INSIGHTS

MAY 2019

UNLOCKING GDPR

Answering your GDPR questions one year on

Call us on:

01905 900001

harrison clark rickerbys

SOLICITORS

INSIGHTS: UNLOCKING GDPR

Answering your GDPR questions one year on

The initial steps towards compliance and the ongoing embedding of the GDPR within 'business as usual' has been, and continues to be, a journey for businesses across all sectors in the UK. In May 2019, one year after the introduction of the new regulation, we invited businesses to ask us their data protection questions. These ranged from queries about data storage, to how to encourage staff to adopt change. In Insights: Unlocking GDPR, you'll find our answers to these questions, with tips and advice on how you can tackle the common GDPR challenges in your business.

67%

of businesses we spoke to said it's been harder to comply with the GDPR than they were expecting.

TALK TO US ABOUT UNLOCKING GDPR
Call us on: 01905 900001

hcr law

THE INTERNATIONAL STAGE

The GDPR impacts every organisation that processes or holds personal data of EU individuals or exports personal data outside of the EU and EEA areas. With the increasing number of UK businesses that operate internationally, and uncertainty over the UK's future relationship with the EU, questions about GDPR and data breach are common.

You asked

Working across two countries in the EU, including the UK, will breaches need to be reported to both jurisdictions when the UK leaves the EU, or just where the breach took place?

We answered

Each supervisory authority is responsible for effectively enforcing GDPR in relation to processing activities of data controllers established in its member state; in the UK this is the Information Commissioners Office (ICO).

In the event of a data breach, an analysis would need to be carried out to establish which is the relevant data controller, and, depending on where it is established, and whose data is affected, which supervisory authority should be notified. Regardless of the UK's membership of the EU, it could in fact be both.

GDPR provides for a lead supervisory authority to be selected where an organisation has entities across the EU. The lead authority arrangements will no longer apply when the UK leaves the EU and, where an organisation is established in both the UK and an EU country, they will have to deal with both the ICO and the supervisory authority in the other EU state where it is established.

You asked

How can we know how to implement Step 5 of the ICO's 'Leaving the EU - Six Steps to Take' leaflet since it doesn't define "what details need updating"?

We answered

The ICO's 'Leaving the EU – Six Steps to Take' leaflet is a useful guide for any business that wants to know more about how Brexit will impact GDPR compliance.

To answer the question, this depends on what your privacy notices, terms and conditions and other documentation say now. But, at the very least, references to EU law and other EU terminology will need to be updated to reflect UK terminology and UK implementing legislation. If your documents refer to international transfers, you may need to amend these, e.g. if your terms say you will not process data outside the EEA, this could be an issue for a UK business if the UK does not remain in the EEA. We urge you to review the documents now so that you are ready to make the necessary changes when the time comes.

TOP TIP

Worried about Brexit?

Take a look at the ICO's 'Leaving the EU – Six Steps to Take' leaflet.

TALK TO US ABOUT UNLOCKING GDPR
Call us on: **01905 900001**

INTERACTIVE LINK

hcr law

ENGAGING YOUR PEOPLE

It's well known that the vast majority of data breaches or incidents involving data mis-use are caused by human error. Training staff in the rules, educating them on the importance of compliance and indeed 'fessing up' if something goes wrong, is vital.

HUMAN ERROR

"The vast majority of both non-reportable incidents and confirmed data breaches are unintentional or inadvertent in nature."

You asked

For companies that don't have an IT department, but for example, have over 150 customers and 300 staff, who do you suggest is involved in GDPR compliance?

We answered

GDPR compliance needs the participation of all sections of an organisation that handle personal data – the IT department is not the default setting for GDPR. If the question is about who should take the lead, it needs to be a person (rather than a team) genuinely empowered to ask the searching questions, with the time to do the work, and the authority to ensure actions are taken. We recommend an exec-level sponsor.

67% **of businesses we spoke to said they'd had a data breach.**

You asked

How do you audit GDPR and how often is this done? Also, how can you encourage other staff members to get involved in rather 'black and white' subject matter?

We answered

Auditing for GDPR compliance should be an on-going process. The principle of 'privacy by design and default' enshrined in the regulation dictates that compliance with GDPR should be built into an organisation's processes as a whole, but also implemented on a project by project basis from the outset (i.e. from the planning stage).

Any organisation, if starting from scratch, should begin the audit process by assessing what data it holds and mapping how data flows around the business. This should also be carried out each time a new project is planned.

Specific, regular audits should be taking place to ensure that GDPR principles are followed and compliance monitored (e.g. not holding personal data for longer than is necessary).

In terms of encouraging staff members to get involved, we advise organisations to take an approach which should be filtered throughout the organisation, so any staff members involved with processing personal data are kept up to date with requirements and encouraged to participate in the spirit of 'privacy by design and default'.

TOP TIP

Engage your people early. Involve them, train them and train them again!

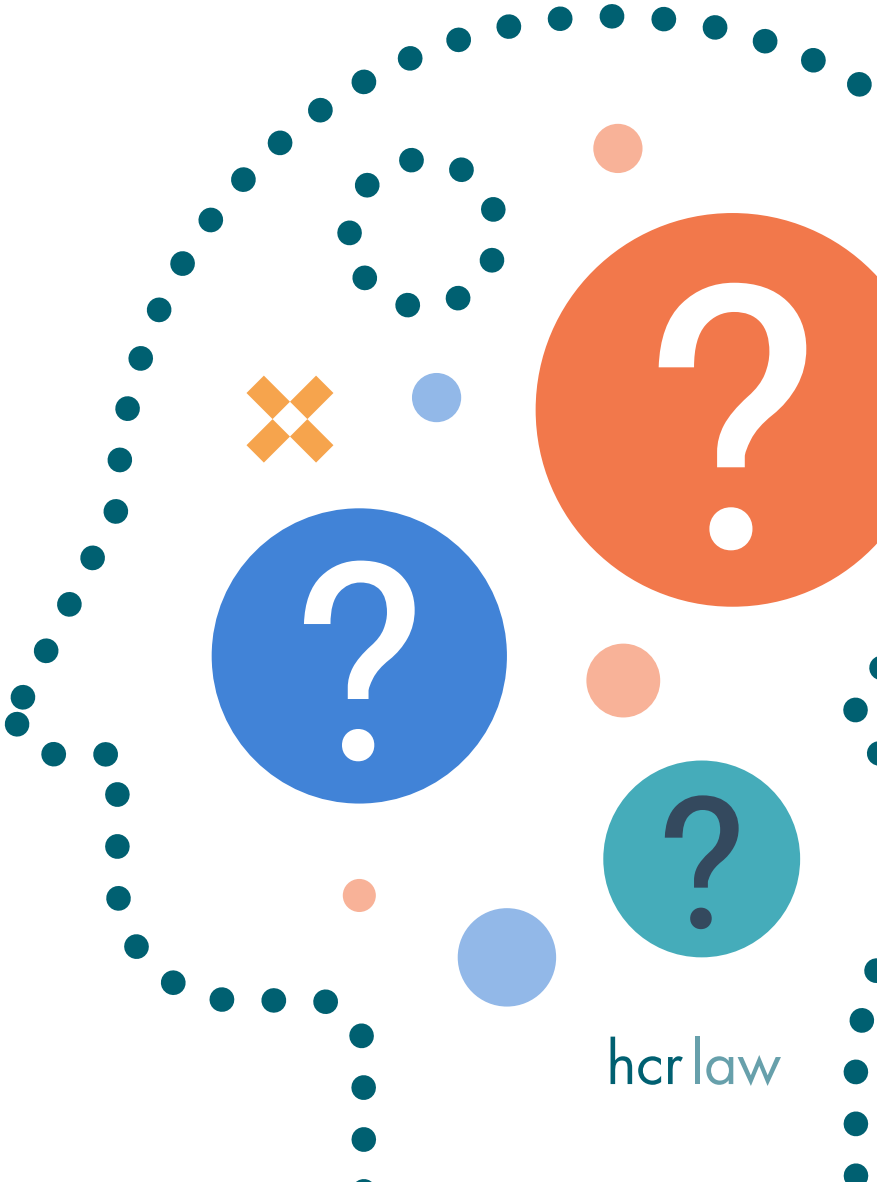
You asked

Recruiters often move elsewhere with their 'little black book'; how can you realistically stop that happening? What about new recruiters you bring in?

We answered

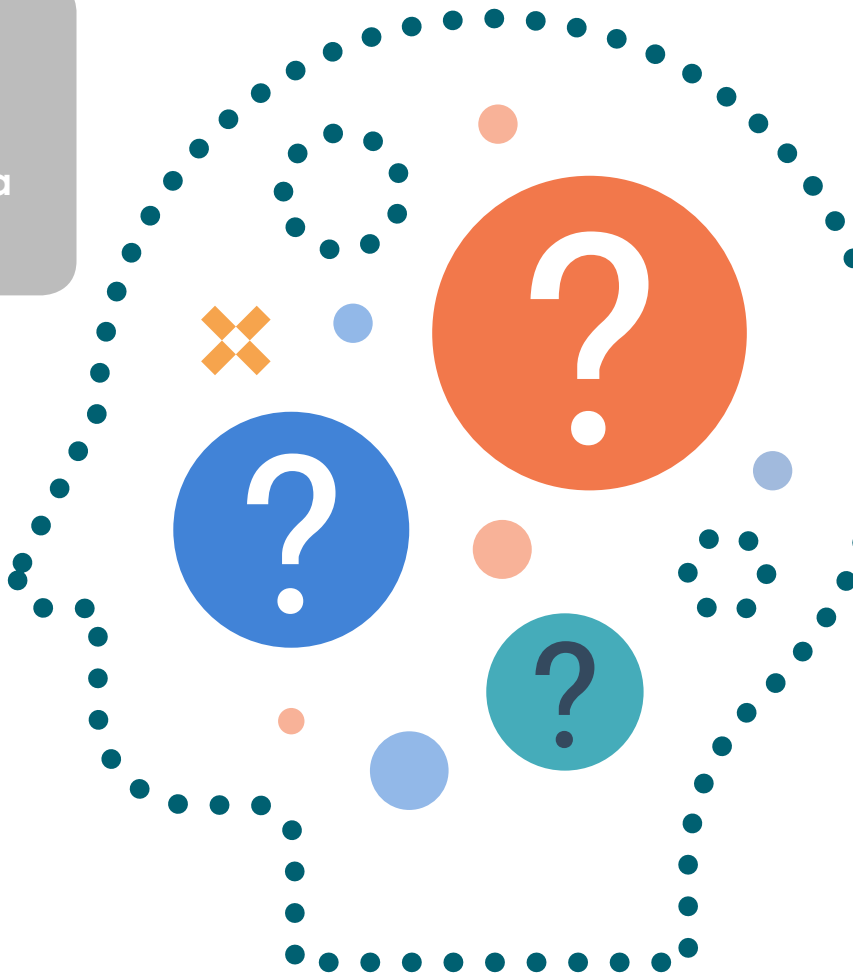
Such practices have implications for recruiters and indeed any employees.

Employers should ensure they communicate clear procedures to recruiters and staff, and plan to enforce these measures, if necessary, when they move on. As an employer, it is in your organisation's interests to make sure new employees are not in breach of their former employment contract terms and GDPR.



You asked

Is staff GDPR awareness training a legal obligation under the GDPR or a recommendation?



We answered

GDPR does not specifically require organisations to provide staff GDPR-awareness training. However, it does state that data controllers are responsible for, and must be able to demonstrate compliance with, the six principles relating to processing of personal data set out in **Article 5 of the Regulation**.

Providing staff training is one of the many ways in which data controllers can demonstrate compliance. In any event, as a matter of good practice, staff training should be provided, especially in medium to large sized organisations where personal data processing is likely to be carried out in various functions around the business, from HR to payroll to 'front of house'.

Aside from needing to demonstrate compliance, it would be hard for most businesses to achieve compliance without filtering that awareness throughout the organisation in a consistent way. Many businesses make data protection training mandatory as part of their induction and on-going training programmes.

39% **of SME owners don't know who GDPR affects.**[1]

TALK TO US ABOUT UNLOCKING GDPR
Call us on: **01905 900001**

hcr law

1 GDPR still a mystery to SMEs: the risks of non-compliance, January 2019, www.hiscox.co.uk

DATA ACCESS AND STORAGE: GETTING IT RIGHT

Most organisations are part of a supply chain. Even as a sole-trader if you use a service such as Office 365 or a server hosted at a remote data centre, you're in a supply chain. As such, the GDPR says that you must have a contract to govern data processing, and that contract must include certain items. We're often asked about such contracts, and how to meet GDPR requirements for transparency. Getting it wrong by not understanding the implications of the way your data is processed, is a business-killer.

You asked

What is your advice to ensure that a back-up system doesn't fall foul of GDPR data retention rules?

We answered

Insofar as back-up data includes personal data, it requires the same protection as production data, and that includes the rules on retaining data for too long. This is where data protection by design is relevant: your back-up system should be designed to facilitate purging personal data at the relevant time. Using tape-based systems can make that difficult.

A difficulty arises when a back-up is used as an archive. Back-up cycles typically wouldn't last so long that unreasonable retention of data is a particular problem. If the question is really about keeping archives of historical data, maybe for years, the risk of keeping data for too long then becomes acute.

TOP TIP

Do not allow another company to handle your personal data unless you know where it is stored.

You asked

If your CRM stores data outside the UK, does that count as transferring data outside the UK?

We answered

Yes - that data probably includes personal data and it is being transferred outside the UK. Right now, storing data outside the UK isn't a problem – the issue is whether you are transferring data outside the European Economic Area (EEA). If your CRM stores data outside the EEA, you will need to meet the requirements for ensuring that data has 'adequate' protection. That requires scrutiny.

You asked

What if a company such as Google handles your company's emails and they are unable to confirm where the data is actually stored?

We answered

You should not allow another company to handle your personal data unless you know where it is stored. You don't need to know the exact building or facility – you do need to know the jurisdiction in which it is stored, who has your data, and how and why it is being processed. You also need to know if that company shares it more widely (e.g. for back-up purposes).

You asked

What are the risks under GDPR of using password managers?

We answered

Password managers could form part of the measures an organisation adopts to deal with information security, even if the tool does not itself store personal data. Assuming a good password manager is used, the GDPR risks associated with using it could include:

- deploying the tool so that personal data is put at risk by over-sharing (a facility available in many solutions)
- failure of an organisation to take control over security tools (because many of these tools are downloaded by employees who might use them to mix personal and employer passwords).

Using tools for the prudent management of passwords is better than having people use the same password for multiple systems, writing down passwords in their diaries, or adopting passwords known to a whole team of employees etc.

96% **of SME owners don't know the maximum fine for breaching GDPR.**[2]

hcr law

2 GDPR still a mystery to SMEs: the risks of non-compliance, January 2019, www.hiscox.co.uk

DATA FOR MARKETING

Many marketers saw GDPR as an opportunity to ask their customers to re-consent to receive email and other marketing communications. Doing this generally led to a loss of contacts as customers didn't sign back up and subsequently had to be removed from mailing lists. But as an unexpected happy consequence, it also led to increased engagement as those that did stay signed up were those that were actively interested in receiving information from the company. With the new e-Privacy Directive on the horizon, replacing the Privacy and Electronic Communications Regulations (PECR) marketers need to be 'on the ball' with the rules.

You asked

If you buy in data for marketing, (name and commercial email addresses only) is this covered by the GDPR or Privacy and Electronic Communications Regulations (PECR)?

We answered

Both. To check if an email sent to individuals included in data bought from a data broker for a specific use was compliant under the GDPR and PECR, we would need to review the contents of the email before advising.

It's important for organisations that do buy email data for marketing purposes to receive appropriate contractual assurances from the supplier that the data can be used for the purpose intended.

TOP TIP

Keep an eye out for news on the e-Privacy Directive as this will undoubtedly affect your business.

SAVVY

You asked

Is the practice of asking for an email address in order to provide you with a receipt and then sending you marketing emails GDPR-compliant?

We answered

Asking for an email address to send a receipt and then using it for marketing purposes is collecting data for one purpose and then using it for another purpose, which would be a breach of both the GDPR and the PECR. A retailer would need to take additional steps to be compliant.

72%

of customers say they are aware of GDPR.[3]

TALK TO US ABOUT UNLOCKING GDPR
Call us on: **01905 900001**

hcr law

3 Chartered Institute of Marketing Catalyst magazine, April 2019

WHAT IF IT GOES WRONG?

Whether you've emailed the wrong recipient or you've suffered a cyber-attack, if you've experienced a data breach of any nature, you must take action. Our GDPR Survival Guide shows you how to structure your data breach response plan and provides practical advice on the action you must take.

55% **of UK firms faced a cyber attack in the last year.**

That's up from 40% in the previous year.

The average cost of an attack in the UK is nearly £190,000[4]

You asked

How do I know if I have to report a data breach to the ICO?

TOP TIP

Ask us for a copy of our GDPR Survival Guide. Email events@hcrlaw.com

We answered

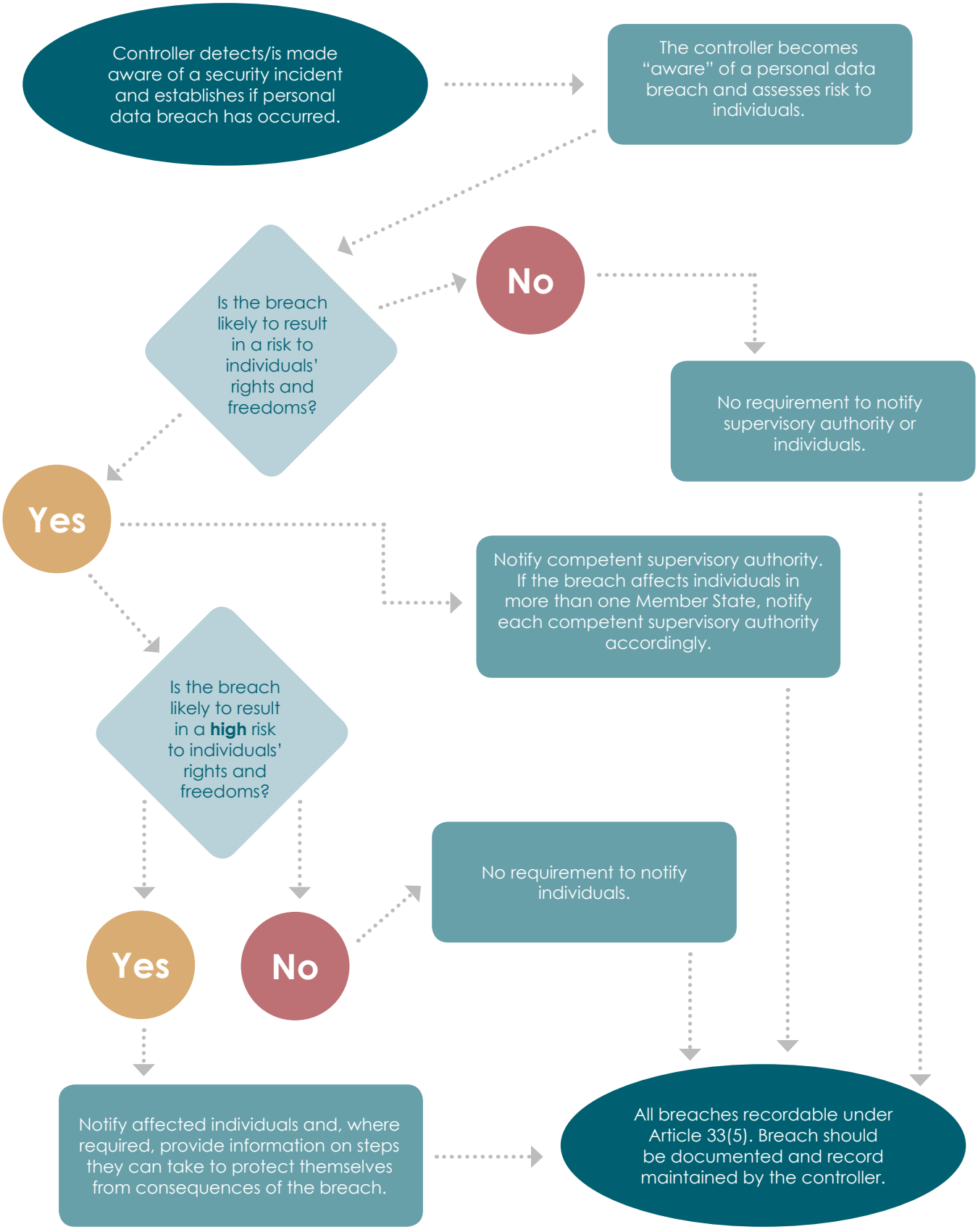
Use our flow chart to work through whether you need to notify the ICO. Remember; not all breaches are reportable but they should all be recorded.

TALK TO US ABOUT UNLOCKING GDPR
Call us on: **01905 900001**

hcr law

4 Third annual Cyber Readiness Report, Hiscox, April 2019, www.hiscox.com

GDPR NOTIFICATION REQUIREMENTS PROCESS



Source: European Commission's 'Article 29 Data Protection Working Party'

You asked

Do all companies, regardless of size, need to register with the ICO?

We answered

Any organisation (including charities and sole traders) which processes personal data belonging to EU citizens, regardless of the size of the organisation, is likely to need to register with the ICO, although there are a few specific exemptions. In most cases there will also be a registration fee to pay. The ICO has three tiers of fees which will apply, depending on the size of the organisation, and it has recently issued its first fines against organisations which failed to pay.

You asked

What is market practice on capping liability for GDPR breaches?

We answered

Among contracts that get reviewed, customers invariably ask for unlimited liability. Among experienced suppliers, most will refuse uncapped liability. The frequent compromise is a so-called 'super-cap', that is a special limit on liability for GDPR breaches, and that super-cap is frequently between 2 and 5 times more than the 'general cap' on liability.

For example, a contract which limits most liability to 100% of the fees paid under the contract in a 12 month period might have a super-cap of 200% to 500% for GDPR breaches.

TALK TO US ABOUT UNLOCKING GDPR

Call us on:

01905 900001

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
3rd Floor
3 St Helen's Place
London
EC3A 6AB

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

harrison clark rickerbys
SOLICITORS