STEVENS&BOLTON

DATA PROTECTION AND THE GDPR – ITS IMPACT ON LIFE SCIENCES AND MEDICAL DEVICE BUSINESSES

As 25 May 2018 approaches businesses in the Life Sciences sector should be preparing for the new General Data Protection Regulation ("GDPR") which builds on the UK Data Protection Act 1998 and invokes data protection best practice. The GDPR brings new concepts and most organisations will need to examine (and tighten) their procedures. Compliance is mandatory!

For Life Sciences organisations the challenge will be understanding how the requirements impact on them, and implementing policies and procedures to demonstrate compliance. We've touched on a few of the key areas below and provided a helpful list to assess your state of readiness. These issues are particularly important in the areas of:

- Customers
- Employees
- Clinical trials
- Pharmacovigilance
- Lifestyle apps
- Medical devices
- Medical research
- Collecting health data for HCPs

Data controllers and processors - Clinical Trials

One of the biggest changes of the GDPR is that it will apply to both data controllers (i.e. the person/business who determines the purposes for and the way in which personal data is processed) and to data processors (i.e. anyone who processes personal data on behalf of the data controller). Historically, data processors were generally not directly impacted by the data protection regimes. Article 28 of the GDPR sets out the mandatory requirements to be set out in the data processing clauses and hence the proliferation of the data processing addenda that are being sent out. The clauses must include provisions such as audit rights, assisting with data subject rights, restricting the appointment of sub processors and ensuring the security and integrity of the personal data as well as imposing obligations on employees to maintain the confidentiality of the personal data. In addition, if there is a joint data controller, the parties have joint and several liability for compensation claims from data subjects. This is relevant, for example, when ascertaining in a clinical trial the position of the sponsor, investigator or the contract research organisation and associated supply chain providers.

Pseudonymisation and patient identifiers

In simple terms, principles such as 'data minimisation' and 'storage limitation' mean that we should not process more personal data than is required – the volume of data collected must be justified and processes put in place to identify and deal with old data (perhaps by deleting, pseudonymising or anonymising it). Under the new accountability principle, businesses will need to demonstrate how they apply these principles and should therefore consider their data use and implement retention policies. Of particular interest is that in clinical trials the use of codifiers and identifiers where the key is still available would still constitute personal data rather than anonymised data and so would be within the ambit of the GDPR.

Privacy Notices – pharmacovigilance and trials

Revised privacy notices for (i) employees, (ii) recruitment, (iii) websites, (iv) participants at trials, or (v) in dealing with pharmacovigilance, or (vi) medical apps will be required. There is also a new requirement to tell individuals such as trial participants, pharmacovigilance reportees, customers, suppliers and employees the legal grounds on which you are processing their personal data, how long you will hold it, what your retention criteria are, and what their new and improved data protection rights are.

Special data, biometric, genetic and health data

The GDPR requires that stricter requirements under both Article 6 and Article 9 grounds of the GDPR are fulfilled for the processing of special personal data. Special data is wider and as well as including sexual orientation, mental health and health data it now includes concepts of biometric data and genetic data. Health data is also specifically defined in the GDPR. The rules on consent and explicit consent in the case of special data have been revisited and strengthened.

Right to be forgotten and individual's rights to data portability

Another consideration is how the business will deal with data subjects' rights post-GDPR. There can be not only wider and enhanced subject access requests from, for example, contacts and employees, but also new erasure requests ('right to be forgotten') and requests for personal data in a form which can be transferred to a new provider (so called 'data portability'). It will not be acceptable to say the IT system does not have the required functionality to sort, delete or port data. Processes should be put in place now to ensure requests are escalated and dealt with appropriately within the necessary timescales.

Data Protection Officers

It will become mandatory in certain circumstances to appoint a Data Protection Officer (DPO) or to demonstrate accountability. Organisations may well choose to appoint one on a voluntary basis. The DPO will receive protected employment rights and rights to training but must be cognisant of data protection laws and the business processes.

Mandatory Privacy Impact Assessments (PIA)

For "high risk" processing, mandatory privacy impact assessments will be required and if undertaking medical research or high volumes of health or special data or using CCTV or monitoring employees you may well be expected to carry out a PIA.

Mandatory records of processing and breach records

The GDPR will bring in obligations to create and hold mandatory records of processing and to hold mandatory records of personal data breaches (which is widely defined). This is in addition to the obligation to report breaches to the new supervisory body immediately or at least within 72 hours. The supervisory authority has rights of audit and to see records.

Fines and compensation

Higher monetary penalties and fines (up to 4% of global turnover or Euros 20 million, whichever is greater) as well as increased compensation regimes means there is no room for complacency.

Conclusion

Once your documents and policies are in place you need to disseminate them appropriately to staff with appropriate training, especially for those employees who collect and use personal data.

ROUND UP

The following may help you assess your GDPR state of readiness. Have you:

- Undertaken a data gathering exercise and audited your personal data?
- Established legal grounds for processing and revisited consents?
- Appointed a DPO?
- Considered if a data sharing agreement is required? Ensured your IT systems can meet the new requirements?
- Undertaken privacy impact assessments where required?
- Complied with the new principles and implemented privacy by design, etc, in your organisation?
- Created both mandatory processing and breach records?
- Revised human resources documentation and created/updated internal policies/procedures?
- Created privacy notices for each area of the business?
- Prepared for new data subject rights (i.e. data portability and the right to be forgotten) and for enhanced data subject requests?
- Put in place mandatory contractual clauses between controllers and processors?

FIND OUT MORE

For more assistance please visit our website and read our briefing notes on the GDPR at https://www.stevens-bolton.com/site/what-we-do/business/data-protection/ or contact our Head of Data Protection, **Beverley Flynn**

BEVERLEY FLYNN
Partner, Head of Data Protection
+44 (0)1483 734264
beverley.flynn@stevens-bolton.com

Tel: 01483 302264
Fax: 01483 302254
www.stevens-bolton.com