HealthManagement.org
Promoting Management and Leadership

GDPR - better and stronger safeguards for personal data

John Deverell CBE
******@***deverellassociates.com

Deverell Associates – The
Prepared Mind, UK

LinkedIn

The General Data Protection Regulation (GDPR) provides better and stronger safeguards for personal data. It will protect all EU citizens and their data. GDPR was implemented in April 2016 and will be enforced in all EU Member States by the end of May 2018. Fines for failure to comply can be as high as €20 million or 4 percent of global turnover.

GDPR will apply to companies processing personal data in the EU, companies offering goods or services to EU residents and companies that monitor the behaviour of EU residents. It is not dependent on the location of the business in question. As a result, people should feel more confident that their personal data is secure.

GDPR stipulates that the data ‘controller’ (senior management of the firm) and the data ‘processor’ (the department or employee working with the data) have equal accountability. It specifies (Article 5(2))) an “accountability principle”. This means that senior managers are required to demonstrate compliance with GDPR and to state their responsibilities for doing so.

GDPR outlines seven obligatory requirements for the purpose of safeguarding the security interests of EU citizens:

- Consent: consent for their personal data to be held must be clearly given by the citizen and must be able to be withdrawn easily;
- Breach Notification: if a security breach is found, the data 'controllers' must notify those whose security has been jeopardised;
- Right to Access: individuals are ensured the right to access their data when they wish;
- Right to be Forgotten: individuals are ensured the right to have their data 'forgotten' or deleted when they choose;
- Data Portability: individuals can 'port' or move data given to one service provider to another provider;
- Privacy by Design: systems within the business must be built with security and information privacy in mind from the beginning, creating systemic safeguards to individual data;
- Data Protection Officers: large businesses (>250 employees) and public institutions must now employ qualified officers to help secure large scale data monitoring.

GDPR is somewhat different to existing requirements for personal data protection in the United Kingdom. In essence, it takes the requirements laid out in the 1998 Data Protection Act and by the Information Commissioner's Office (ICO) somewhat further. In comparison to the Data Protection Act - which it will replace - the GDPR is specific about such aspects as the "right to be forgotten", the principle of consent, the appointment of data protection officers and the necessity to report breaches.

As for the Information Commissioner's Office, the GDPR reinforces the good practice championed by the ICO. Such practice includes privacy impact assessments and "Privacy by Design". The difference is that the GDPR imposes a legally binding obligation in certain circumstances. The GDPR also makes it clear that businesses are expected to put in place comprehensive but proportionate governance measures.

The GDPR continues the trend of the last few years in making senior managers specifically accountable. In the United Kingdom, the Corporate Manslaughter Act, the Bribery Act, the Modern Slavery Act, the Senior Managers' Regime (for the financial sector) and now the GDPR place accountability on senior managers in ways previously not specified. Gone are the days when managers could legitimately defend themselves by simply and plausibly claiming that they were ignorant of their employees' wrongdoings. Senior managers are now specifically accountable for putting in place the procedures, resources and training to reduce the likelihood of a widening range of adverse events – and for demonstrating that they have done so. While this requires more effort and probably more expenditure on their part, it will – assuming that managers fulfil their responsibilities – increase public and shareholder confidence in business and in the intention to handle risk more effectively.

Source: Deverell Associates

Published on : Fri, 30 Mar 2018