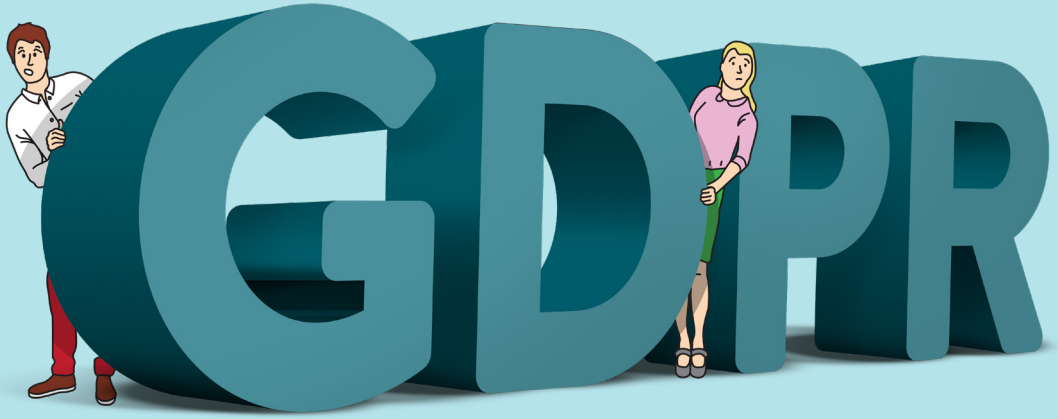


Where are you on the journey?

A PASSION FOR PEOPLE

harrison clark rickerbys
SOLICITORS

A PASSION FOR PEOPLE

Our passion for people is at the heart of everything we do. It's the engine that keeps us ticking and inspires us to do our best. We're not satisfied unless we're making a real difference to people's lives, and we'll keep working hard to ensure we get the best outcome possible for our clients.

The General Data Protection Regulation (GDPR), which came into force in May 2018 affects everyone and all organisations. Rarely has a change in legislation had such a wide reaching impact. Our specialists can provide you with sector specific information that will help you to navigate and to maximise the opportunities and minimise the challenges that the regulations will bring. In the meantime, we hope that the information within this brochure is useful to you.


Robert Capper
Head of Commercial team
and sectors

GDPR - Key terms

Expanded Territorial Reach

The location of the data subject and not the organisation will determine whether or not the GDPR applies to organisations that do not have an establishment within the EU.

Action point: This means that many non-EU organisations will be required to comply with the GDPR even if they were not previously required to comply with the Data Protection Directive.

Consent

Consent must be freely given, specific, informed and unambiguous. It must be a clear indication of the data subject's agreement to the processing of their personal data. Consent has to be given on an opt-in basis and the data subject must have the right to withdraw their consent at any time.

Action point: Existing practices for obtaining consent will need to be reviewed and amended to meet GDPR standards. Consider refreshing existing consents where they do not meet these standards.

Rights of Data Subjects

The rights of data subjects under the GDPR are enhanced and, as a result, organisations should carefully ensure that these rights are appropriately addressed.

Data subjects will have the right to be forgotten, data portability rights, the right to have inaccuracies corrected and the right not to be subject to automated decision-making, including profiling.

There are also new rules in relation to subject access requests, including changes to the response time which will be just one month.

Accountability

The GDPR adopts a risk-based approach and requires data controllers to implement appropriate measures to ensure and demonstrate compliance with the GDPR.

Action point: Data Protection Impact Assessments are required to be carried out prior to the use of new technologies that are likely to result in a high risk to data subjects. Any measures identified must be monitored and updated.

Privacy Notices

The GDPR increases the amount of information organisations need to include in privacy notices, such as notification of the expanded rights of data subjects.

Action point: Organisations should therefore review existing privacy notices and ensure that any necessary changes are implemented prior to the GDPR coming into force. These notices and any communications to data subjects must be clear, concise and intelligible.

Data Protection Officers

A senior member of your organisation should take overall responsibility for GDPR compliance. Organisations should also consider whether they are obliged to appoint a Data Protection Officer who has the knowledge and authority to monitor compliance effectively.

Action point: As the changes under the GDPR are comprehensive and far-reaching, all members of your organisation should be trained on the GDPR requirements.

Data Security

Organisations must ensure that personal data is kept secure at all times. In some cases, enhanced measures such as encryption will be necessary.

The GDPR requires mandatory reporting of security breaches to the regulator and in serious cases to the data subject.

Action point: Organisations should put in place processes to deal with breaches in accordance with the GDPR.

Processors

The GDPR imposes duties directly on data processors in addition to data controllers. The GDPR will impose sanctions for breach on both data processors and data controllers.

Action point: Data controllers should identify contracts with data processors and ensure they reflect the GDPR. Data processors should review existing arrangements to ensure these meet their updated compliance requirements.

Transfer out of EU

The GDPR allows the transfer of data outside of the EU only when certain safeguarding criteria are met. A broader range of mechanisms to transfer personal data out of the EU has also been introduced, including approved codes of conduct and certification processes.

Action point: Organisations should review their procedures to check whether they are adequate under the GDPR and consider whether new documentation is required, such as binding corporate rules.

Sanctions

The GDPR will significantly increase the maximum fines for non-compliance and regulators will be able to impose fines on data controllers and data processors. The maximum level of fine is €20 million or 4% of total worldwide annual turnover (whichever is greater).

Action point: In addition to financial sanctions, there will also be significant reputational damage to organisations if they fail to adequately comply with the GDPR.

8 Steps to

1 Consent

How are you seeking, obtaining and recording consent?

You must be able to demonstrate that consent has been freely given and is specific, informed and unambiguous. It must be given on an 'opt-in' basis. You may need to update existing consents now if they do not comply. Special rules will apply to obtaining consent for processing children's personal data.

2 Communication

Are your privacy notices GDPR compliant?

In addition to the current information you are required to give when you collect personal data, you will need to set out your legal basis for data processing and your data retention periods, as well as advise individuals that in addition to other rights, they have a right to complain to the ICO. This information must be communicated clearly and concisely.

3 Holding and Processing Data

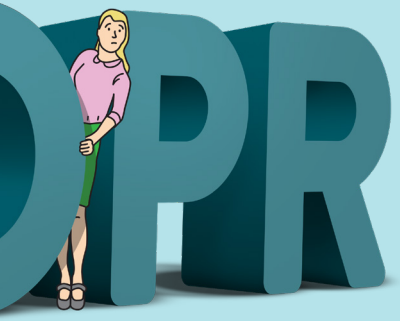
What information do you hold and what is your legal basis for processing it?

Under the GDPR you are required to maintain records of your processing activities. You may need to carry out an information audit to ascertain what information you hold, where it came from, what you do with it and who you share it with.

4 Rights of Individuals

Do your procedures comply with individuals' new rights under the GDPR?

Individuals will have greater rights in relation to their data under the GDPR, including rights of access and data portability, to have inaccuracies corrected, to have information erased, to prevent direct marketing and to prevent automated decision-making and profiling.



Compliance

5 Subject Access Requests (SARs)

How will you comply with the new rules on SARs?

You will now have just a month to comply with a subject access request and will only be able to refuse or charge for requests if they are manifestly unfounded or excessive. Consider what systems you may need to implement to meet the challenge of having to deal with requests more quickly.

6 Data Protection Impact Assessments (DPIAs)

Do you have a strategy for dealing with the new DPIA requirements?

DPIAs will become mandatory in some cases, e.g. where new technology is deployed, where profiling is likely to significantly affect individuals or where processing is large-scale and involves special categories of data. Where a DPIA identifies high-risk processing, you will need to consult the ICO. Take steps now to identify how DPIAs will be carried out and by whom.

7 Data Breaches

Do you know what to do if you detect a data breach?

Make sure you have procedures in place to detect, report and investigate a personal data breach. The GDPR will require you to notify the ICO of certain types of data breach and, in serious cases, the individual affected.

8 International

Do you carry out cross-border data processing within the EU?

If so, map out where your organisation makes its most significant decisions about data processing to determine who your lead data protection supervisory authority is and document it.

Your journey beyond  compliance

Where are you on your journey?

Our quick guide will help you to identify where you and your business are in the journey and what you need to do now to ensure that you are compliant.

1 Lack of knowledge

You have little or no knowledge of what GDPR is, you may not even know what the acronym means, let alone what it means for your business or the potential reputational risk to your business if you get this wrong.

To help companies understand the implications of GDPR and what they need to do, we have created an extensive range of articles, practical guides and other materials available via our website which are designed to give a user-friendly and accessible introduction to the new data protection regime coming into force in May 2018.

2 Awareness of issue

Through reading some articles or watching video content, you are developing an awareness of the scope and potential impact of GDPR and now need to deepen your understanding.

We have developed a programme of interactive seminars and workshops tailored to your needs that will provide you with an action plan to take back to your organisation – take a look at our current events listing at **www.hcrlaw.com/events**. We also work with organisations to deliver bespoke briefings for their employees.

3 How does this affect me?

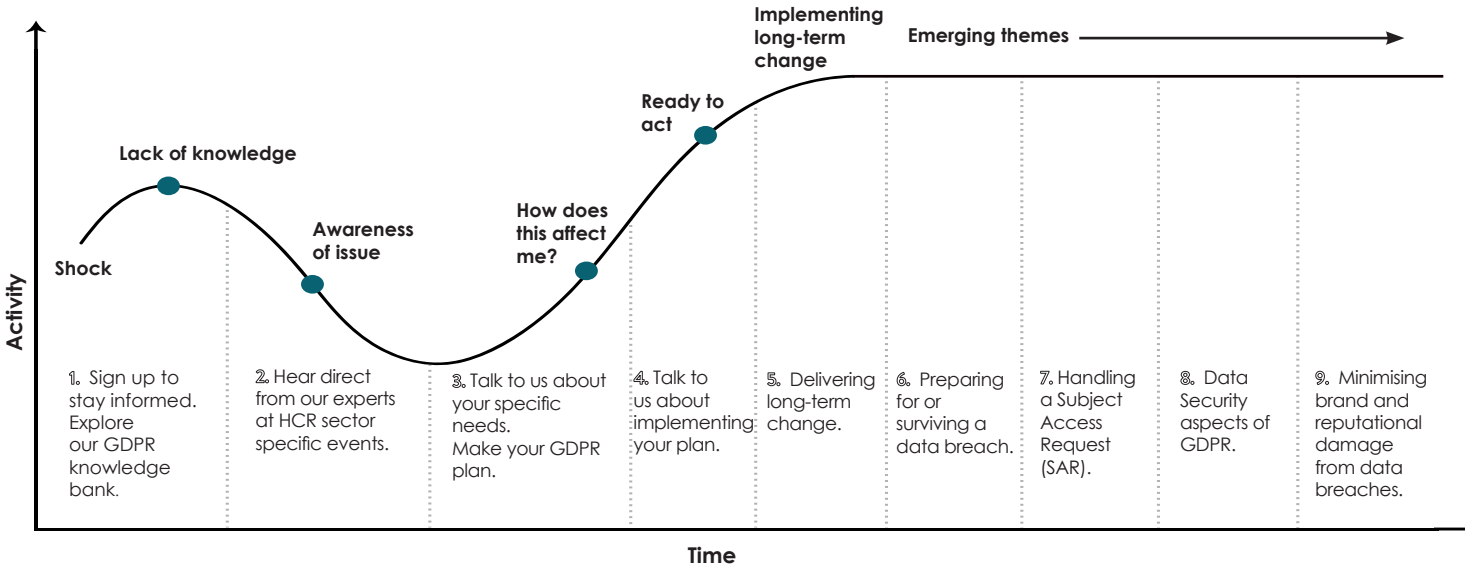
You now need to move from your general understanding of GDPR to more tailored guidance on what your sector and your business needs to do in order to comply.

At Harrison Clark Rickerbys we have established sector teams who understand the commercial context in which you operate and can help design your road map to compliance. This will typically start with 1-2-1 meetings with key stakeholders, following which we can work together to devise an action plan.

4 Ready to act

Having made the decision that you need to do something, we can provide you with expert advice to inform your decision.

We can support you in designing, scoping and carrying out data audits and guide you in mapping how data flows within your business. Our experienced lawyers can help you update your existing documentation (data protection policies, terms and conditions, privacy notices and data processing agreements) to ensure you are compliant.



5 Implementing long-term change

By now, you know you will need to continue to integrate changes to your business processes and want expert help doing this. This will mean training existing and new staff and monitoring your processes and policies to ensure they continue to be compliant. We can help you develop training resources, update your policies, notices and other data protection materials as well as carry out periodic compliance monitoring to make sure you continue to meet your obligations.

6 Managing a data breach

You recognise that a data breach can have a serious impact on your business and brand value, as well as compromise your employees, suppliers and customers. You are ready to face up to the reality and avoid becoming the subject of an unwanted headline.

7 Handling a Subject Access Request (SAR)

You may have already heard others talking about the amount of time subject access requests (SAR) take to process, or have had to deal with one first hand. Either way you are ready to find out how to minimise the impact on your organisation of a SAR by taking expert legal advice.

8 Data Security aspects of GDPR

You understand the connection between GDPR and data security and that often, no matter what systems you have in place it is human nature to take short cuts and unintentionally raise your exposure. You are ready to take expert advice on how to minimse the risk to you and your organisation.

9 Minimising brand and reputational damage from data breaches

Planning for the worst is an unpleasant business but necessary, especially when your customers' trust in your brand can disappear overnight. The middle of a crisis is not the time to learn lessons, you recognise that failing to prepare is preparing to fail.

What does it mean for your employee data?

On 25 May 2018 the General Data Protection Regulation (GDPR) came into force and applies to any entity that handles personal data on EU citizens, including employee data. As the UK will soon introduce a new Data Protection Act which echoes the GDPR, Brexit will not mean your organisation should ignore the GDPR. Given the breadth of personal employee data which HR departments handle, it is imperative to get it right.

Rather than view GDPR as yet another legislative hoop to jump through, HR departments should use it as an opportunity to revisit existing data policies and procedures to check that they are fit for purpose.

Know your data

The starting point for GDPR compliance is knowing what data your organisation holds. Undertaking a data audit and mapping data flows across your organisation will not only help to increase awareness of where and how employee details are held, it could identify a more effective way of processing it. Remember to include contractors and agency staff - for example, you may need to consider how you receive and store CVs.

Do you know what data you currently retain and for how long?

The HR team should consider carefully how long it needs to retain any data - for example, are historic HR records for former employees needed for legal reasons? If data is no longer needed, it must be securely destroyed. Employers who have a high volume of seasonal employees, who they contact when needed, may need to consider how they retain this data.

Don't just rely on consent as the legal basis for processing employee data

Under GDPR, while consent is still a legal basis for processing data, the thrust of the new regime is that consent should not necessarily be the first option. Within an employment law context, it would be more appropriate to rely on other lawful purposes for processing, such as it being necessary for the performance of the employment contract, or necessary for the purposes of the organisation's legitimate interests - these do not override the freedoms of the data subject. For example, the employee's rights would not be overridden by payroll being processed by a third party.

Update your privacy notice

To ensure GDPR compliance, an organisation should have a clearly worded data protection and privacy notice. This enables people to understand the personal data (information) held about employees, workers and job applicants as well as:

- How data will be collected and stored
- How the organisation will use the data and if information is to be shared during employment and after the employment ends
- How long the information will be held for
- The rights of data subjects (see below)
- Details of the right to complain to the regulator (the ICO).

Understand data subject rights

An employee (or data subject) has nine rights under the GDPR, including the right to access the data held by the organisation and to ascertain who this information is shared with. HR departments should prepare for being able to respond to such requests without undue delay, and within the new 30 day period, although this period maybe be extended for a further two months where providing a response is particularly complex.

Ensuring data is kept up to date in the case of a subject access request will be critical, particularly for those employers who outsource some services or enable employees to update personal data remotely.

The new regulations also give employees the right to have incorrect or irrelevant data deleted and errors corrected. When they leave they can request to be 'forgotten' officially, although there may still be data which the former employer is permitted to retain (for example, to defend any legal proceedings).

Do you share employees' data with a third party?

Many smaller organisations outsource payroll and most will share employee data with a pensions or other benefit provider. Do you know how they are handling your employees' data – is it transferred securely? Under GDPR it would be prudent to review the contracts that you have in place and ensure that your employees also know how and why you share their data with the third party. Such contracts should be carefully reviewed, as third party data processors may seek to impose unreasonable conditions on the employer or limit their own liability.

OUR GDPR SURVIVAL PACKS

Small business GDPR survival pack

What's in the box?

1. Privacy Policy
2. Data Processing Agreement
3. Third Party Contract Variation Agreement
4. GDPR guidance on collecting data

£250 **+ VAT**
one off purchase

Credit against fees for further GDPR advice

Ring the GDPR helpline if:

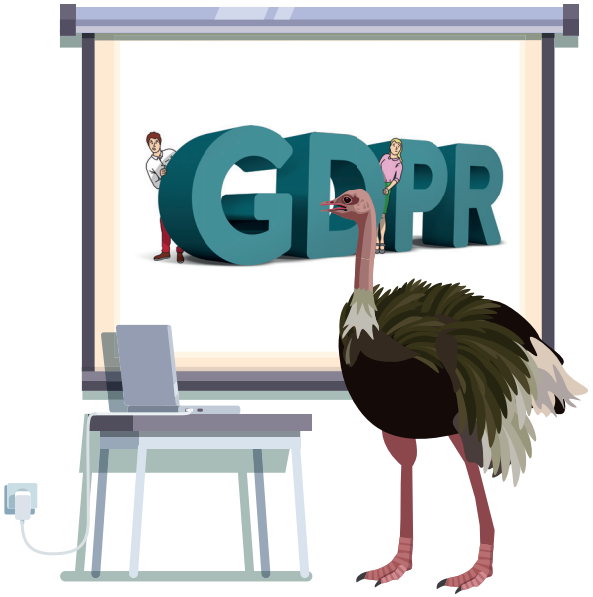
1. You have a question about GDPR in your business
2. Someone has asked to be deleted or requested a copy of the data you hold about them
3. Your business or one of your suppliers has had a data breach

GDPR Helpline

0800 910 1189

Our GDPR training offer:

1. Is for all staff and teams in your business
2. Includes briefing, workshop and webinar formats
3. Supports specific needs via 1-2-1 & bespoke group courses



The team

Robert Capper
Partner, Head of Commercial team and Sectors
T: +44(0)1905 744 814
M: +44(0) 7909 970 323
E: rcapper@hcrlaw.com

Adam Finch
Partner
T: +44(0)1242 211 635
M: +44(0)7772 481 550
E: afinch@hcrlaw.com

Rajeshree Bonjarvi
Partner
T: +44(0)118 945 0164
M: +44(0)7860 924 363
E: rbhojnani@hcrlaw.com

Stephen Thomas
Partner
T: +44(0) 1242 246 489
M: +44(0) 7765 238 895
E: sjthomas@hcrlaw.com

Guy Hollebon
Senior Associate
T: +44(0)1242 246 494
M: +44(0)7921 498 467
E: ghollebon@hcrlaw.com

Rachael king
Senior Associate
T: +44(0)1905 746 466
M: +44(0)7715 060 345
E: rking@hcrlaw.com

Steve Murray
Senior Associate
T: +44(0)1242 246 494
M: +44(0)7921 498 467
E: smurray@hcrlaw.com

David Ashcroft
Senior Legal Counsel
T: +44(0)1432 349 670
M: +44(0)7926 090 484
E: dashcroft@hcrlaw.com

This document is not intended to be an exhaustive statement of the law and gives general information only on the key principles of the GDPR. It is not a substitute for legal advice and we do not accept liability to anyone who does rely on its contents.

For further advice and assistance relating to compliance with the GDPR contact:

Robert Capper,
Partner, Head of Commercial team and Sectors

+44 1905 744 814 | rcapper@hcrlaw.com

harrison clark rickerbys

SOLICITORS

Birmingham
63 Church Street
Birmingham
B3 2DP

Cambridge
Compass House
Chivers Way
Histon
Cambridge
CB24 9AD

Cheltenham
Ellenborough House
Wellington Street
Cheltenham
GL50 1YD

Hereford
Thorpe House
29 Broad Street
Hereford
HR4 9AR

London
New Broad Street House
35 New Broad Street
London
EC2M 1NH

Thames Valley
100 Longwater Avenue
Green Park
Reading
Berkshire
RG2 6GP

Worcester
5 Deansway
Worcester
WR1 2JG

Wye Valley
Overross House
Ross Park
Ross-On-Wye
HR9 7US

www.hcrlaw.com | @HCRlaw