOR. IT'S NOT JUST REPUTATION THAT IS AT STAKE FOR FAILURE TO COMPLY."

CHAIRMAN'S VIEW: LESS THAN SIX MONTHS TO GO – ARE YOU READY FOR THE GENERAL DATA PROTECTION REGULATION?

BLAKE MORGAN

From 25 May 2018, all organisations will need to comply with the General Data Protection Regulation (GDPR). Brexit will not affect this. The GDPR includes new concepts such as the 'right to be forgotten', the accountability principle and the duty to report security breaches, which businesses need to fully understand and prepare themselves for. It's not just reputation that is at stake for failure to comply – businesses will be liable for fines up to the greater of 4% of their annual worldwide turnover or €20 million for serious breaches of the GDPR (up from the current £500,000 limit). Yet fines will be a last resort. The Information Commissioner's Office (ICO) is the statutory regulator for data protection law and, in addition to fines, it has a range of sanctions to encourage organisations to comply, such as warnings, reprimands and corrective orders. Being compliant makes good business sense. Being transparent as to how data is used – and ensuring adequate security for the data – help to build trust with customers and internal stakeholders including your staff, for your employment practices and policies will also be impacted by the GDPR. It also enhances the value of your business.

When we surveyed our clients in the Summer of 2017 on their GDPR compliance we found that almost 40 per cent of organisations had not taken steps to prepare for the GDPR, while more than a third were not confident they would be able to comply with the GDPR by the 25 May 2018 deadline. The ICO has made it clear that there is no 'grace period' after this deadline. Organisations that bury their heads in the sand and infringe the GDPR can expect tough treatment, while those that do their best to comply and engage with the ICO if problems arise are more likely to receive a sympathetic hearing from the ICO.

This guide to the General Data Protection Regulation was first published in May last year and seeks to summarise the key changes that the new law will bring, and to highlight the most important actions that your business should take in preparing to comply with it. Many clients and contacts of the firm have found it helpful. We have taken the opportunity to update it, so it remains current as we move into 2018.

If you have any questions on the GDPR our data protection and regulatory experts are available to answer your questions at GDPR@blakemorgan.co.uk

Bruce Potter, Chairman

WHAT IS THE GDPR?

The GDPR is a single new data protection law for the whole of the EU. It's the biggest reform of data protection law for decades and represents a significant strengthening of, and upgrade to, the current data protection rules.

Even if you feel confident dealing with the existing Data Protection Act, the GDPR will bring big changes and make good data protection compliance even more important. The GDPR retains the basic tenets of existing data protection law. For instance, personal data must only be processed in line with a set of principles, and in accordance with specific conditions (the principles and conditions are similar, but not quite identical, to the existing law). There are obligations on controllers to provide fair processing information to individuals and to comply with subject access requests.

There will also be plenty of changes. There will be tighter rules for processing personal information, enhanced rights for individuals and direct obligations on data processors (those who process personal data on behalf of the data controller, for example, outsourcing providers). Crucially, the consequences of getting it wrong will be much more severe, with fines of up to €20 million or 4% of worldwide turnover for very serious breaches, as well as compensation claims from individuals.

Two areas of unfinished business at the time of writing are the UK's Data Protection Bill and the EU's ePrivacy Regulation. The Bill, which is currently passing through Parliament, will repeal and replace the existing Data Protection Act 1998. It aims to deal with those areas of data protection law that are not covered in the GDPR. Once passed, the Bill and the GDPR will together form the data protection law that organisations in the UK will need to comply with.

The ePrivacy Regulation complements the GDPR and, among other things, deals with the use of cookies and electronic direct marketing including by email. Until we know more about the final shape and implementation date of this Regulation, our best advice to clients is to continue to comply with the UK's Privacy and Electronic Communications Regulations 2003 (as amended) when using cookies and engaging in direct marketing. We expect prior consent (i.e. express opt-in) to remain a condition for e-mail marketing except where limited 'soft opt-in' consent for existing customers applies. In any event, the core of the new legal framework is the GDPR, and that is what this guide focuses on.

WHAT SHOULD YOU BE DOING NOW TO PREPARE?

May 2018 is fast approaching, so organisations that haven't already done so should start preparing for the changes. And those that are already in the midst of their compliance project should be checking to see how their action plans are progressing and whether all key issues are being addressed.

We always advise clients that the place to start in achieving GDPR compliance is to ensure key stakeholders and decision-makers are aware of the issues and are committed to compliance, that budget and resources are appropriately allocated, and that an initial audit or information gathering exercise is carried out – so you can document what personal data you hold, where it came from (and how it was obtained e.g. were privacy notices or similar used), how you use the data and who you share this data with. Having done this, you are then in the best possible place to take the necessary actions in order to achieve compliance.

Bear in mind too that GDPR compliance is an evolutionary process – no organisation ever stands still. As ICO has recently stated: "you will be expected to continue to address emerging privacy and security risks in the weeks, months and years beyond May 2018."

We have summarised in the table on the next page some of the key changes under the GDPR, together with actions you can take now to help ensure that your organisation is ready.

KEY CHANGES IN THE GDPR:	ACTIONS TO TAKE NOW:
BEING MORE TRANSPARENT WITH INDIVIDUALS The GDPR requires controllers to give individuals more information at the time their data is collected – this includes explaining the legal basis of your processing, your data retention periods, and that individuals have a right to complain to ICO. There are also additional obligations whenever you seek consent from an individual to the processing of their data. Bear in mind that your employees, other workers and consultants also benefit from the enhanced transparency required by the GDPR.	Review your customer-facing terms and your privacy policies. These are likely to need substantial revisions to meet the new requirements. If you are relying on customer consent to legitimise your processing, check that the method of obtaining consent will meet the new rules – note that under the new rules the data subject can withdraw their consent at any time and consent requires a positive opt-in – you cannot infer consent from silence, pre-ticked boxes or inactivity. As an example, property investors and social landlords might not think that the GDPR affects their business but they will need to identify what data they collect from their individual tenants and analyse what they do with that data as part of their everyday property management activities to determine what their transparency obligations are, the legal basis of their processing and whether consent is required. The GDPR's obligations apply to all businesses and organisations that process personal data – large or small. If you cannot rely on consent, can you rely on an alternative condition for processing? Also don't forget your employees and other workers – you won't be able to rely on employee consent so you will need to determine on what other legal basis you will process your employee data going forward. Employees will require privacy notices and there are likely to be changes needed to your employment contracts and policies in order for you to comply with the GDPR. The processing of sensitive personal data (what the GDPR calls 'special categories of data') and criminal records are also subject to additional regulation and conditions under the Data Protection Bill – for example, an employer is likely to need to have an appropriate policy document in place if they process such personal data.
DEMONSTRATING YOUR COMPLIANCE An overarching theme of the GDPR is the principle of 'accountability'. There are new requirements on controllers (and processors) to demonstrate their compliance by fully documenting all their data processing activities. Organisations may be required to carry out data protection impact assessments and implement privacy-by-design and privacy-by-default techniques.	Consider what records you keep of your decision making and your processing activities. Can you demonstrate your compliance? Review your contracts with processors to ensure that they have robust provisions around record-keeping. If you don't already use them, think about introducing data protection impact assessments for new projects – these are a requirement of the GDPR where the proposed processing is high risk. Note also that whilst the GDPR does not require you to notify your processing to the ICO (as is currently the case) you will still need to pay the ICO an annual data protection fee – these fees are likely to range from £55 to £1000 or so depending on the size and nature of the processing of the organisations concerned.
MANDATORY BREACH NOTIFICATION Controllers will have no more than 72 hours to report any data protection breach unless the breach is unlikely to put individuals at risk and, where the breach is likely to result in a high risk to individuals, they must also notify individual data subjects without undue delay.	Review your internal systems to ensure that you can meet the new breach notification requirements. Review your processor contracts to ensure they contain obligations to report breaches to you. Bear in mind too the best place to be regarding security breaches is to avoid them – this means taking your IT security procedures very seriously, investing in and using secure systems including passwords and encryption, firewalls, and current anti-virus software, but also addressing the human element through training and procedures designed to minimise the risks of hacking, phishing and other cyber security breaches.
APPOINTING A DATA PROTECTION OFFICER Companies that process large volumes of data as part of their core activities (whether as a processor or controller) will in certain cases be required to appoint a 'Data Protection Officer', as will public bodies. This will be a statutory role (with appropriate employment protections), reporting directly into senior management, with specific functions set out in the GDPR.	Decide whether you need to appoint a Data Protection Officer (DPO) – 'public authorities' must appoint one (it is currently anticipated that if the public authority is subject to the Freedom of Information Act 2000 then they will also need to appoint a DPO). If you do, think about who is best placed within your organisation to take on the role. Alternatively, explore whether you could outsource the DPO role under a service contract.

KEY CHANGES IN THE GDPR:	ACTIONS TO TAKE NOW:
MUCH HIGHER PENALTIES WHEN THINGS GO WRONG Companies will face much stiffer penalties for non-compliance. Under the GDPR the regulator will be able to issue administrative fines of up to the higher of €20 million or 4% of worldwide turnover, a very significant increase on the current monetary penalties (which are limited to £500,000).	Ensure that the risks of penalties for non-compliance with the GDPR are fully understood at senior management / board level. Consider what measures you can take to reduce these risks. Review your processor contracts to ensure that liability is adequately flowed down.
DIRECT OBLIGATIONS ON PROCESSORS Under existing data protection law, the controller is solely responsible to data subjects and the ICO for compliance, and the processor is only liable under contract to the controller. By contrast, the GDPR imposes direct obligations on processors, such as to take appropriate security measures to protect personal data, and maintain certain records of all processing activities. Processors won't be able to subcontract their processing without the controller's prior consent. The ICO will be able to impose administrative fines on a processor in the event of a breach of these processor obligations under the GDPR. Individuals (data subjects) will also be entitled to receive compensation from processors where the processor acts in breach of its obligations under the GDPR or where it has acted outside or contrary to lawful instructions of the controller.	Map out all your arrangements with data processors, such as outsourced services and cloud suppliers. The direct obligations on processors will affect all of your service providers who process personal data, so you may find they want to renegotiate terms to reflect the increased risks. Consider whether your organisation is acting as a processor on behalf of anyone else. If so, you will need to comply with the direct obligations under the GDPR. This could have significant implications for groups of companies which provide services to each other.
ENHANCED RIGHTS FOR INDIVIDUALS The GDPR includes a suite of rights for individual data subjects. In addition to subject access rights, which are retained from the current law, but with some important changes, individuals will have the right to receive their data in a commonly used and machine-readable format (the right to data portability) and the right to have their data erased (the right to erasure – also called the 'right to be forgotten'), with certain exceptions, for example, where an employer or landlord needs to retain the data and has lawful grounds for doing so.	Review your process for responding to subject access requests and make any changes necessary to comply with the new rights for individuals. Communications with individuals will need to be changed to ensure they are aware of the new rights.
NEW(-ISH) RULES ON DATA TRANSFERS The current law restricts transfers of personal data outside the European Economic Area. This has become a major talking point since the demise of 'Safe Harbor', the introduction of the EU-US Privacy Shield and the implications of Brexit. The GDPR repeats much of the existing law in this area and in some circumstances narrows the scope for organisations to legitimise transfers of personal information outside of Europe.	Take stock of your data export activities. Whilst the GDPR does not offer any easy solutions, it is important to understand your level of risk and ensure that each of your export arrangements has a legitimate basis.
FOREIGN REGULATORS Where organisations offer services in more than one EU member state, they will be subject to regulatory enforcement from data protection supervisory authorities in other jurisdictions where customers are located. Organisations will be subject to a 'lead' authority and there will be a mechanism to ensure that decisions are made consistently across jurisdictions.	The lead supervisory authority will be the regulator in the country where you have your 'main establishment'. Consider where this is and identify the lead authority. Keep a close eye out for guidance issued by your lead authority (which will be the ICO for organisations with their main establishment in the UK).
CHILDREN For the first time there will be specific data protection rules applying to children, with an age of consent for the processing of children's personal data in relation to 'information society services', which broadly means services offered over the internet. The Data Protection Bill currently before Parliament sets this age of consent at 13.	If you offer information society services to children (which we expect to be defined for data protection purposes as those under 13) then you may need a parent or guardian's consent to process their personal data lawfully. Consent must be verifiable and privacy notices must be written in language that children will understand.

BLAKE MORGAN'S DATA PROTECTION AND INFORMATION GOVERNANCE EXPERTISE

We provide pragmatic advice on data protection and information governance law for organisations across the private and public sectors. As well as GDPR compliance, we help clients understand their existing obligations, implement appropriate systems for compliance and manage specific challenges as they arise from time to time.

We provide well informed, practical advice in connection with information requests made under data protection law, handling investigations by the ICO and managing potential data security breaches.

As well as providing legal advice on data protection and information governance issues, our expert lawyers provide guidance on:

- GDPR-compliant employment contracts and policies
- GDPR-compliant leases and management documents relating to commercial and residential properties
- Privacy notices, data protection policies and breach notification procedures
- Confidentiality and non-disclosure agreements
- Cross-border data flows and the cloud
- Data protection audits and advice on information security and governance (including data retention, privacy impact assessments and privacy by design)
- Data sharing and data processing agreements
- Litigation disclosure rules
- Marketing and privacy (including guidance on electronic marketing consent requirements and the use of cookies and apps)
- Public procurement rights of access
- Re-use of Public Sector Information Regulations
- Sale and use of databases
- Social media and confidentiality, including employment and related aspects such as bring your own device (BYOD)
- Data breaches and cyber security

HOW WE CAN HELP YOU PREPARE FOR THE GDPR

Blake Morgan's expert lawyers can assist you every step of the way in getting ready for the GDPR.

We would be very happy to support you by:

- Discussing how the GDPR may affect your business
- Advising you on the steps to take to gear up for the GDPR
- Carrying out data protection audits in your organisation
- Drawing up a comprehensive plan for your GDPR compliance project
- Reviewing and amending your existing customer-facing contracts, privacy policies and fair processing notices
- Advising on customer consent wording
- Reviewing your existing employment contracts and policies and revising them to meet the requirements of the GDPR and the Data Protection Bill
- Drafting data protection policies and procedures
- Reviewing existing contracts and drafting data protection clauses for new contracts
- Supporting your Data Protection Officer

We can also provide a range of bespoke data protection training courses to suit your needs.

Blake Morgan is the only law firm accredited to provide the BCS Certificate in Data Protection course, which is an intensive five-day course leading to a professional qualification (on successful completion of an externally marked exam). This qualification is ideal for anyone with data protection responsibilities, particularly those taking on the Data Protection Officer role under the GDPR.

A WEALTH OF EXPERIENCE IN HELPING MITIGATE RISK AND PROTECTING YOUR DATA

We have helped our clients:

- Advising a large building society operating in a regulated sector on a major business transformation project designed to work towards GDPR compliance, including reviewing significant supplier contracts
- Advising an international media producer and distributor on its GDPR compliance project, supporting its data audit and, reviewing and updating its policies and procedures
- Conducting a GDPR audit for a leading retail payment and loyalty technology provider
- Advising a number of agencies in the recruitment sector on reviewing policies in line with GDPR requirements and identifying issues associated with launching new software and data collection practices
- Drafting and implementing new GDPR-compliant employment contracts, handbooks, privacy notices, policies and procedures
- Advising a UK/US charity on an ICO investigation plus preparing updated GDPR compliant privacy policies and data collection statements
- Providing bespoke training to a major religious and charitable organisation and providing ongoing advice on their GDPR compliance project
- Conducting a GDPR audit for an academy trust company
- Acting for the claimant in high court proceedings arising from a contested subject access request
- Advising on cross border data processing arrangements and related trans-border data privacy issues between the UK and US for an international bank
- Working with a leading insurance claims management provider to put in place compliant and practical data sharing and processing arrangements
- Guiding a leading fitness club through a self-reporting process to the ICO and related communication with members following a potential data breach
- Drafting data sharing agreements for use between a utility company and individual local authorities and advising on the processes to be put in place when individual requests for data are made
- Advising an international hotel chain in connection with international data sharing and consent requirements when engaging in e-marketing

MEET THE EXPERTS
YOUR KEY BLAKE MORGAN CONTACTS

Email your questions to GDPR@blakemorgan.co.uk

SHEILAH MACKIE
PARTNER

☎ 023 8085 7039
✉ sheilah.mackie@blakemorgan.co.uk

Sheilah has a wealth of experience in data protection and privacy law advising clients on compliance with relevant UK and EU legislation in their processing of customer, employee and third party data and their use of cookies and similar technology in relation to both day-to-day transactions and large-scale corporate and outsourcing deals.

SIMON STOKES
PARTNER

☎ 020 7814 5482
✉ simon.stokes@blakemorgan.co.uk

Simon is experienced in data protection including compliance, trans-border data flows, privacy policies, cookie laws, cloud services, international issues, e-commerce law, software and patent/technology licensing. His experience includes advising clients in the financial services sector on trans-border privacy issues including relating to the cloud and advising clients on processing data for marketing purposes. He also advises on the IP protection and licensing of data and databases.

JOHN MITCHELL
PARTNER

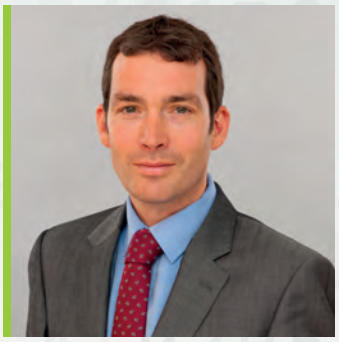
☎ 023 8085 7231
✉ john.mitchell@blakemorgan.co.uk

John focuses on contentious matters. In particular, he assists businesses that have breached the Data Protection Act and advises on compliance with subject access requests, an area where his experience with IT based document management and litigation support systems is invaluable.

ELISABETH BELL
LEGAL DIRECTOR

☎ 0118 955 3045
✉ elisabeth.bell@blakemorgan.co.uk

Elisabeth has substantial experience advising on implementing data protection compliance terms, conditions and procedures on major IT and commercial outsourcing and projects. She advises on data sharing between processors and controllers, particularly in the health sphere. She has particularly been working with SMEs helping them to implement GDPR compliance programmes.



JON BELCHER
ASSOCIATE

029 2068 6268
jon.belcher@blakemorgan.co.uk

Jon specialises in data protection and information governance issues. He advises clients on data protection issues in relation to the exploitation, sharing and security of personal data. Jon has significant experience in advising on data sharing arrangements and the data protection implications of commercial transactions including data export and direct marketing campaigns. He also provides regular training on data protection matters and is a tutor on Blake Morgan's BCS Certificate in Data Protection course.

MERERID MCDAID
ASSOCIATE

029 2068 6145
mererid.mcdaid@blakemorgan.co.uk

Mererid is a member of the commercial team and advises clients from the public and private sector on commercial and information governance issues. Mererid is currently providing assistance to a number of clients on their requirements to comply with GDPR . She has provided extensive training to clients from the private, education, health, housing, charity and local authority sector on the GDPR requirements, such training being delivered to a diverse range of audiences from board and senior management level to general staff training. Mererid is also assisting clients on their GDPR compliance projects. Such advice includes assisting with data audits and data flows, reviewing and updating policies and procedures and advising on data processing arrangements.

HOLLY CUDBILL
ASSOCIATE

023 8085 7472
holly.cudbill@blakemorgan.co.uk

Holly advises employers and HR professionals on data protection issues concerning job applicants, current and former employees, workers, consultants and apprentices. Holly's experience includes defending employment tribunal claims with data protection issues, drafting data protection compliant contracts, handbooks and polices and carrying out in-house training. Holly has previously held the role of Data Protection Officer and is currently assisting clients with GDPR compliance including HR data audits and staff privacy notices.

RAJIV JOSHI
PARTNER

0118 955 3035
rajiv.joshi@blakemorgan.co.uk

Rajiv is a partner in the employment team whose work includes advising on unfair dismissal, discrimination, jurisdictional matters and the employment aspects of corporate transactions. Rajiv regularly advises employers on strategic matters and often will deal with complex senior level exits and settlement arrangements. He also drafts and advises on directors' service agreements, employment contracts, staff handbooks and settlement agreements. He is currently supporting business owners and HR teams on ensuring that employee data handling is GDPR compliant and has delivered training to employer organisations in this area.

WILLIAM DOWNING
PARTNER

01865 254265
william.downing@blakemorgan.co.uk

William is head of the Employment law team in the Thames Valley. He provides immediate and commercially sensitive advice concerning all compliance issues. In particular William guides clients through complex situations, providing draft letters, aide memoirs and key pointers for handling difficult exits and assisting in dealing with internal client investigations and processes. He also has a wide range of experience advising on business protection for businesses in the Thames Valley. His data protection interests lie in ensuring that employer's policies and written documentation is compliant and handling of employee and other data in commercially sensitive situations abides by the new regulations.

CARDIFF
029 2068 6000
029 2068 6380

LONDON
020 7405 2000
0844 620 3402

OXFORD
01865 248607
0844 620 3403

PORTSMOUTH
023 9222 1122
0844 620 3404

READING
0118 955 3000
0118 939 3210

SOUTHAMPTON
023 8090 8090
0844 620 3401

info@blakemorgan.co.uk
www.blakemorgan.co.uk

BLAKE MORGAN