COLLYER BRISTOW

TOP 10 DATA PROTECTION ISSUES FOR PROFESSIONAL ADVISERS

Despite the introduction of the General Data Protection Regulation (GDPR) in 2018, data protection compliance does not seem to have been the highest priority for many professional adviser firms. However, the UK GDPR imposes significant duties on data controllers, with equally significant enforcement measures for serious regulatory breaches, including fines. In addition, the pandemic has brought about a greater focus on security of personal data, so professional advisers would do well to undertake regular reviews of their current policies and procedures, in particular, if this has not been done since Brexit.

1. IDENTIFYING PERSONAL DATA AND SPECIAL CATEGORY 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, clients, suppliers, business contacts and prospects.

Special category data is considered especially sensitive and is afforded greater protection under the GDPR so professional advisers need to be alert to the rules for obtaining, holding and processing it. Special category data includes data relating to (among others) an individual's: racial or ethnic origin, religious or philosophical beliefs, health, sex life and sexual orientation.

Advisers should be mindful that they will frequently obtain personal data and special category data of third parties from their clients and deal with such data accordingly. For example, a client describing her children's relationships will not only be providing 'regular' personal data in the form of their names but may also be providing special category data relating to their sexual orientation.

COLLYER BRISTOW

TOP 10 DATA PROTECTION ISSUES FOR PROFESSIONAL ADVISERS

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 AN EFFECTIVE PROCEDURE FOR DEALING WITH DATA SUBJECT ACCESS REQUESTS (DSARS)

Although there were concerns that the enhanced access rights offered to data subjects under the GDPR would cut across existing law relating to disclosure of information (especially in trusts and estates law), this is not generally the case and professional advisers may be entitled to withhold information to the extent that they would be entitled to do so under established trusts and estates law.

However, 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 in accordance with GDPR and it is important to have effective procedures in place to respond appropriately when a DSAR is made.

4. CLARIFY THE LEGAL BASIS FOR PROCESSING DATA AND SPECIAL CATEGORY 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.

There are exceptions on which professional advisers may be able to rely, in particular where processing is necessary for compliance with a legal obligation to which the controller is subject or where processing is necessary for the controller's legitimate interests.

Processing of special category data requires additional justification – which must be determined before processing starts. Express consent is one option (although may be withdrawn at any time). Alternatively, professional advisers may process special category data without express consent to the extent that it is necessary for the purposes of establishing, exercising or defending legal rights.

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. 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 firewalls, 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 £17.5 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.

COLLYER BRISTOW

TOP 10 DATA PROTECTION ISSUES FOR PROFESSIONAL ADVISERS

9. COMPETITIVE (DIS)ADVANTAGE

Any professional advisory 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. Advisory 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.

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