Seven key data protection New Year's Resolutions companies should be making

Ann Bevitt, Partner, and Amy Collins, Associate, Cooley (UK) LLP, explain what ought to be top of the agenda for organisations at the start of 2016

With the landmark rulings of the Court of Justice of the European Union ('CJEU') on the 'right to be forgotten' and invalidating the US-EU Safe Harbor scheme in 2015, and the adoption of the General Data Protection Regulation ('GDPR') expected in early 2016, the focus on data protection in the EU has never been greater.

Whilst the UK regulator, the Information Commissioner's Office ('ICO'), has emphasised in respect of the GDPR that 'the best preparation for an organisation is to comply with the current law', the privacy landscape in the EU is clearly changing rapidly and bringing with it challenges that organisations should seek to address sooner rather than later.

So what data protection New Year's resolutions should organisations be making both to ensure their current compliance but also to prepare themselves for the changes which the GDPR will bring?

1. Keep track of personal data being processed

Organisations should ensure that they are keeping track of the personal data they are processing and that those data are appropriately protected. One way that this may be achieved is by requiring customer-facing parts of the business and HR to complete and regularly review and update responses to a standard form data protection questionnaire. Group legal and data protection and compliance functions should be kept up-to-date on changes to the types of data processed and the purposes for which they are processed so that they can advise on any ramifications or compliance issues (including, for example, updates to privacy policies and other customer agreements).

Broadly speaking, the GDPR maintains the distinction between personal data (being information which identifies an individual or from which it is reasonably likely that an individual could be identified) and anonymised data, which falls outside its scope. The GDPR also introduces a new category of 'pseudonymous data' and expressly encourages 'pseudonymisation' whereby data are processed in such a way that they can no longer be attributed to a data subject without the use of additional information, provided such information is kept separately and subject to technical and organisational measures to ensure non-attribution of such data. Although pseudonymous data are still a form of personal data, organisations should consider how pseudonymisation may help them unlock the utility of the data they process whilst protecting the privacy of individuals. By way of example, when looking at purpose limitation under the GDPR, where data have been obtained for one purpose and a company wants to use such data for another, one of the factors to be taken into account when assessing whether the new purpose is compatible is whether the data have been pseudonymised.

2. Monitor data flows

Organisations should keep track of data flows and ensure that transfers of personal data overseas and in particular outside of the EU are monitored and managed appropriately. In the absence of an adequacy decision by the European Commission, organisations must ensure that they compensate for the lack of data protection in a country outside the EU by way of appropriate safeguards. In the wake of the CJEU decision invalidating the US-EU Safe Harbor scheme in 2015, organisations should ensure in particular that standard contractual clauses or alternatives are in place to legitimise transfers of personal data to the United States where necessary.

Standard contractual clauses, along with Binding Corporate Rules and contractual clauses authorised by a supervisory authority on an ad hoc basis, are still considered adequate safeguards under the GDPR.

It is also worth bearing in mind that the GDPR will apply to non-EU established organisations in the context of their activities in the EU, regardless of whether the processing itself takes place in the EU. Non-EU established organisations will be subject to the GDPR where the processing activities are related to (i) the offering of goods or services in the EU and/or (ii) the monitoring of the behaviour of data subjects in the EU. The

(Continued on page 14)

(Continued from page 13)

determination as to whether a company is offering goods or services in the EU will be based on a number of factors (including, for example, the mentioning of customers or users in the EU in materials, and the use of a language or ability to place orders in a currency used in a Member State which is not the language or currency of the country in which the company is established).

The GDPR expressly states that the mere accessibility of a company's website in the EU is insufficient to bring it under the Regulation's scope. A company will be considered to be monitoring the behaviour of data subjects in the EU where such individuals are tracked on the internet, particularly in order to take decisions concerning that data subject or for analysing or predicting the data subject's personal preferences, behaviours and attitudes.

Non-EU established organisations should therefore consider whether their activities are likely to fall into either of these categories, and whether they will therefore be subject to the new legislation when it comes into force.

> ***"Companies should test their data breach responses before they need to be invoked in a real life scenario and these should include a breach notification process and internal incident management process."***

3. Flow down contractual obligations

Organisations should ensure that contractual obligations imposed on them with respect to data provided by third parties are passed down as necessary to their employees and subcontractors. Organisations should also ensure that their arrangements with third parties to whom they provide personal data adequately protect data subjects' rights, and that they exercise audit and other rights granted to them under such arrangements where appropriate.

Under the GDPR, data controllers must ensure that their data processors provide sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of the Regulation, and to ensure the protection of the rights of the data subject. The GDPR also increases the accountability of data processors, including, for example, by requiring them to allow for and contribute to audits and inspections conducted by controllers. Processors are also prohibited from enlisting sub-processors without the prior written consent of controllers, and they must inform controllers of any intended changes concerning the addition or replacement of processors, thereby giving controllers the opportunity to object to such changes.

These changes will undoubtedly help SMEs in the negotiation of 'non-negotiable' and 'standard form' agreements, and put pressure on larger service providers (particularly in the cloud space).

From a compliance perspective, meeting some of these requirements may be challenging. Organisations should review their agreements and ensure that any amendments are made prior to the coming into force of the GDPR.

4. Train your workforce

Organisations should ensure that their employees are given appropriate training to ensure compliance with existing data protection legislation and are made aware of the requirements of the GDPR before they come into force.

It is now anticipated that the GDPR will be formally published in the official journal of the EU in the first quarter of 2016 and it will come into force two years from its publication date. Organisations should use this two year period to ensure that they and their employees are well prepared.

Although strictly speaking, organisations need not make any changes to comply with the new legislation before it comes into force, practically to be in a position to comply then, they will need to start taking steps now or very shortly. It is also likely that the text of the GDPR will influence how data protection authorities approach compliance between now and then. For example, although the existing legislation doesn't require organisations to complete impact assessments, we are already seeing authorities, including the ICO, recommend that such assessments be carried out.

The GDPR requires organisations to designate a Data Protection Officer in certain circumstances, including where its core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale. Where necessary, organisations should consider designating (or where appropriate, engaging) a designated officer to assist with the training of its workforce before the coming into force of the GDPR. It may be appropriate for key individuals to obtain a suitable data protection qualification.

5. Obtain consents where required

Organisations should review their existing consents to ensure that they are obtaining data subject consent to the processing of personal data as necessary. This should include consents to direct marketing and cookies where applicable.

The GDPR tightens the requirements for consent and states expressly that consent should be given by a clear affirmative action establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing. Consent to the processing of sensitive personal data must also be explicit.

Although the consent requirements are seemingly onerous, the GDPR confirms that consent to the processing of personal data can still be obtained by ticking a box when visiting a website, choosing certain technical settings or by other statements or conduct which clearly indicate acceptance of the processing. Silence, pre-ticked boxes or inactivity will not, however, constitute consent.

The GDPR has also clarified that consent will be presumed not to be 'freely given' in certain circumstances, including where it has been bundled and cannot be given separately to different data processing operations.

One of the most controversial provisions of the GDPR requires that parental consent must be obtained in respect of the processing of personal data of children below the age of 16 or, if provided for by the law of a Member State, a lower age of no less than 13. These provisions are specific to the offering of information society services, so to the extent that the processing is in respect of offline activities, the rules of each Member State will apply.

6. Update social media policies

Organisations should ensure that their social media policies are reviewed regularly and updated as necessary to ensure they reflect reality. They should consider, for example, whether the types of data stated to be collected, purpose limitations and circumstances in which data may be disclosed to third parties, as well as the identity of those parties, are correct.

Policies and processes should ensure that the 'right to be forgotten' and 'right to erasure' are respected and actioned within the organisation where appropriate.

Organisations should also consider to what extent changes may be required to reflect the new requirements of the GDPR when they come into force, including, for example, in respect of the processing of personal data of children, as well as how consent to any updated social media policy should be obtained.

7. Implement and update data security and data breach policies

Data security and data breach policies should be implemented and organisations should provide training to employees to ensure they are aware of the content of such policies. These should be regularly updated to ensure they reflect any technological changes. Organisations should test their data breach responses before they need to be invoked in a real life scenario and these should include a breach notification process and internal incident management process.

Under the GDPR, data controllers will be required to notify breaches to the competent supervisory authority as soon as they become aware of the same and, where feasible, not later than 72 hours after having become aware, unless they are able to demonstrate that the breach in question is unlikely to result in a risk to the rights and freedoms of individuals. The data subjects concerned must also be notified without undue delay if the breach is likely to result in a high risk to the rights and freedoms of individuals.

Data controllers must keep a log of breaches to allow the supervisory authority to verify compliance with the notification requirements of the GDPR. Organisations will need to build these requirements into their data breach policies and procedures and should test them before the GDPR comes into force.

The GDPR sets a maximum level of fine for breaches of EUR 20 million or 4% of total worldwide annual turnover and the consequences of breaches therefore present a significant risk to businesses. Organisations should consider to what extent their contractual arrangements limit or exclude losses for breaches of data protection legislation and whether their approach to these issues needs to be revised going forward. They should also consider whether they require cyber-insurance, or, if they already have cyber-insurance, whether the level of the cover provided is adequate in light of these changes.

Conclusion

Whilst the GDPR will not come into force until 2018 at the earliest, organisations should not underestimate the extent of the changes it will bring and the effort required to prepare for its implementation. That said, the UK regulator has stated that its priority for 2016 is 'making sure that we do all in our power to ease the introduction of the new rules', and we can therefore expect much advice and guidance over the course of the next two years.

Ann Bevitt and Amy Collins
Cooley (UK) LLP
abevitt@cooley.com
acollins@cooley.com