Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 16, NUMBER 4 >>> APRIL 2016

The U.K. Data Protection Dozen—ICO Publishes 12 Step Checklist to Prepare for GDPR

By Shannon K. Yavorsky and Emma L. Flett

In preparation for the overhaul of the longstanding European data protection regime, the U.K. Information Commissioner's Office (ICO) published on March 14, a 12 step checklist to assist companies in preparing for the implementation of the General Data Protection Regulation (GDPR). The GDPR, which strengthens and harmonizes existing European data protection legislation, is expected to come into force in early 2018. The ICO's guidance is a checklist which sets out 12 key steps that organizations can start to take now to ensure that they are in compliance when the new legislation comes into force.

Shannon K. Yavorsky is an intellectual property partner in Kirkland & Ellis LLP in San Francisco. She can be reached at syavorsky@kirkland.com.

Emma L. Flett is an IP partner in Kirkland & Ellis International LLP in London. She can be reached at emma.flett@kirkland.com.

The ICO points out that the GDPR's main concepts and principles are fundamentally similar to those in the current EU legislation (the Data Protection Directive 95/46/EC) so if organizations are complying with the existing law, then much of the existing compliance approach will remain valid under the new legislation. However, there are several new provisions and certain adjustments that organizations will have to make to ensure compliance with the new law. The ICO notes that it is important to start thinking about GDPR compliance early since, amongst other things, new procedures may need to be implemented with respect to the GDPR's new transparency and individuals' rights provisions—so it's important to get the ball rolling.

The Twelve Step Programme

Step 1: Awareness

The ICO states that it is imperative that decision-makers and key people within an organization are

aware that the GDPR is coming into force and understand the impact that the new law is likely to have on an organization. The ICO highlights that lead time is critical since implementation may be costly and time consuming, particularly for larger organizations.

Step 2: Information You Hold

The ICO recommends that organizations take stock of the personal information they hold to understand where it came from and how it is shared. If inaccurate personal data is shared with another organization, it is important to ensure that the other organization is advised accordingly so it can update its records; this cannot be done unless an organization knows what information it holds and with whom it is shared. If an organization documents the information it holds and knows who it is shared with, this will help with compliance with the GDPR's accountability provision.

Step 3: Communicating Privacy Information

An organization should review its current privacy notices and implement a plan for amending such notices in advance of the new law according to the ICO. The GDPR provides that additional information must be provided to individuals when their personal information is collected. For example, an organization now needs to explain the legal basis for processing personal data, the data retention periods and that individuals can complain to the ICO if there is an issue with the way in which an organization is processing the data. The ICO indicates that it is currently consulting on a new version of its Privacy Notices Code of Practice which will be published later in 2016.

Step 4: Individuals' Rights

The Information Commissioner's Office notes that organizations will have to explain the legal basis for processing personal data when responding to a subject access request.

A key feature of the new legislation is enhanced rights for data subjects. Accordingly, the ICO points out that organizations should review procedures to understand how personal information is currently deleted or provided to individuals and whether these processes need to be updated. The guidance sets out the key rights for individuals under the GDPR: (i) subject access; (ii) the right to have inaccuracies corrected; (iii) the right to have information erased; (iv) the right to prevent direct marketing; (v) the right to prevent automated decision making and profiling; and (vi) the right to data portability. An organization should consider how it would react if faced with, for example, a request to have data deleted. The right to data portability is new to the GDPR and requires organizations to provide data electronically and in a commonly used format.

Step 5: Subject Access Requests

As to subject access requests, the ICO provides that organizations should update procedures and plan how subject access requests will be handled within the new timeframes. Unlike the current legislation which allowed organizations to charge for subject access requests and had a timeframe of 40 days in which to respond to a request, the new legislation makes subject access requests mostly free and imposes shorter timeframes for organizations to comply with a request.

Step 6: Legal Basis for Processing Personal Data

Under the GDPR, certain individuals' rights will be modified depending on an organization's legal basis for processing their personal data. The ICO therefore recommends that an organization audit the types of data processing it carries out and the legal basis for doing so (i.e., consent to processing) and keep a record of the same. The ICO notes that organizations will have to explain the legal basis for processing personal data when responding to a subject access request.

The Information Commissioner's Office highlights that in large organizations, implementation could require significant budgetary, information technology, personnel governance and communications implications.

Step 7: Consent

The GDPR, like current data protection legislation, requires consent to data processing to be specific, informed and freely given. The ICO suggests that organizations audit how consent is sought, obtained and recorded and determine whether any changes to these processes may be required.

Step 8: Children

The GDPR introduces special protection for children's personal data. If an organization collects information about children, then a parent or guardian's consent will be required in order to process their personal data. The ICO recommends that organizations think about implementing systems to verify individuals' ages and how consent from a parent or guardian will be obtained and document this process.

Step 9: Data Breaches

The ICO provides that, because of the new requirements with respect to reporting data breaches under the GDPR, organizations should ensure that processes are in place to detect, report and investigate data breaches. Under the new rules, not all data breaches need be reported: only those relating to personal data which are likely to result in a risk to the rights and freedoms of individuals. The ICO notes that organizations should develop policies and procedures for managing data

   ISSN 1473-3579

breaches since failure to report a breach, where required to do so, could result in a fine.

Step 10: Data Protection by Design and Data Protection Impact Assessments

The ICO notes that it has always been good practice to adopt a privacy by design approach and to carry out an impact assessment but the GDPR makes this a legal requirement. However, the ICO notes that a privacy impact assessment is not always required except where there is a "high-risk" situation such as where a new technology is being deployed. The GDPR also requires organizations to consult the ICO to make a determination as to whether the high risk processing complies with the new law.

Step 11: Data Protection Officers

There is a requirement under the GDPR for certain organizations to appoint a data protection officer who will take responsibility for data protection compliance. The ICO recommends that organizations ensure that someone within the organization (or an external adviser) takes responsibility for data protection compliance and has the requisite knowledge and support to do so. Organizations should therefore audit who is currently responsible for data protection compliance, if anyone, and make any necessary changes.

Step 12: International

The GDPR includes new provisions with respect to which an entity within an organization should be primarily responsible when investigating a complaint with an international component. The ICO points out that the lead authority will be determined according to where an organization has its main administration or where decisions about data processing are made. In the event of uncertainty as to which entity should be the lead, the ICO suggests that an organization map where it makes the most important decisions about data processing to assist in determining which entity should be the lead authority.

Data Dozen

The requirements of the new law are detailed and many. However, there are over 18 months until the GDPR takes effect and organizations should use this time to audit their data protection practices in line with the ICO's guidance and make any necessary adjustments or changes. The ICO highlights that in large organizations, implementation could require significant budgetary, information technology, personnel governance and communications implications so getting ahead of any issues now to kick-start the process will ensure that an organization is ready when the new legislation kicks-in.

Further guidance can be expected from both the ICO and the Article 29 Working Party over the coming months. Until then, the data dozen from the ICO provides a good place to start. As well as developing internal procedures and systems that can cope with the logistical demands presented by the new rights and obligations introduced by the GDPR, businesses should be thinking carefully about reviewing arrangements with data processors and third parties with whom they share personal data to ensure that those arrangements are GDPR compliant where they extend beyond 2018.

Full text of the ICO's guidance is available at https://dpreformdotorgdotuk.files.wordpress.com/2016/03/preparing-for-the-gdpr-12-steps.pdf.