Personal data breach framework
Putting you in the best position to deal with challenge

March 2018
Personal data breach framework

Expert help with personal data breaches to put you in the best position to deal with challenge

Compulsory breach notification will bring a new era to data privacy from May 2018, when the GDPR comes into force. For the first time, organisations will be under a statutory duty to report certain contraventions of data protection law to both regulators and people affected.

The new regime under Articles 33 and 34 GDPR will surface issues which may have previously remained hidden. This is likely to herald a huge increase in regulatory sanctions, compensation claims and brand/reputation damage, which will come as a seismic shock to the unprepared.

Articles 33 and 34 contain a complex set of rules for notification which can be difficult to operationalise. Failure to understand and properly implement these requirements will increase the risks of:

- Non-compliance, exposing the controller to regulatory sanctions, compensation claims and brand/reputation damage; or
- Over-notification, attracting unnecessary and unwanted attention from adverse scrutineers.

Mistakes in the immediate aftermath of a breach could have costly long-term consequences.

We can support you throughout with our Personal Data Breach Framework, which provides the structures needed for successful breach handling.

1. We are a leading professional services firm and understand the business, regulatory and legal context in which organisations operate. This enables us to view the challenges of personal data breach through a practical, organisational lens.

2. Data breach can take many forms and knows no jurisdictional boundaries. We can leverage PwC's global presence and extensive legal network to solve quickly the most complex cross-border issues arising from a data breach.

3. PwC has been able to recruit leaders in all the different disciplines which are needed to address a substantial data breach. This pooling of varied experience and perspective is seldom found in one organisation. Our understanding of technology and our ability to assist you with avoiding and remedying technological failure is unparalleled.

4. Our Personal Data Breach Framework will be tailored to complement the regimes you have currently to deliver, assure and audit secure, compliant and lawful data handling.

Personal data breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

(GDPR Art 4(12))

Enforcement tracker

Our Privacy and Security Enforcement Tracker monitors decisions in regulatory enforcement cases for data protection and security in over 20 different jurisdictions. This unique analysis informs all elements of our Personal Data Breach framework and enables us to keep you regularly updated on key developments and trends.

65% increase in ICO enforcement action

2016 saw a 65% increase in ICO enforcement action (Monetary Penalty Notices, Prosecutions, Enforcement Notices and Undertakings).
Our methodology

Process review and gap analysis
We can review your breach notification processes against the requirements of Articles 33 and 34 and prevailing regulatory practice, providing a gap analysis report on areas of compliance and make recommendations for improvement.

Risk appetite and posture setting
We can help you establish your risk appetite in marginal situations and develop your posture when dealing with the ICO, data subjects and third parties at breach notification. We can recommend a series of tailored exploratory workshops with key stakeholders, considering various breach scenarios which might arise. We will set out our findings and recommendations in a detailed report.

Playbook for personal data breach
We can help you develop a playbook for dealing with all aspects of personal data breaches and reporting requirements. This will include: organisational charts with clearly defined roles and responsibilities; process flows for the 72-hour period following incident detection; guidance notes for all key issues; and scripts for notification and responses.

Training and testing
We can help you develop detailed role-based training and supplement this with business-wide awareness training that highlights the key risks associated with data breach, the pressing timetable and need for early escalation of incidents.

We can also provide scenario-based ‘war games’ for testing your personal data breach playbook. These exercises build awareness and understanding in a safe learning environment and ensure your playbook survives contact with real-world breaches.

Applying your playbook

Development of triage mechanism
A key part of your data breach playbook is an effective triage mechanism, which ensures an informed and expeditious response to a personal data breach. We can help you create protocols which allow personnel involved in the Articles 33 and 34 procedures to consider the evidence, take steps to preserve relevant material, apply the personal data breach definition and assess the risk to rights and freedoms. These protocols will identify points of escalation to senior management and, taking into account your risk appetite and posture, facilitate prompt decisions on breach reporting.

Accurately assessing risks to rights and freedoms
Perhaps the most difficult aspect of mandatory breach notification is assessing whether the breach represents a risk or high risk to the rights and freedoms of natural persons.

Our approach to assessing the level of risk caused by a specific breach is unique. We draw on the key elements from the wider framework of human rights law, analysis from our Enforcement Tracker and the insights we have gained through our Privacy Transformation work with some of the world’s largest organisations.
Contacts

Stewart Room
Partner, PwC UK
T: +44 (0)20 7213 4306
E: stewart.room@pwc.com

Kate Macmillan
Director, PwC UK
T: +44 (0)7718 979744
E: kate.macmillan@pwc.com

Ben Prior
Manager, PwC UK
T: +44 (0)7730 597011
E: ben.prior@pwc.com