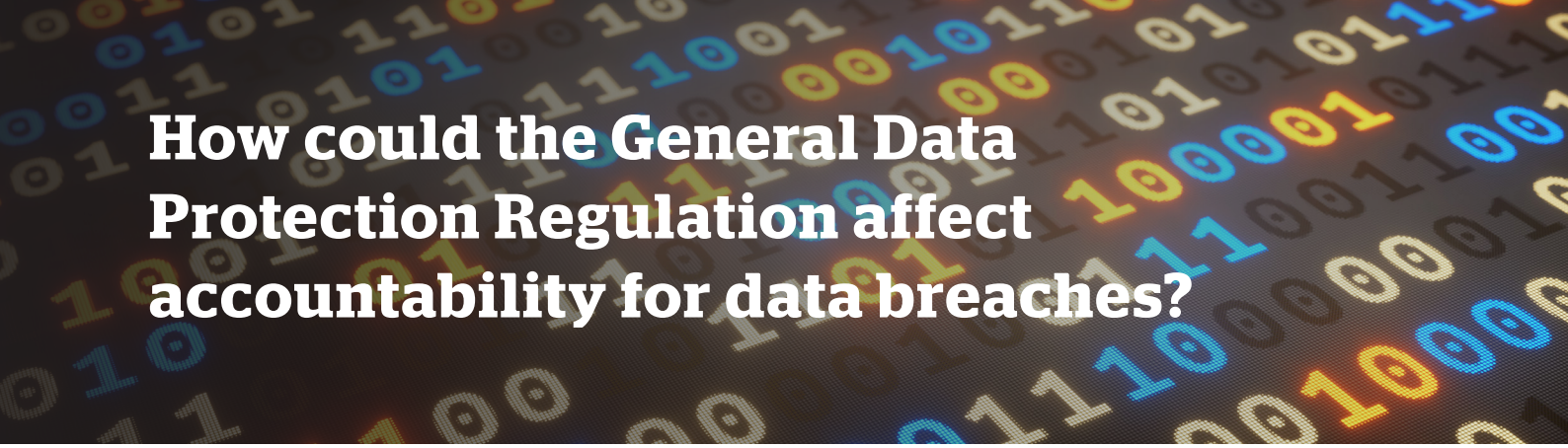

How could the General Data Protection Regulation affect accountability for data breaches?

When the General Data Protection Regulation (GDPR) comes into effect in May 2018, for many organisations it will affect more than just data processing. It may also alter your company line-up, because new responsibilities need to be allocated. This article looks at the mandatory DPO role as well as other roles you might consider creating if you are to meet its requirements.

The mandatory data protection officer (DPO) role

Under the GDPR, organisations and businesses must appoint a data protection officer if they carry out:

- Large-scale systematic monitoring of individuals; or
- Large-scale processing of specific categories of data or data which pertains to criminal convictions and offences; or
- If they are a public authority (with the exception of courts acting in a judicial capacity).

The DPO's role is to inform and advise the data controller or processor of their obligations to comply with the GDPR. They are further required to train employees who process data and monitor the company's compliance with the regulation. They will also work and cooperate with the designated supervisory authority on issues relating to the processing of data and be available for inquiries from data subjects.

The data protection officer can be an existing employee or an external appointment and is not obliged to have any specific training or credentials. However, the GDPR does require that they have professional experience and expert knowledge of data protection law and practices (proportionate to the type of data processing the organisation undertakes and the level of protection this data requires).

Given the obligations of the DPO and the seriousness of the penalties should a breach occur (fines of up to €20m or 4% of the company's worldwide annual turnover – whichever is greater), organisations should look at whether their Directors & Officers (D&O) insurance policy would indemnify the DPO in the case of litigation. Whilst many insurers have extended the definition of insured persons to include data protection officers under their D&O cover, it shouldn't be assumed that all insurers have followed suit.

Chief data officer/chief information officer (CDO/CIO)

Many organisations already have a chief data officer in place. Typically, they are corporate officers, responsible for general data governance and usage, and cover such things as data processing, data mining and information trading. The role of chief information officer differs slightly in that the CIO is also responsible for the IT systems supporting data processing. They will also review the maintenance of software, updating of old systems and the planning of new ones.

Whilst a CIO is not directly responsible for meeting requirements under the GDPR, they are held accountable should a breach occur. Given the role of a CIO is becoming increasingly high profile, it is likely your D&O policy would cover a breach as a result of any negligence on their behalf.

Chief cybercrime officer (CCO)

When the TalkTalk data breach took place in 2016, there was much discussion about how organisations might want to start appointing officers with specific day-to-day responsibility for fighting cybercrime. The role of such an officer would sit in the area of prevention – educating the board about potential data-breach risks and how to mitigate them, as well as working closely with the DPO.

Digital training officer (DTO)

It might feel like you've covered all the bases with your DPO, CDO, CIO and CCO, but in the new GDPR era it's crucial that compliance is company-wide. With human error one of the leading causes of data breaches, it is critical that all employees are aware of the risks and ramifications. Employee training is crucial to raise the awareness of cyber risks and is an importance defence in keeping hackers out of companies' networks.

How to meet the GDPR role requirements

With all new data roles, it's important to be very clear about their responsibilities. If you don't meet the criteria that requires you to employ a DPO, then there's no point in needlessly taking on the wider responsibilities this entails – so be careful not to give someone the title and status if you don't have to.

"Although the DPO role is only mandatory for particular organisations, one thing we're saying to a lot of our clients – particularly large ones – is that it's going to be hard to comply with GDPR unless you have an overseer who effectively is a DPO," says Jon Bartley, specialist in data protection and cybersecurity at corporate and insurance law firm Reynolds Porter Chamberlain (RPC). He adds, "Operationally you have to have people who understand privacy by design, so they can make sure every time something is thought up they are there with knowledge."

Bartley's colleague Richard Breavington, a specialist in technology-related litigation and cyber breach response, says that the idea of having even a voluntary DPO is useful in the breach notification stage: "We are already seeing sophisticated questioning and that getting the story you tell to the ICO (Information Commissioner's Office) straight first time is important. Having a DPO is a helpful part of this." And though cyber-insurance policies are still fairly inclusive, underwriters are and will remain very interested to understand if companies have implemented robust policies and procedures to avoid and respond to a breach of the GDPR.

As previously stated, the GDPR requires that someone with professional standing and experience fulfils a DPO role, however it is predicted that there's going to be a significant shortfall of skilled people available. It might be that you contract out the DPO role. Educational trusts, for example, may find it easier to appoint a regional consultant, meaning it's quite likely that new services will open up in this area. It's important to ensure that the DPO you appoint is easily accessible by your employees and data subjects, so if your head office is in Truro and you have a branch in Leeds, you will need to be sure that the DPO can easily respond and interact as required. Any DPO contract should carefully detail the level of service.

With accountability as a key theme within the GDPR, Cyber insurance is no longer the only relevant insurance to consider in the event of accidental non-compliance. Having the right roles in place is also a matter of responsibility to your shareholders and hence D&O insurance should be also considered. There have been several high profile data breaches in the past that have consequently resulted in shareholders attempting to make a claim against the breached company for not adequately protecting the company against this risk. With the updating of the data protection regulations and the requirements that this brings there is now no excuse for not ensuring adequate risk management is in place and this will include employing the right roles.

QBE would like to thank Jon Bartley and Richard Breavington from Reynolds Porter Chamberlain (RPC), for their expertise in developing this article.

QBE European Operations
Plantation Place 30 Fenchurch Street London EC3M 3BD
tel +44 (0)20 7105 4000 **QBEeurope.com**

8583/JAN/2018