CB COMPLY
Getting your business GDPR ready

The GDPR

Top 10 data protection issues for professional advisers

Collyer Bristow

Top 10 data protection issues for professional advisers

Data protection compliance may not have been the highest priority for many professional adviser firms in recent years. However, the General Data Protection Regulation (GDPR) comes into effect on 25 May 2018 and imposes significantly increased duties on data controllers, and eye-watering fines for serious breaches. Consequently, professional advisers would do well to undertake a review of their current policies and procedures and, where necessary, plan for changes to be made in order to be GDPR - compliant by next year.

THE TOP 10 ISSUES FOR PROFESSIONAL ADVISER FIRMS ARE:

1 Identifying Personal Data

Personal data is any data by which an individual may be identified. This is not restricted to names and addresses, but includes telephone numbers, computer IP addresses, and other data, which, when taken in combination, enables an individual to be identified. This will include employees, customers, suppliers, business contacts and prospects.

2 Establish where personal data is located

Data is likely to be held both in hard copy and electronically. Multiple copies of data are also likely to be held at different locations around an organisation. For the reasons which appear below, it will be vitally important for an organisation to know where all such data is located.

3 Have a procedure for dealing with Data Subject Access Requests (DSARs)

A DSAR can be made under the current law, but under the GDPR requests must be dealt with more quickly and thoroughly. A DSAR may well be followed by a request to rectify any inaccurate data that the organisation holds and/or for the erasure of all personal data without undue delay. It is important to have procedures in place to respond quickly and effectively when a DSAR is made.

4 Clarify the legal basis for processing data

Personal data can only be held and processed for lawful purposes. For marketing purposes, businesses often rely on implied consent from the data subject. Under the GDPR, consent cannot be implied. It has to be expressly given for specific purposes. This is likely to require a significant change in the way that professional advisers collect, store and use personal data. There are other legal grounds, but these need to be assessed carefully to ensure that they apply.

comply@collyerbristow.com

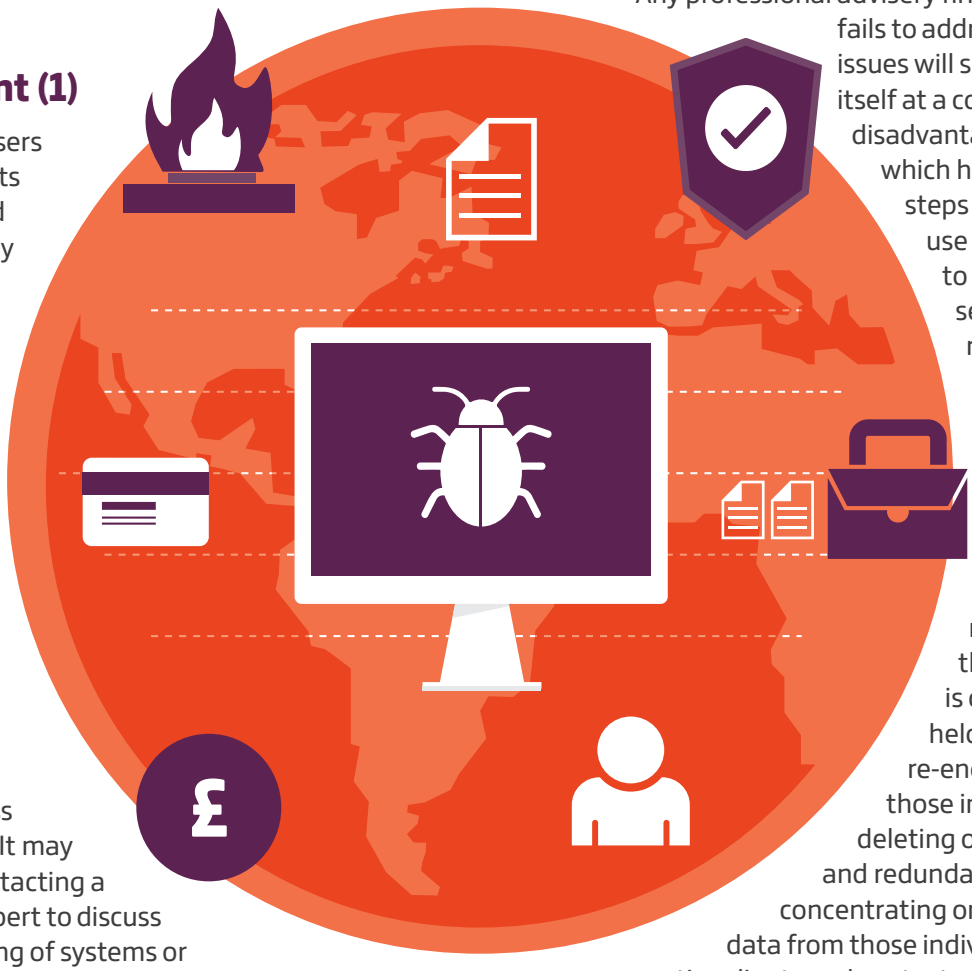
Top 10 data protection issues for professional advisers

5 Accountability

This principle underpins all of the GDPR. It requires data processers to be open and transparent in their dealings with data subjects and to have detailed policies and procedures in place to safeguard personal data. It is linked to the principles of 'data privacy by design and default'. This means that all new projects, policies and procedures will need to have data protection at their heart. Detailed records will need to be kept to prove that data privacy considerations are being given priority.

6 Risk Management (1)

Professional advisers are obvious targets for fraudsters and hackers. It is vitally important to update and strengthen fire walls, anti-virus and malware software, and that active consideration is given to checking the security of systems through which an unauthorised intruder may be able to gain access to personal data. It may well be worth contacting a cyber-security expert to discuss penetration testing of systems or other measures to improve security.



7 Risk Management (2)

The second big area of risk is unauthorised exposure of personal data. This can happen by an intruder accessing personal details, including financial and other confidential information, and using it for fraudulent purposes. It can also be caused deliberately by a disgruntled employee, or accidental loss by employees transporting data in an unsecured form (e.g. a laptop without a secure password or an unencrypted memory stick).

8 Fines / Penalties

The Information Commissioner's Office (ICO) can impose penalties which depend upon the seriousness of the breach. At the top end, the maximum fine is the higher of €20 million or 4% of global annual turnover. In addition, firms which are sanctioned by the ICO will suffer significant reputational damage which may be even longer lasting.

9 Competitive (Dis)Advantage

Any professional advisery firm which fails to address these issues will soon find itself at a competitive disadvantage. Firms which have taken steps to comply will use this as a tool to promote their services and to reassure clients that their data is safe. In addition, this is an opportunity to conduct a thorough review of the data that is currently held and to re-engage with those individuals. By deleting old, inaccurate and redundant data and concentrating on accurate data from those individuals who are active clients and contacts, the marketing value of such data is significantly increased.

10 Regulatory

Regulators across the professions are paying greater attention to data protection and privacy, in parallel with the ICO's obligation to enforce the GDPR. Advisery firms have the opportunity to get ahead of the curve by making their procedures compliant and will therefore reduce the risk of needing to take reactive steps for regulatory reasons.

comply@collyerbristow.com

CB COMPLY

Getting your business GDPR ready

How CB Comply can help

Our dedicated CB Comply team has substantial experience working with organisations on their data protection requirements. We provide a range of advice and assistance to support you in identifying and addressing the compliance challenges posed by the GDPR, from an initial discussion on your compliance gaps to a detailed audit, flexible and tailored specifically to your business, establishing the state of your current policies and procedures.

Once a thorough assessment of your business has been carried out and the compliance gaps have been identified, we will provide recommendations to reduce the risk of breaches occurring in the future and we can work with you to implement the necessary changes.

We have also identified a small number of experts in data security who can help you to establish the level of vulnerability of the data in your business and offer solutions to improve security, where needed.

Moving towards complying with the GDPR is likely to be a very significant task. Your organisation needs to start now to minimise the risk of a regulatory breach and a potentially large financial penalty.

If you are interested in discussing how we can support you in your programme towards GDPR compliance, please contact a member of our team on ☎ +44 (0) 20 7242 7363 or at comply@collyerbristow.com

Collyer Bristow