hot topICS
keeping you informed

29 May 2019

HT 2019 – 05

GDPR - One year on

It's over a year since the General Data Protection Regulation came into force on 25 May 2018. This article looks at what has happened since in terms of compliance and enforcement.

The much-publicised changes to Data Protection law and regulation provided rich fodder for legal and compliance experts across the UK, Europe and, to some extent, the rest of the globe. There were many complex aspects to the requirements and the penalties for non-compliance looked draconian.

Compliance with GDPR is a board level responsibility, and firms should be able to show the steps that they have taken to comply. Insurance intermediaries have set about putting the complexities of the GDPR into context, devising new privacy notices and subject access procedures, conducting data audits, training staff, adapting their marketing arrangements and reviewing their data retention policies.

Although it may appear to be largely 'business as usual', Data Protection is an on-going commitment and it is important to keep it high on the compliance agenda. Rather like Y2K (remember the millennium bug?) the potential for turmoil never materialised but, unlike Y2K, the effects of the GDPR are far reaching and here to stay, Brexit or no Brexit.

GDPR basics

The GDPR has provided new rights for people to access, rectify, erase and transport any personal information held about them. At the same time, controllers and processors of personal data are obliged to make sure personal information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

Perhaps most importantly, the 'accountability principle' means that firms must take full responsibility for what they do with personal data and how they comply with the other principles. The Data Protection Act 2018 has given extensive powers to enforce the requirements in the UK to the Information Commissioner's Office (ICO).

Enforcement under GDPR

The ICO can impose fines for data breaches of up to €20million or four percent of global turnover, whichever is greater. Failings in relation to consent, data subject rights, transfer of data, lack of security or any other breach can lead to repercussions that could seriously affect a firm's viability. But, so far, there have been few regulatory actions, based on GDPR.

A case against Equifax leading to a £500,000 fine in September 2018 was made under the DPA 1998, as the breach occurred before the GDPR/DPA 2018 came into force. Similarly a £500,000 fine against Facebook in October 2018 was enforced under former legislation. This related to Facebook's role in the Cambridge Analytica scandal.

The ICO issued its first GDPR enforcement notice to a Canadian data analytics company, AggregateIQ Data Services Ltd, in October 2018. The notice required the firm to "cease processing any personal data of UK or EU citizens obtained from UK political organisations or otherwise, for the purposes of data analytics, political campaigning or any other advertising purposes".

In November 2018 the ICO fined a number of organisations for non-payment of the data protection fee under the new DPA. The fee ranges from £40 and £2,900 and becomes due when a firm's existing registration expires.

A handful of GDPR enforcement actions have been taken by state regulators against organisations elsewhere in Europe but many more are to be expected as the new regime beds in and more incidents come to the attention of the regulators.

Probably more significant is the incidence of breaches under the Privacy in Electronic Communications Regulations (PECR) which sit alongside the GDPR/DPA – see below.

Whilst the ICO regulates data protection, compliance with the GDPR requirements is also something the FCA can take into account under its rules; for example, the requirement (in SYSC) to maintain appropriate technology and cyber resilience systems and controls. The FCA and ICO collaborate on relevant matters.

The Privacy and Electronic Communications Regulations (PECR)

The Privacy and Electronic Communications Regulations (PECR) work alongside the GDPR and DPA, giving specific privacy rights in relation to electronic communications, including specific rules on:

- marketing calls, emails, texts and faxes
- cookies (and similar technologies)
- keeping communications services secure

Some changes were made to PECR in January 2019 to cover changes made by the GDPR. Other changes have been made to ban cold-calling by claims management services, to introduce director liability for serious breaches of the marketing rules and to ban cold-calling on pensions schemes in certain circumstances.

The EU is in the process of replacing the e-privacy Directive with a new (potentially more onerous) e-privacy Regulation to sit alongside the GDPR but, for now, the PECR continues to apply in tandem with the GDPR and DPA 2018.

The PECR restrictions on marketing by email and SMS are particularly significant for insurance intermediaries. ICO guidance says; *"You must not send marketing emails or texts to individuals without specific consent. There is a limited exception for your own previous customers, often called the 'soft opt-in'. You can send marketing emails or texts to companies. However, it is good practice to keep a 'do not email or text' list of any companies that object."*

The soft opt-in means firms are not prevented from emailing or texting a customer who has bought (or discussed buying) a similar product or service from the firm – but only if they were given a clear chance to opt out of receiving marketing emails or texts when their details were collected and in every subsequent message.

Firms can still use bought-in lists to make live marketing telephone calls, but should screen against both the TPS and their own 'do-not-call' list of people who have previously objected to or opted out. Recorded calls, texts and emails can only be used for marketing if the people on the list specifically consent to receive that type of message from the firm - generic consent covering any third party is not enough. PECR also covers marketing using direct messaging via social media.

Online marketing presents a slightly different challenge, so ICO has produced a checklist to help smaller businesses that operate online to make sure they collect and use information about the people they deal with properly. This checklist applies to information such as customers' names and email addresses, or records of their purchases or enquiries. It also applies to information collected through the use of a 'cookie', for example where this is used to target marketing at people. [See 'Further Information' below for links to ICO guidance.]

Enforcement under PECR

It appears currently that firms are much more likely to fall foul of the electronic marketing regulations under PECR than the more general GDPR requirements.

In one case investigated in 2018 involving an insurance business, the ICO issued fines totalling £120,000. The action was taken against Leave.EU and Eldon Insurance trading as Go Skippy Insurance based on Regulation 22 of PECR. This prevents unsolicited emails unless the conditions for a soft opt-n are satisfied. The ICO investigation found that Leave.EU and Eldon Insurance were closely linked and that systems for segregating the personal data of insurance customers' from that of political subscribers' were ineffective. This resulted in Leave.EU using Eldon Insurance customers' details unlawfully to send almost 300,000 political marketing messages.

In December 2018 a London-based firm, Tax Returned Limited, was fined £200,000 by the ICO for sending out millions of unsolicited marketing text messages without valid consent through a third party service. Although some of the consents were received through generic consent forms, the regulator found that the wording was "not clear enough" and that Tax Returned was not always named in privacy notices.

In Jan 2019 Alistar Green Legal Services Limited based in Liverpool was fined £80,000 for making 213 nuisance calls to TPS subscribers. Numerous other cases involving PECR breaches are listed on the ICO website.

hot topICS
keeping you informed

Putting data protection into practice

The GDPR has prompted firms to take action to introduce, refine and update their internal processes and procedures regarding data protection. They should be able to show what measures they have put in place and why and what steps they have taken to protect the data they hold.

Starting with obvious steps such as password protection, access restriction and keeping anti-virus and firewall protection up-to-date, the security of IT systems is of paramount importance. On an even more basic level firms can implement security measures such as clear desk policies and strict record handling procedures. Personal information, including within renewal papers and new business records, may be left in paper form on desks or elsewhere unsecured in office. This presents a clear security risk and it would be difficult to identify and quantify any breach that occurred. Even worse, client records may be kept in employee's cars between visits or for more extended periods of time.

New threats continue to emerge with insurance firms holding substantial amounts of personal data, including some special category data and information about criminal convictions. The FCA is taking a specific interest in the cyber resilience in financial services firms, saying on its website: "*Firms of all sizes need to develop a 'security culture', from the board down to every employee. Firms should be able to identify and prioritise their information assets - hardware, software and people. They should protect these assets, detect breaches, respond to and recover from incidents, and constantly evolve to meet new threats.*"

Data audits

In order to implement the GDPR, most firms will have conducted an information audit to identify the data held, show how it was obtained and to map the flow of information into and out of the organisation. Amongst other things, this process assists firms to identify the lawful basis under which they can hold and process the data. It could also assist them to identify some of the risks to their data security and to recognise a breach.

The processing of personal information is necessary, in the case of arranging and administering insurance, to deliver a contractual service, so 'contract' is the lawful basis generally relied upon by insurance intermediaries. But, for the purposes of other activities, such as marketing, the firm would need to justify the use of a different lawful basis such as consent or legitimate interests.

The data audit process should be ongoing and the resultant information asset register kept up to date.

Documentation

In addition to the information asset register, policies and procedures should be documented to cover all the firm's data processing activities; for example, data security, staff responsibilities, IT systems, subject access arrangements, data retention policy etc. A record of the firm's terms of business with insurers and customers and of any data processor agreements should be maintained. A breach reporting record should also be kept along with details of any subject access requests and how they were satisfied. Such records, policies and procedures are vital to firms' compliance and governance.

When data is collected it may be helpful to categorise it based on, for example whether it is personal data or commercial, how the data is shared and/or processed and its intended retention period.

Firms should also keep a record of any consent obtained from data subjects (such as consent to marketing) and issue a privacy policy which gives data subjects the necessary information about how their data is used and states the firm's lawful basis for processing.

What do we need to do now?

Here are some steps firms could take as part of an on-going data protection strategy:

- Confirm your governance structure sets out clear roles and responsibilities for data protection
- Update your information assets register
- Ensure your legal bases for processing are still appropriate
- Keep a detailed record of all your data processing activities
- Review data protection policies and procedures
- Review and update Privacy Notices and ensure these are issued/made available as necessary
- Consider carrying out data protection impact assessments (DPIAs) for any high-risk processing operations
- Implement appropriate measures for data security, including measures against cybercrime
- Refresh staff awareness of data protection issues and ensure they receive appropriate training

Further information

ICO guidance on Direct Marketing: https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf
ICO Direct Marketing checklist: https://ico.org.uk/media/for-organisations/documents/2259802/direct-marketing-checklist.pdf
ICO guidance on using Marketing Lists: https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/using-marketing-lists/
ICO Personal information online small business checklist: https://ico.org.uk/media/for-organisations/documents/1586/personal_information_online_small_business_checklist.pdf
ICO Data Protection Impact Assessments: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

If you would like any help or information on any FCA or related regulation issues, ICS Services, e-learning or anything else we might be able to assist you with, please contact your usual ICS representative, Head Office on 01892 539600 or admin@insurancecompliance.co.uk