General Data Protection Regulation:

Working towards compliance

The General Data Protection Regulation ('GDPR', 'Regulation') comes into effect on 25th May 2018

GDPR is the new EU data protection legislation which will replace the current Data Protection Directive, and the Data Protection Act 1998 ('DPA') in the UK.

The UK Government has confirmed that 'Brexit' will not affect the implementation of the GDPR in the UK. Are you on track to be compliant?

Some key areas where GDPR strengthens previous legislation.

1. **Significantly increased fines** – GDPR significantly increases organisations' risk exposure by imposing far tougher financial sanctions for breach of the Regulation. The most serious breaches of the GDPR could result in fines of up to €20million or 4% of the organisation's total worldwide annual turnover in the preceding financial year (whichever is greater). While GDPR is not just about financial penalties, such fines should make its implementation a board-level issue.
2. **Data breach notification**
   - Controllers are required to notify the appropriate supervisory authority (in the UK this will be the Information Commissioner's Office) of data breaches without undue delay and within 72 hours (if feasible) of learning about the breach, unless the breach is unlikely to result in risk to the rights and freedoms of individuals. Controllers are also required to notify the data subject of the breach without undue delay if the breach is likely to result in a high risk to the rights and freedoms of individuals.
   - Processors are required to notify the Controller of a data breach 'without undue delay'.
3. **Data protection officers ('DPO')** – Any controller or processor that is (i) a public authority or body (except for courts acting in their judicial capacity), (ii) whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale, or processing on a large scale of 'special categories' of data and personal data relating to criminal convictions and offences, will need to appoint a DPO.
4. **Greater rights for data subjects** – The new and enhanced rights afforded to individuals under the GDPR include the 'right to erasure' or 'to be forgotten', the right 'to restrict processing', the right 'to data portability', the right 'to object and automated individual decision-making' and enhanced data subject access requests rights. The broader rights available to a data subject means organisations are likely to receive a wider range of data subject access requests.

LOCKTON®

Broking done differently

Below are some key points to consider when planning for GDPR compliance:

1. **Board-level buy-in** - Key decision makers and executives need to be made aware of the new Regulation and its potential impact. Organisations should determine and document whether it is mandatory for them to designate a data protection officer, and also consider conducting Data Protection Impact Assessments ('DPIA'). This may help you to identify any GDPR concerns early – potentially reducing costs and reputational damage.
2. **Information analysis** – Organisations should conduct an information audit to establish what personal data it holds, what it is used for, where it came from, who it is shared with, and how it is stored and transferred. Once the types of data held and processes are established, the legal basis for carrying out data processing should be reviewed and documented.
3. **Individual's rights** – Organisations should check their policies and procedures to ensure that all individuals' rights are covered – such as 'right to be forgotten' and 'right to erasure' – and that individuals' data can be provided to them in a commonly used format.
4. **Communication and data breaches** – Organisations should review and update privacy policies, procedures and documentation – data protection authorities can ask for these at any time. Data breach detection, reporting and investigation should also be planned for and thoroughly tested, with robust incident management processes in place.

Many organisations still have a lot of work to do, and an ever-decreasing timeframe to complete it in time for the commencement of the GDPR.

The Regulation will make data processes and protection even more of a board-level issue, with high penalties for those who fail to prepare and comply.

If you have any queries or would like more information on Lockton's Cyber Insurance products do not hesitate to contact your Lockton account servicing team or a member of the Lockton Global Cyber and Technology team.

Liam Brown – Associate
+44 0 (20) 7933 2719
+44 (0) 7979 414 655
liam.brown@uk.lockton.com

Brett Warburton Smith – Partner
+44 0 (20) 7933 2242
+44 (0) 7768 917 550
brett.warburton-smith@uk.lockton.com
