Navigating Data Protection Compliance

Introduction - Why is data protection compliance important?

With recent data breaches in the sector hitting the headlines, the moral and ethical importance of complying with data protection regulations, (as well as the financial and reputational risks associated with non-compliance) are widely documented.

Generally speaking, stages 1 (discovery) and 2 (pre-clinical) life sciences organisations typically have limited exposure to the processing of personal data, except regarding day-to-day operations (current/former employees and recruitment applicants). Whilst this still constitutes the processing of personal data (and requirement to comply with data protection regulations), the point at which organisations move into Stage 3 (clinical stage) is when data protection risks significantly increase, as organisations process increasing volumes of personal and special category data about patients, either by conducting clinical trials, or outsourcing this to clinical research organisations (CROs). Later in the organisational lifecycle, for those looking to exit, due diligence processes invariably include a review of data protection controls, and a high-profile data breach could significantly impact the marketability of an organisation and its value.

Staying up to date with data protection compliance requirements in an evolving global regulatory landscape can be really challenging for organisations processing personal data in line with the UK General Data Protection Regulation (UK GDPR), and in the wake of new country-specific data protection regulations, globally. Organisations operating in the US will also be aware of ever-evolving, state by state privacy regulations, which can create compliance challenges

The challenge however for many life sciences organisations is knowing *where* to begin when implementing (or maintaining) data protection compliance, so here are five important steps that you can take, to get started.

1. Understand and document what you do with personal data

Developing a Record of Processing Activity (RoPA) is an important first step to ensure that you can demonstrate organisation-wide oversight of data processing activity. This will inform the contents of your Privacy Notice and data subject rights procedures but will also identify which third parties you are sharing personal data with. In turn, this will enable you to ensure that contracts are in place with third parties, which include the relevant data sharing clauses.

2. Develop and implement data breach and data subject rights processes - where strict time limits apply

The UK GDPR introduced the requirement for organisations to report certain types of data breaches to the relevant supervisory authority within 72 hours, therefore it is vital to ensure that data breach procedures have been defined and understood by all employees, for swift external notification (if required).

Subject access requests can also be time and resource intensive and should be processed within one calendar month of receipt (though this can be extended in certain circumstances). You should define and implement data subject rights request procedures, to ensure that the deadline is met and reduce the risk of complaints to the supervisory authority.

3. Review your privacy notices

Transparency is one of the key principles of UK GDPR, and the primary way in which organisations comply with the principle is to communicate data processing activity to individuals via published privacy notices. Privacy notices should be regularly reviewed and updated to ensure they remain accurate and up to date.

4. Train your employees

Regular data protection training and awareness throughout the employee lifecycle, is a key control to ensure that employees know how to identify a data breach or a subject access request, who to escalate these queries to internally and the timescales for escalation (to enable your organisation to meet reporting deadlines).

5. Review retention and deletion arrangements

The more personal data an organisation retains, the more it has to lose in the event of a cyber-attack (resulting in a data breach). One of the key principles of data protection compliance is to retain personal data only for as long as required, and the only way to achieve this, is by defining and operationalising data retention periods. Whilst it is recognised that there are valid justifications to retain data for extended periods of time, life sciences organisations should balance retention requirements against an increased exposure, in the event of a data breach.

Summary

Regularly reviewing your data protection compliance maturity can deliver significant benefits, by enhancing trust and reputation (with key stakeholders), reducing the risk of fines and reprimands, gaining a competitive advantage and promoting data management and operational efficiency.

Whilst these five key steps do not comprise an exhaustive list of how organisations can meet data protection compliance requirements, they serve as a useful starting point on your road to embedding compliance into 'business as usual.'

Why BDO?

How your organisation operates and uses personal data are the starting points for how we work with you. We invest the time to understand your organisation, the multiple purposes for processing personal data as well as how data is managed throughout your organisation.

You will benefit from our wide-ranging data protection expertise, built on extensive experience across governance, operations, technology, compliance, and risk management. Our deep sector knowledge of Life Sciences and Healthcare organisations enables us to effectively support you in addressing your immediate data protection challenges.

Contact us

For further support regarding your organisation's data protection compliance, please feel free to contact:

Louise Sadler
Associate Director, Privacy & Data Protection, BDO LLP

louise.sadler@bdo.co.uk

www.bdo.co.uk