Overview

The General Data Protection Regulation ('GDPR') takes effect from 25 May 2018, expanding the scope of the current Data Protection Act and creating a new material penalty risk for firms deemed to be non-compliant.

The Information Commissioner's Office ('ICO') will remain the Data Protection Authority for the UK; however the GDPR sets a punitive standard regarding fines for non-compliance (up to the higher of 4% of global turnover or EUR 20 million).

In practical terms, there are a number of steps that firms can take to ensure a smooth transition to GDPR compliance.

Step 1: Changes for current registered data controllers

The majority of FCA authorized firms will be registered as data controllers with the ICO at present due to their need to process personal information relating to staff and investors. As such, senior management and staff who process such personal information must be aware of some key changes to the UK data protection regime, which are summarised here.

Increased liability for data processors

Data processors (i.e. the individuals who process personal information on behalf of the firm) will need to keep written records of how and why personal information is processed and stored and to undertake to ensure that potential breaches of the GDPR are immediately reported. This does not remove any obligations from the firm as data controller; however, it does introduce a stricter focus on the activities of those processing data.

Expansion of definition of 'personal information'

The GDPR expands the definition of 'personal information' to include identifiable information such as an individual's IP address. It is therefore recommended that firms review their internal or third party IT suppliers to ensure compliance with the new regime.

Step 2: Procedure updates and essential training

Subject Access Requests

Subject Access Requests must now be answered within one month of receipt. Additionally, the £10 administrative charge which can currently be levied on such requests under the existing Data Protection Act will not be allowed. Therefore unless requests are repetitive or highly onerous, they must be handled free of charge.

Breach notification procedures

A data controller must notify the ICO within 72 hours of any breaches that are likely to impact the 'rights and freedoms' of the individuals who are the 'data subjects'. Furthermore, in material cases where there is a high risk to the rights and freedoms of the data subject, the individual must be

notified directly by the firm. The firm's compliance manual, or other relevant policies and procedures must be updated to reflect this new requirement and staff must be suitably trained.

For those requiring online training to aid in transition preparations, please visit www.tailoredcompliance.co.uk

Step 3: Contractual updates and ongoing monitoring

International data transfer

All firms must ensure that there are suitable equivalent protections in place in the recipient country and that explicit consent by the data subject has been obtained before sending personal information outside of the EU. This may be an issue for both staff and investor/prospect related data. Firms should consider updating the wording for contractual agreements to include explicit consent for data to be sent outside of the EU if required to fulfill the contract.

Staff details

Staff details in scope include all payroll and HR information. It is therefore essential that such information is stored securely and has controlled access. Any external contracts regarding the processing of HR or payroll must be reviewed for compliance with the new regime. Internally, such information must be suitably restricted and only held for an appropriate length of time.

Investor/prospect details

Details of all prospective and actual individual investors will be in scope, including simple contact details through to investment objectives, history and meeting notes. It is therefore essential that the Client Relationship Management system ('CRM') is only accessed by staff members who require that information to fulfill their roles and is kept up to date and accurate at all times. Firms should consider including detailed recordkeeping reviews of the handling of personal data in their compliance monitoring programmes.

Please contact us to discuss your firm's next steps.

Regent's Compliance
info@regentscompliance.com
0203 710 0142
07795261311
www.regentscompliance.com