Mind the GDPR (Pt 4)

In the fourth of this special series on the GDPR, Rollits LLP turns the spotlight on the changes & challenges that still lie ahead as the Regulation rolls out

IN BRIEF

- As the GDPR comes into force, organisations must ensure compliance as a matter of urgency, with a number of steps they should be considering on an ongoing basis.
- There are a range of enforcement actions available to the ICO when it suspects a breach.

After months of ever increasing media coverage, the General Data Protection Regulation (GDPR) has arrived and with it we say a fond farewell to the Data Protection Act 1998 (DPA)—although its flame still burns brightly within the GDPR.

Organisations now have increased statutory obligations with regard to the way in which they can collect, hold, use, store, retain, delete or in any way process personal data, and the potential consequences for getting it wrong have been amplified significantly.

In previous instalments in this series on the GDPR we have provided an overview of the key provisions of the legislation, analysed issues regarding the appointment of a Data Protection Officer, considered how to obtain valid consent, looked at the importance of data processing agreements, and outlined the impact of the GDPR on processors (see Pt 1, 167 *NLJ* 7762, p8; Pt 2, 167 *NLJ* 7774, p11; & Pt 3, *NLJ* 13 April 2018, p12).

With the GDPR now in force, our focus turns to immediate actions that organisations should consider taking and look at how the GDPR is enforced.

Immediate actions to consider

Many organisations have, over recent months, been creating the building blocks necessary to try to ensure compliance with the GDPR from the date it takes effect (ie 25 May 2018). Now that the GDPR is in force, that work does not stop and organisations should continue to identify and address data protection risks in their business practices. Organisations that have buried their heads in the sand over the last year and ignored warnings about the changes are likely to receive little sympathy from the Information Commissioner's Office (ICO) in the event that they suffer a data breach or receive a complaint.

Irrespective of the steps taken to date, the following points should be considered on an ongoing basis by all organisations which handle personal data:

- All staff who deal with personal data should be made aware that the law has changed and receive appropriate training. Data breaches often result from lack of appropriate training and staff can be the organisation's greatest potential weakness. Conversely, if staff are appropriately trained and have a strong understanding of what they can and cannot do with personal data they could be the organisation's best defence against a breach.
- Appropriate accountability measures should be put in place and should be tested and reviewed to ensure that staff are aware of them and that they work for the organisation. For example, if a Data Protection Officer has been appointed, do staff know who that is? Are the security measures adopted practical for the organisation or do they unnecessarily restrict working practices such that staff try to use workaround solutions which may not be compliant? Have appropriate policies been provided to staff on data protection and have they been read and considered (or are they sat in a draw or hidden within a staff handbook)?
- Data protection has to be considered at board level on an ongoing basis. There needs to be a culture of transparency and accountability as to how personal data is processed from the outset, rather than it be a matter considered further down the line once it becomes difficult to consider and address any potential issues.
- Organisations should continually review and update records documenting what personal data they hold, where it came from and with whom it is shared. Records produced pursuant to a data protection audit in preparation for the GDPR will quickly become outdated if there is not an appropriate procedure in place for reviewing them. Organisations that have not carried out an audit and recorded the personal data they hold would be well advised to do so as a matter of urgency.
- Any third-party arrangements entered into by an organisation should be reviewed to ascertain whether any

personal data are shared pursuant to the arrangement. While many organisations have been proactive in reviewing the circumstances in which they share personal data with third parties and have sought to enter into appropriate agreements with those third parties, there may still be arrangements in place which are not GDPR-compliant—or new arrangements may have been entered into since the last audit. Organisations should continue to take steps to update those arrangements as appropriate (or consider alternative arrangements where necessary).

- Organisations should continually review what security (both physical and electronic) is in place in respect of personal data. IT systems can quickly become outdated and leave the organisation vulnerable if they are not monitored and updated on a regular basis.
- Certain fair processing information has to be provided by the organisation to data subjects at the point at which the data are collected. This may prove problematic for organisations in some scenarios—for example, when personal data are collected over the telephone or in person or when personal data are collected in a business to business context. The exemptions in respect of this are very limited and will not apply to the majority of activities carried out by organisations. There is also limited guidance from the ICO on how, practically, organisations are expected to comply with this requirement. Nonetheless, organisations should review how the fair processing information is made available to data subjects and ensure that steps are taken to provide the information at the point of collection of the personal data, or at the very least that steps are taken to advise the data subject as to where that information can be located (which should be somewhere that is easily accessible).
- Prior to the GDPR taking effect organisations should have reviewed what consent mechanisms they have in place and updated them as appropriate to ensure that they are GDPR-compliant. Where consent is used as the lawful basis for sending direct marketing (which, in many cases, is the only lawful basis that organisations can rely upon for sending direct marketing), organisations should only send direct marketing to those data subjects in respect of whom it is possible to verify that GDPR-compliant consent has been provided. If it is not possible to verify the consent provided, or if the consent provided is not GDPR-compliant, the data subject should be removed from the marketing database.

Enforcement

Enforcement of the GDPR in the UK is predominantly the responsibility of the ICO, which has a wide range of powers at its disposal. Typically, when a potential data breach has been reported to the ICO (whether by an affected individual, the organisation itself or pursuant to an investigation carried out by ICO) the ICO will undertake an investigation into the matter. If, pursuant to the investigation, the ICO believes that there may have been a breach there are a range of actions the ICO may take, some of which are considered below.

> *"Much media attention regarding the GDPR has focused on the ICO's increased fining powers"*

Information Notice

If the ICO requires additional information in relation to the matter they may issue an Information Notice to the organisation which requires the organisation to provide the additional information within a set timeframe.

If served with an Information Notice, the organisation should promptly carry out an internal audit to establish whether it believes there has been a breach and (if there has been) take appropriate remedial action in order that such action can be outlined in the response to the ICO when providing the required information.

Enforcement Notice

If the ICO is satisfied that there has been a breach, the ICO may serve an Enforcement Notice on the organisation which specifies the steps that should be taken by the organisation to remedy the breach. The Enforcement Notice could also require the organisation to refrain from processing personal data for a specific purpose (for example, it could require the organisation to cease marketing individuals on a particular database if the ICO is satisfied that the organisation does not have a lawful basis for doing so).

Monetary Penalty Notice

The maximum amount which the ICO could fine an organisation for breach of the DPA was £500,000. The ICO's fining powers have now increased substantially. Under the GDPR, the level of fine which can be imposed by the ICO will depend on the nature of the breach. For those offences that are considered more minor, the maximum level of fine that can be imposed on the controller or processor is 2% of the organisation's total annual worldwide turnover or €10m—whichever is higher. For the offences that are considered more serious, the maximum level of fine is double that (ie 4% of the organisation's total annual worldwide turnover or €20m—whichever is higher).

One common misconception is that the money paid by organisations pursuant to the fines issued by the ICO is retained by the ICO. While the ICO would probably welcome that, the money raised through fines is actually held centrally by the government.

Much media attention regarding the GDPR has focused on the ICO's increased fining powers. The Information Commissioner has described this focus as being 'scaremongering' and has commented that the ICO's role is first and foremost to guide, advise and educate organisations about how to comply with the law. It is worth noting that the highest fine issued by the ICO to date is £400,000 (to both TalkTalk and Carphone Warehouse) and so the ICO has determined that no breach has—to date—warranted the maximum fine that could be imposed. Nevertheless, the ICO does have increased fining powers at its disposal and we will have to wait and see the extent to which they are used.

Overview

Achieving compliance with the GDPR is undeniably a challenge for organisations, but it should be seen as a permanent culture change rather than a job which can be completed then forgotten about. Never before has data protection been so high-profile with the result that issues are now being raised more widely than ever.

The ICO has been working hard to produce guidance, but it only goes so far and cannot address specific queries. We are likely to see much more information being released over the coming weeks and months; in the meantime, organisations should continue to foster a positive data protection culture and use GDPR as an opportunity to help improve their processes with the positive benefits that will bring in terms of efficiency, professionalism, reputation and innovation. NLJ

David White, senior solicitor & **Tom Morrison,** partner, Rollits LLP (*www.rollits.com*).