
# ARE YOU READY FOR THE GDPR?

WHAT BUSINESSES NEED TO KNOW ABOUT THE GENERAL DATA PROTECTION REGULATION AND ITS RELEVANCE TO CYBER SECURITY

Made possible

QBE

# Contents

# The cyber landscape is changing – fast

It is the biggest change in data protection law in 20 years. On 25 May 2018, the European Union's General Data Protection Regulation (GDPR) comes into force – replacing the UK's 1998 Data Protection Act (DPA).

The scope of the new regulation is wider and penalties for failing to comply more onerous. The latter could amount to as much as 4 per cent of a company's global turnover or €20m – whichever is greater.

No company will be immune. UK businesses will soon find themselves rethinking their data storage and security procedures.

Brexit has no bearing on this. The government has confirmed that the UK's decision to leave the EU will not affect implementation. Moreover, the GDPR will apply to UK companies dealing with people in the European Union.

There are good reasons for the new regulation. Recent high-profile data breaches illustrate that companies need to get their house in order when it comes to data protection. If not, companies leave themselves open to cyber attack, which can compromise the security of their data.

It's a myth that small and medium-sized businesses are less at risk. In fact, there's a trend towards targeting those with less robust measures in place and using them to gain access to larger companies. In 2016, companies in the UK experienced a total loss of more than £1 billion that was attributed to online crime.

Businesses are finding that encrypting data isn't enough on its own to prevent fraud or misuse. Cyber-security encompasses more than just hacking and phishing and data protection covers everything from email marketing to hanging on to files longer than is necessary.

# So what is the GDPR?

It's been a long time coming. The result of four years' work, the GDPR is a regulation designed to strengthen and unify data protection for individuals within the EU. It clarifies for businesses how to process and store data, and as a result reduces mismanagement of data and encourages a better corporate culture around personal information.

Currently the Data Protection Act 1998 allows the Information Commissioner's Office (ICO) to issue fines of up to £500,000 for serious breaches.

The GDPR is altogether broader and the consequences for breaches more punishing. Jade Kowalski, solicitor at DAC Beachcroft and specialist in data protection, says

**"This is a milestone moment in the world of data protection law. The GDPR is the first substantive update of data protection laws in two decades. With the countdown to compliance already well on its way, every organisation should be preparing for the impact that the GDPR will have on business practices."**

**"Much of the GDPR will be familiar territory, supplementing and enhancing those rights and obligations which are already present in the Data Protection Act 1998 and associated guidance. However, the GDPR does make the obligations on companies processing personal data more prescriptive and the rights of data subjects clearer and easier to enforce. Compliance with the new principle of accountability is likely to prove particularly onerous with the paper trail of compliance becoming crucial."**

She adds

> Every organisation will need a greater command over the data it holds, why it is held and how long it is held for. This will require a seismic change of attitude for many. Fines, which can now be as much as 4% of annual worldwide turnover, will mean that data protection will need to be on the boardroom agenda.

Currently, the DPA applies to data controllers only and not to processors. A data controller is the person, business or organisation that determines how and why data is processed. A data processor is one who is acting on the controller's behalf. For example, a payroll service running payments for a business would be the processors while the business would be the controller.

The GDPR will place specific legal obligations on processors and controllers – such as being required to maintain records of personal data and processing activities, and for the first time, they will also have direct legal liability if a breach occurs. Civil claims can also be brought by data subjects affected by a breach against both the data controller and data processor, who may have joint and several liability. Controllers will be required to ensure that contracts with all processors comply with the GDPR and cover off liabilities appropriately.

## Consent: a big change

One major area in which the GDPR differs from the DPA is that of consent. Under the GDPR, data controllers will have to go to greater lengths to demonstrate valid consent for data usage. For example, sending marketing emails to a customer who hasn't explicitly chosen to receive them.

Under the DPA, individuals have the right to have personal details erased if their retention results in unwarranted and substantial damage or distress. Under the GDPR, the threshold is different and consent must be verifiable, which means a record must be kept of how and when consent was given.

Moreover, individuals have a right to withdraw consent at any time. Companies will also need to make sure it's as easy to withdraw as it is to give consent. If withdrawn, their data should be permanently deleted and not just removed from one document or mailing list.

Consent must be a positive indication of agreement to personal data being processed and cannot be inferred from silence, pre-ticked boxes or inactivity. Controllers must be able to demonstrate that consent was given, so a clear and effective audit trail – such as saved consent forms – is key.

For more information on issues around consent, visit https://ico.org.uk/about-the-ico/consultations/gdpr-consent-guidance/

## Subject access requests

Subject access requests allow an individual to ask for a copy of any data an organisation may hold about them, as well as details of why it's being processed and the source of the data.

GDPR rules for dealing with subject access requests are different. In most cases, companies will not be able to charge for complying with a request. They will also have only a month to act, rather than 40 days. Grounds for refusing to comply with subject access requests are different; unfounded or excessive requests can be refused or charged for.

However, policies must exist to demonstrate why the request meets these criteria. Controllers will also be obliged to provide extra information to anyone making a request, such as data retention periods, and the right to have inaccurate data corrected.

## Notification of a breach

In the event of a data breach, businesses have an obligation to inform the local supervisory authority in their home country within 72 hours of having been made aware of it. the GDPR defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, transmitted, stored or otherwise processed".

The notification must include the number and categories of data subjects and personal data records affected, the data protection officer's contact information, a description of the likely consequences of the breach and a description of how the controller proposes to address it, including any mitigation efforts. Such breaches can lead to fines of up to 4 per cent of global annual turnover, regardless of the country in which the incident took place.

# Do you need a data protection officer?

Under the GDPR, organisations and businesses are obliged to appoint a data protection officer (DPO) if they are a public authority (with the exception of courts acting in a judicial capacity) or if they carry out large-scale systematic monitoring of individuals, large-scale processing of special categories of data or data pertaining to criminal convictions and offences.

The job of the DPO is to independently supervise compliance with GDPR requirements as well as advise staff who deal with personal data. DPOs, therefore, are required to have expert knowledge of data protection law and practices. Companies by law will not be able to block or influence the work of their DPO.

# What types of data are affected?

The GDPR applies to personal data. However, its definition is more detailed than that of the DPA and includes such things as online identifiers, including IP addresses. It's reasonable to assume that if the data you hold falls under the remit of the DPA, it will also do so under the GDPR.

This also extends to data that in isolation couldn't identify an individual but if combined with information from elsewhere could identify them. There will be situations where the data you hold enables you to identify an individual whose name you do not know and you may never want to know.

Equally, a combination of data about age, sex, and remuneration may facilitate the identification of a particular employee without even a name or job title.

# GDPR in a nutshell

The GDPR is enforceable from **May 2018**

It **replaces** the existing **Data Protection Act**

Companies based **outside of the EU** but dealing with people within it will be **subject to the GDPR**

Data controllers must notify their local supervisory authority **within 72 hours** of having been made aware of a data breach

Maximum fines of up to **4%** of annual worldwide turnover or **€20m** whichever is greater – can be applied for breach of the GDPR

# What can you do?

### Worst case is best

All organisations should assume that they will be breached at some point and work backwards from there. Adopting this defensive mentality means robust security measures will be implemented.

Under the GDPR, businesses have an obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk and must be able to show they have considered and integrated data protection into all data processing activities.

### Staff training. It's a cultural thing

Changing staff culture should happen from the ground up and the top down. While board members perhaps haven't traditionally concerned themselves with IT issues, the more companies realise that their reputation is at stake the more likely the board are to buy into it. The requirement that DPOs have to report into boards will help change company culture.

The earlier you begin planning for GDPR compliance, the better. It might be necessary to adopt new procedures to deal with the need to be transparent about data handling and the new data subject rights (such as the 'right to erasure') – and this could have budget, personnel and governance implications.

It's also wise to set up standard operating procedures – outlining exactly what will happen after a data breach before any incident occurs. Conduct breach scenario testing and rehearse what each person would do in such a situation. It's a good idea to have a register of people assigned to each part of the process, from public-facing to operations.

### Storage protocols. Know where you put data

Correctly storing your data is as important as protecting it from a data breach. Consider undertaking a data audit to understand what information you hold, where it came from, who you share it with and who's doing the sharing; recording the outputs in a data register.

The procedure should include details of how data will be shared and deleted if requested by a customer. Under the GDPR, individuals will have the right to subject access, to have inaccuracies corrected, to have information erased, and to prevent direct marketing, automated decision-making, profiling and data portability (the movement or copying of personal data from one IT environment to another).

Have a procedure for locating and deleting the data as well as agreeing on who makes the deletion decisions. You will also have to explain your legal basis for processing personal data in any notice (the information you make available to anyone whose data you collect).

### Levels of compliance and certification. Get ahead of the game

You should have a robust system for seeking, obtaining and recording consent as well as the correct procedures to detect, report and investigate a data breach.

Since 2014, the UK government's Cyber Essentials Scheme has been obligatory for suppliers of government contracts involving the handling of personal information and providing some ICT products and services. It is a government-backed, industry-supported scheme to help organisations to protect themselves against common cyber attacks. The scheme is still voluntary, but getting a Cyber Essentials certificate is a great way to protect against common cyber threats.

Moreover, having a Cyber Essentials 'kite mark' shows customers you're taking the issue seriously. Many procurement departments will demand certification before agreeing to a tender. Having this will put your company at an advantage. Rushing to catch up when you don't have one could put you at a competitive disadvantage.

## Cloud services don't get you off the hook

If you store or use data in the Cloud, you remain the data controller for that data, not the Cloud provider. As such, you are still responsible for that data under the GDPR, meaning you have to notify individuals within 72 hours following a data breach. If you use a Cloud-based data processor, such as an online payroll system for your employees, both of you could be jointly liable. Much of the GDPR will be played out in court and this fact could lead to contract conflicts between the parties involved.

## Privacy by design

Privacy by design requires companies to build security and privacy upfront into systems. A Privacy Impact Assessment (PIA) is a useful tool for identifying and reducing any privacy risks. Having one can help when designing more efficient and effective processes for handling personal data. A PIA should outline potential risks to the individuals whose data is being processed as well as corporate risks to the company carrying out the task. This may involve the financial and reputational impact of any data breach. The ICO (Information Commissioner's Office) has produced guidance on PIAs and how and when to implement them.

## What should you implement to be compliant?

- Privacy should be designed into the processing of personal data by default.
- A Privacy Impact Assessment will outline potential risks to everyone handling data.
- Ensuring staff are fully aware of data risks and regulations means that external breaches are less likely to occur.
- Implementing a clear-desk and data retention policy reduces issues due to human error. The same applies to electronic data, but remember you have to be able to demonstrate deletion in some cases.
- Having data encrypted (strongly enough) is deemed less of an issue if that data is lost
- Regularly reviewing your security infrastructure is crucial. Consider penetration testing annually to identify network vulnerabilities.
- Data controllers should carefully review contracts and other arrangements when sharing data with outside organisations.

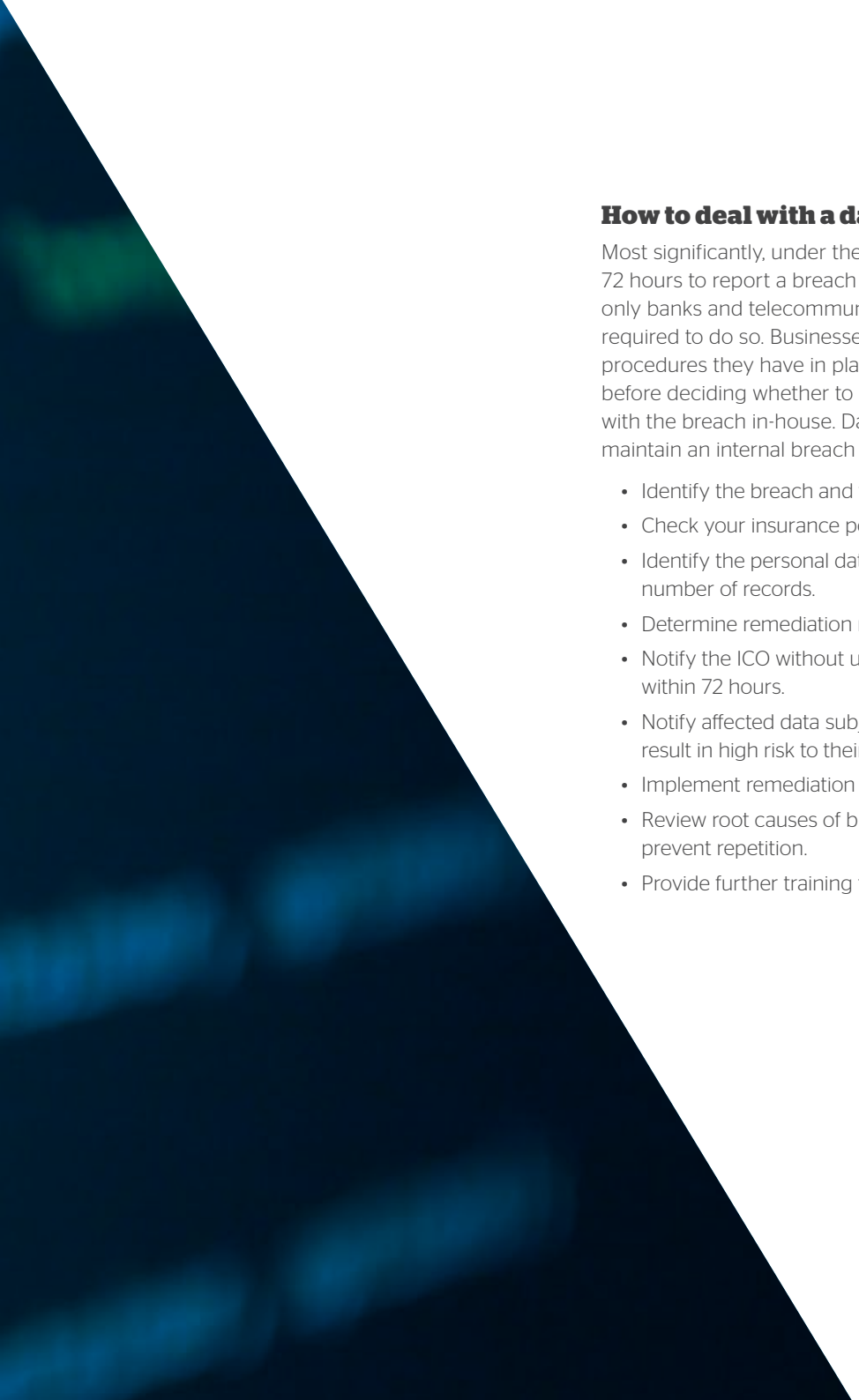
# Case study: QBE

As soon as the GDPR came into view, QBE set up a working group comprising experts in compliance, legal, information security, data governance architecture and project management.

The group drew up a model – to define the organisation's data protection capabilities – and went through the new legislation line by line to determine what would be required for each clause. The group ended up with an analysis tool.

Crucially, says Iain Heron, enterprise information architect at QBE European Operations: "We identified that this is a business-change issue and not an IT issue. There is a lot of personal data floating around, but actually it's not the systems that are important, it's the culture change."

Heron adds: "The people who handle calls from customers need to be aware not only that the stuff they're handling every day has a value, but also that if we don't look after it properly it has a negative value." The company also runs breach scenarios: "Because you don't know whether someone can do the job until they're tested."



## How to deal with a data breach

Most significantly, under the GDPR a data controller has 72 hours to report a breach to the regulator. Currently only banks and telecommunications companies are required to do so. Businesses should consult the procedures they have in place to manage incidents before deciding whether to call in the experts or deal with the breach in-house. Data controllers should also maintain an internal breach register.

- Identify the breach and take steps to end it.
- Check your insurance policy and notify your insurer.
- Identify the personal data breached - type of data and number of records.
- Determine remediation measures.
- Notify the ICO without undue delay and in any event within 72 hours.
- Notify affected data subjects if the breach is likely to result in high risk to their rights and freedoms.
- Implement remediation measures and monitor.
- Review root causes of breach and take steps to prevent repetition.
- Provide further training to staff as required.

## What duty do you have to your customers?

If a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller is obliged to contact the data subject. However, if the controller has put measures in place to mitigate these risks or the contact process would involve disproportionate effort then this may not be required.

If a breach has occurred, follow your internal notification procedures and incident response strategy, check for cover in relevant insurance policies and notify your insurer. Consider temporarily storing your electronic data at a third-party location, if you believe it remains vulnerable to damage, destruction, alteration, corruption, copying, stealing or misuse by a hacker.

In the aftermath, data processors and controllers should learn from the incident and update their internal notification procedures and incident response strategies accordingly.

# After a breach

## Dealing with reputation management

Data breaches are great fodder for journalists and many high-profile cases could have been minimised with the right PR. It's worth engaging prior to an incident the services of a PR company experienced in reputational damage so that you are ready to respond in the event of a breach and that ensure key messages are communicated. Make sure all staff know the agreed procedure for dealing with press enquiries and are aware of how any statement they make could be interpreted.

## Getting back on your feet

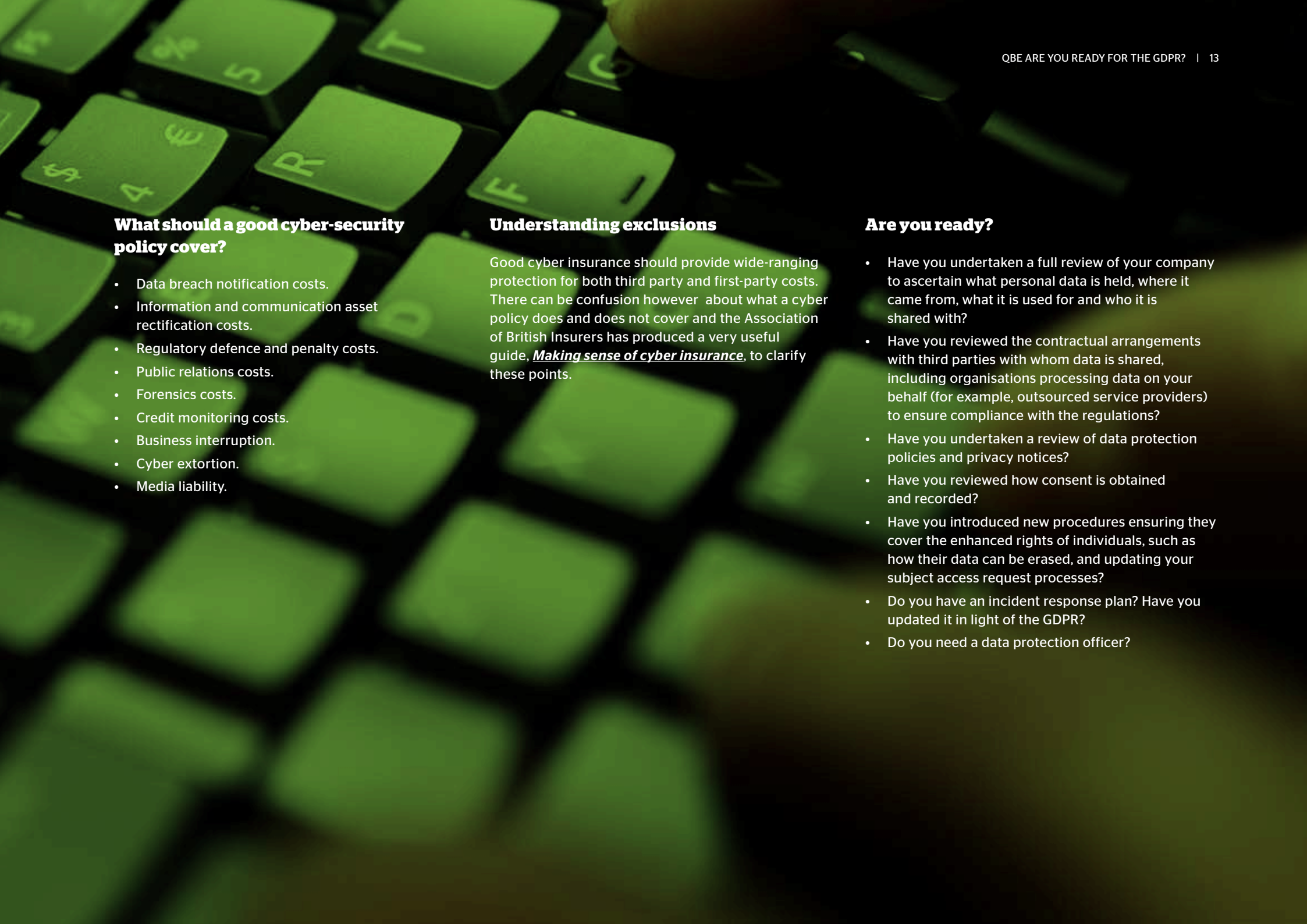
Having a crisis management plan will help to maintain continuity and reassure customers that your business is operating as usual. It's crucial to establish clear communications with all stakeholders, both external and internal.

## Dealing with a breach

- Make sure you inform the relevant authority within 72 hours.
- Consult your incident management procedures; don't respond impulsively.
- Quarantine data that has been breached.
- Consider engaging a PR company experienced in crisis management.
- Inform any individuals who are likely to be adversely affected.

## Big breaches

- In 2013 Target Corporation's data breach resulted in the credit card numbers and personal information of around 70m people passing into the hands of cyber-criminals.
- An attack on JP Morgan Chase in 2014 resulted in compromised data of around 76m American households and 7m small businesses.
- In the UK in 2016, Tesco Bank revealed that 40,000 of their customers' accounts had been compromised, with as many as 20,000 having had money stolen from them.



## What should a good cyber-security policy cover?

- Data breach notification costs.
- Information and communication asset rectification costs.
- Regulatory defence and penalty costs.
- Public relations costs.
- Forensics costs.
- Credit monitoring costs.
- Business interruption.
- Cyber extortion.
- Media liability.

## Understanding exclusions

Good cyber insurance should provide wide-ranging protection for both third party and first-party costs. There can be confusion however about what a cyber policy does and does not cover and the Association of British Insurers has produced a very useful guide, ***Making sense of cyber insurance***, to clarify these points.

## Are you ready?

- Have you undertaken a full review of your company to ascertain what personal data is held, where it came from, what it is used for and who it is shared with?
- Have you reviewed the contractual arrangements with third parties with whom data is shared, including organisations processing data on your behalf (for example, outsourced service providers) to ensure compliance with the regulations?
- Have you undertaken a review of data protection policies and privacy notices?
- Have you reviewed how consent is obtained and recorded?
- Have you introduced new procedures ensuring they cover the enhanced rights of individuals, such as how their data can be erased, and updating your subject access request processes?
- Do you have an incident response plan? Have you updated it in light of the GDPR?
- Do you need a data protection officer?

# QBE cover 24/7 protection from cyber risk

Costs and liabilities arising from the use of information technology can hit your business in many different ways. In a digital and online business world, threats can emerge from almost any angle: from cyber attacks by criminal or activist hackers, to accidental or deliberate misuse or loss of customer data by one of your own employees.

At QBE we have put together an exceptionally wide range of specialist cyber covers and services to help keep your business safe.

**Our cover includes:**

- Cyber, data security and multimedia liability
- Data breach notification costs
- Information and communication asset rectification costs
- Regulatory defence and penalty costs
- Public relations costs
- Forensic costs
- Credit monitoring costs
- Cyber business interruption
- Cyber extortion.

# About QBE

QBE Insurance Group is one of the few global general insurance and reinsurance companies, with operations in all the key insurance markets.

QBE is listed on the Australian Securities Exchange and is headquartered in Sydney. It employs more than 14,500 people in 37 countries and has specialist cyber underwriters across its offices in the UK, Europe and Canada providing cyber cover to companies all around the world. QBE also offers free access to an online portal – QBE E-Risk Hub – which presents a wide range of information on data breaches and cyber attacks, as well as how to protect yourself from them.

Made possible


**QBE European Operations**

Plantation Place
30 Fenchurch Street
London EC3M 3BD

**Get in touch**

Visit QBEeurope.com
or email us at enquiries@uk.qbe.com
Tel: +44 (0)20 7105 4000





7706/AreYouReadyForTheGDPR/MAY2017