Personal Data Breach Framework

Putting 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.

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.

2016 saw a 65% increase in ICO enforcement action

(Monetary Penalty Notices, Prosecutions, Enforcement Notices and Undertakings)
Our methodology

Preparation

- Analyse: Process review and gap analysis
- Design: Playbook
- Develop: Training and testing

Process review and gap analysis

We can review your breach notification processes against the requirements of Articles 33 and 34 and prevailing regulatory practice, provide 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 and beyond. We can recommend a series of tailored exploratory workshops with key stakeholders, considering various data breach scenarios which might arise. We will set out our findings and recommendations in a detailed report.

Defence

- Defence
- Civil litigation
- Criminal

INCIDENT

- Data breach notification
- Evidence evaluation
- Apply ‘Personal Data Breach’ definition
- Assess ‘Risk to Rights and Freedoms’
- Consider risk appetite and posture
- Notify as appropriate

Art. 33 and 34 GDPR

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 account of your risk appetite and posture, facilitate prompt decisions on breach reporting.

Risks to rights and freedoms calculator

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 Risk to Rights and Freedoms calculator can deliver this for you. Our calculator draws on 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.

This product is unique to PwC's human rights landscape.

The risk of damage arising from a data breach has never been greater. In the post-GDPR era, claimants, backed by litigation funders, will be better placed to bring class actions, rely upon multiple causes of action and seek damages for distress.

We can help you navigate the challenges of this new climate:

- **Pre-notification**: avoid hostages to fortune
- **Post-notification**: defend yourself robustly

We also recognise that personal data breach presents a substantial threat to your reputation and brand. Our highly experienced and specialist team can help you rebut misconceived narratives and unfair criticism in order to put you in the best position with key influencers and customers.

"It is very disappointing to see the company is apparently still uncovering additional problems despite the length of time since the breach occurred."

(Source: ICO)

"Over half of CEOs are concerned about their readiness to respond to crisis."

(Source: PwC 19th Annual CEO survey)
Why choose PwC for your Personal Data Breach Framework?

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 andremedying 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.

Stewart Room
PwC | Partner

T: +44 (0) 20 7213 4306
E: stewart.room@pwc.com

Kate Macmillan
PwC | Director

T: +44 (0) 7718 979744
E: kate.macmillan@pwc.com

Ben Prior
PwC | Manager

T: +44 (0) 7730 597011
E: ben.prior@pwc.com

Stewart is the global leader of the cyber security and data protection legal services practice, the joint global leader of the multi-disciplinary data protection practice, and the UK data protection practice leader.

He has more than 25 years of experience as a Barrister and Solicitor, focusing for the majority of this time on data, technology and communications.

He is recognised widely as pre-eminent in data protection. He was one of only three experts invited to give evidence to the House of Lords on how the UK should maintain unhindered data flows with the EU post Brexit. The PwC practice he has built from scratch is recognised as being ‘brilliant’ by the Legal 500. He is described as an ‘excellent, first-rate, tactical lawyer’ and ‘the kind of lawyer who inspires confidence’ by Chambers UK.

Kate has been recognised as a leading privacy, data protection and reputation management lawyer since 2006. She has over 20 years of experience in these areas.

Chambers UK has described her as ‘prominent reputation management specialist’ who is ‘calm in a crisis’, ‘reassuring to people in the eye of the storm’ and noteworthy for providing ‘clear advice, which is not bogged down with legalese.’

The Legal 500 2017 describes her as ‘a real star in the data protection space’ - ‘a very clever litigator with huge experience’ and ‘masterful at managing tricky cases.’

Ben is a leading cyber security and data protection lawyer, who couples his legal expertise with a practical approach to managing the implications of a cyber incident.

Ben joined PwC from the National Crime Agency, where he was the lead lawyer for the National Cyber Crime Unit and advised on the UK’s high priority investigations.

Ben is also an expert on the policy, legislative and security considerations which underpin the culture of our cyber environment, having participated in Government steering boards for the implementation of the new data protection regime and the Investigatory Powers Act 2016.