April 1, 2019

UK Data Protection Survey Reveals Mixed Compliance Progress

Attorneys
Rohan Massey
Edward Machin

The UK Information Commissioner's Office (ICO) is calling on UK data controllers and processors to be more accountable in the wake of the latest Global Privacy Enforcement Network's (GPEN) annual intelligence gathering operation which looked at "*how well organisations have implemented the core concept of accountability into their own internal privacy policies and programmes*". While the joint report on the 2018 GPEN Sweep suggests a good level of understanding of the concept of accountability, in particular by the 28 organisations that responded to the ICO (as a data protection authority participating in the sweep), the UK regulator echoes the report's conclusion that "*in practice there is significant room for improvement*". Key areas where organisations were found wanting include monitoring internal performance in relation to data protection standards, staff training and complaints handling.

Background

The GPEN was established in 2010 upon recommendation by the Organisation for Economic Co-operation and Development. Its aim is fostering cross-border co-operation among privacy regulators through "*the establishment of an informal network of Privacy Enforcement Authorities and other appropriate stakeholders to discuss the practical aspects of privacy law enforcement co-operation, share best practices in addressing cross-border challenges, work to develop shared enforcement priorities, and support joint enforcement initiatives and awareness raising campaigns*". The informal network comprises over 60 privacy enforcement authorities in 39 jurisdictions around the world.

Results of the GPEN Sweep

The 2018 GPEN Sweep saw participating GPEN members, including the ICO, elicit meaningful responses from 356 organisations in 18 countries, representing just over half the organisations that were approached. The key findings, positive and negative, are discussed below:

- a large percentage of organisations across all sectors and jurisdictions had appointed an individual or team who would assume responsibility for ensuring their organisation's compliance with relevant data protection rules and regulations. There were examples of good practice. For instance, some organisations were found to have a central individual at the senior level who was responsible for data protection, with data protection "champions" in each office or business unit. Other organisations had data protection officers at different levels to ensure a clear communication network was in place;
- organisations were generally found to be "quite good" at providing data protection training to staff, but often failed to provide refresher training or only provide training to some employees;
- a large majority of organisations actively maintain privacy policies that explain how they handle personal data, and these were often easily accessible to the public, with less than 10% of organisations having no policies at all;
- when it comes to monitoring internal performance in relation to data protection standards, organisations fell short, with more than 20% of organisations having no programmes in place to conduct self-assessments and/or internal audits;
- over half of the organisations surveyed indicated that they have documented incident response procedures, and that they maintain up-to-date records of all data security incidents and breaches. However, just under 15% of organisations surveyed indicated that they have no processes in place to respond appropriately in the event of a data security incident. Nonetheless there were examples of good practice. For instance, some organisations have developed risk management manuals, while others have set up dedicated teams to respond to and handle security

risks. Some organisations stated that they maintain up-to-date incident logs that are tested annually and sit alongside breach/incident escalation policies and incident management procedures. Some organisations noted that they have checklists that detail every step to follow in the event of a security incident;

- attitudes to risk management were variable. In this respect, of 287 organisations surveyed, 46% indicated that they have documented processes in place, such as privacy impact assessments, to assess the risks associated with new products, services, technologies and business models. However, just under 20% demonstrated little to no understanding of the importance of assessing risks associated with new products, services, technologies and business models. Around half of respondents stated that they actively maintain logs of all data held by them, and most of those maintain records of any data flows. However, some organisations had little to no understanding of the sort of data they hold and fail to maintain an adequate inventory. A small minority of organisations appeared to have a limited understanding of what constitutes "personal information", in particular, that it extends to employees as well as customer information.

Comment

If this had been a GDPR sweep, the report would make ugly reading. But the GPEN's investigation is a global exercise covering non-EU jurisdictions whose privacy regimes are less prescriptive, for example, as to the need for data protection impact assessments (DPIAs) or the appointment of data protection officers. Nevertheless, the message from the ICO, a GDPR regulator, is clear: organisations, including UK controllers and processors, should be doing more to achieve privacy accountability. The ICO is likely to take an increasingly robust approach towards the sanctioning of systemic failings, which indicate that organisations, particularly large data controllers, have failed to understand the significance of the key principles of accountability and privacy by design that lay at the heart of the GDPR.

As ICO Head of Intelligence, Adam Stevens, said, this means having appropriate technical and organisational measures in place, including "*clear data protection policies in place…and continuing to review and monitor performance and adherence to data protection rules and regulations*". Ultimately, the GDPR principle of accountability requires controllers and processors to demonstrate GDPR compliance through implementation of internal mechanisms such as DPIAs, auditing and certification, consistent staff training and allocation of responsibility for overseeing compliance to individuals who possess the necessary expertise in national and European data protection laws and practices and an in-depth understanding of the GDPR.