COLLYER BRISTOW

TOP 10 DATA PROTECTION ISSUES FOR PROFESSIONAL ADVISERS

Since 2018, data protection compliance has been much higher profile for many professional adviser firms. The Data Protection Act, which contains the UK GDPR, imposes significant duties on data controllers, with significant enforcement measures for serious regulatory breaches, including fines, and rights for individuals. In addition, both the impact of Brexit and the pandemic have heightened concerns about security of personal data, and both laws and guidance are changing on a regular basis. Professional advisers need to keep up to date about this changed and changing landscape. Our Top 10 Tips are as follows:

1. IDENTIFY PERSONAL DATA AND SPECIAL CATEGORY DATA

Personal data is widely defined. Employees, clients, suppliers, business contacts and prospects are included. Any data by which an individual may be identified is covered: names and addresses, telephone numbers, computer IP addresses, and other data, which, when taken in combination, enables an individual to be identified.

Special category data includes data relating to an individual's: racial or ethnic origin, religious or philosophical beliefs, health, sex life and sexual orientation. It is considered especially sensitive and is afforded greater protection under the GDPR so professional advisers need to exercise greater care in collecting and processing it.

COLLYER BRISTOW

TOP 10 DATA PROTECTION ISSUES FOR PROFESSIONAL ADVISERS

2. MAP 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. As explained below, it will be vitally important for an organisation to know where all such data is located, ideally by creating a data map.

3. KNOW HOW TO DEAL WITH DATA SUBJECT ACCESS REQUESTS (DSARS)

Data Subjects are entitled to ask for a copy of all personal data that a data controller holds about them. There are only limited grounds to refuse or limit such requests. Professional advisers may be entitled to withhold disclosure to the extent that they would be entitled to do so under established trusts and estates law, but this needs to be carefully assessed.

The fact that certain data may be withheld does not exempt the professional adviser from their obligations to deal with the DSAR quickly and thoroughly, since there is a one month time limit in most cases. It is therefore critically important to have effective procedures in place to respond appropriately when a DSAR is received.

4. KNOW YOUR LEGAL BASIS FOR PROCESSING DATA AND SPECIAL CATEGORY DATA

Personal data can only be held and processed for lawful purposes, and these must be notified to data subjects. It is important for advisers to be clear which purpose they rely on for each class of data. This should be clearly set out in a Privacy Policy, which needs to be tailored to the specific requirements of the individual business.

Processing of special category data requires additional justification – which must be determined before processing starts. The rules are complicated and professional advice is the best way to avoid problems and complaints.

COLLYER BRISTOW

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. Detailed records will need to be kept to prove that data privacy considerations were properly considered at the right time and to record why decisions were taken.

6. RISK MANAGEMENT (1)

Professional advisers are obvious targets for fraudsters and hackers. It is vitally important to update and strengthen technical security such as firewalls, anti-virus and malware software, and to check the security of systems periodically. It may well be worth contacting a cyber-security expert to discuss testing of systems or other measures to improve security.

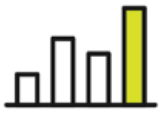
7. RISK MANAGEMENT (2)

The second big area of risk is unauthorised exposure of personal data. This can happen either accidentally or deliberately, whereby personal details, including financial and other confidential information, is accessed and used for unauthorised and/or fraudulent purposes. This may be caused deliberately by a disgruntled employee, or accidentally by a careless employee (e.g. losing a laptop without a secure password, or an unencrypted memory stick).

8. FINES / PENALTIES

The Information Commissioner's Office (ICO) can impose a range of penalties and enforcement measures which depend upon the seriousness of the breach. The maximum fine is the higher of £17.5 million or 4% of global annual turnover. In addition, firms which are sanctioned by the ICO will probably suffer significant reputational damage which may be even more damaging and longer lasting.

TOP 10 DATA PROTECTION ISSUES FOR PROFESSIONAL ADVISERS



9. COMPETITIVE (DIS)ADVANTAGE

Any professional advisory firm which does not keep its data privacy policies and procedures up to date will soon find itself at a competitive disadvantage. Effective policies and procedures can be used as a tool to promote services and to reassure clients that their data is safe. A thorough audit of the data that is currently held and processed can be used as an opportunity to re-engage with existing and former clients. Deleting old, inaccurate and redundant data and concentrating on accurate data from those individuals who are active clients and contacts increases the marketing value of such data.

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. Advisory firms without updated policies may find themselves under scrutiny. In addition, professional indemnity insurers take a keen interest in effective data privacy measures, the absence of which can result in greatly increased premium payments. Effective policies and procedures can greatly reduce these risks.

TO DISCUSS YOUR SPECIFIC REQUIRMENTS PLEASE CONTACT OUR DATA PROTECTION TEAM COMPLY@COLLYERBRISTOW.COM OR +44 20 7242 7363