SQUIRE PATTON BOGGS

GDPR Webinar – Data Breach Notifications and Response Plans

26 January 2017

Your Speakers

Dr. Annette Demmel, Berlin

Rechtsanwältin
Certified Specialist for Information Technology Law
Certified Specialist for Copyright and Media Law

Monika Kuschewsky, Brussels

Rechtsanwältin
Certified Information Privacy Professional/Europe (CIPP/E)
Betrieblicher Datenschutzbeauftragter (GDDcert.)

The General Data Protection Regulation ("GDPR")

SQUIRE PATTON BOGGS

- 4 May 2016: **Publication**
- 25 May 2016: **Date of entry into force**
- As of 25 May 2018: **Date of application**

Including to companies that process personal data outside of the EU but offer their goods or services to individuals within the EU

Overview

SQUIRE PATTON BOGGS

- Background
- What is a personal data breach?
- What are the notification obligations?
- How to prepare a personal data breach response plan?

Background

SQUIRE PATTON BOGGS

- GDPR introduces for the first time a general data breach notification at EU level:
  - Requiring both notification to the supervisory authority ("SA") and communication to the data subjects.
  - The Article 29 Working Party ("WP29") is expected to update guidance on data breach notification in 2017.

- At present:
  - At EU level, there exist special regimes for:
    - providers of "publicly available electronic communications services" under the ePrivacy Directive (will be replaced by proposed ePrivacy Regulation); and
    - for operators of essential services under the Directive on the security of network and information systems ("NIS Directive").
  - At national level, there exist some mandatory or voluntary data breach notification regimes, such as in Germany or the UK.

What is a Personal Data Breach?

Article 4(12) GDPR

SQUIRE PATTON BOGGS

- 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.

- Not covered:
  - Other forms of non-compliance; and
  - Security breaches concerning other types of data or information, such as company data or proprietary data (e.g., business secrets, IP).

Notification to the SA

Article 33 GDPR

SQUIRE PATTON BOGGS

- **What** triggers the obligation?
  - In the case of a personal data breach.
  - Exception: If the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

- **Deadline:**
  - Without undue delay.
  - Where feasible: Not later than 72 hours after having become aware of the breach.
    - If later than 72 hours: justification required (reasons for the delay)!

Notification to the SA (cont.)

Articles 33, 55 ff. GDPR

SQUIRE PATTON BOGGS

- **Who** must notify **whom**?
  - The processor must notify the **controller**.
  - The controller must notify the ***competent*** SA.
    - New: One-Stop Shop: **Lead SA** for EU-wide processing.
      - **Cooperation mechanism** between lead SA, concerned SAs and the European Data Protection Board.
      - For Article 29 WP guidance on identifying the competent lead SA, see here.

Notification to the SA (cont.)

Article 33 GDPR

SQUIRE PATTON BOGGS

- **How to** notify?
  - Content:
    - Name and contact details of the data protection officer or other point of contact.
    - Description of:
      - the nature of the personal data breach;
      - the likely consequences of the personal data breach;
      - the measures taken or proposed to be taken by the controller to address the personal data breach.
  - In principle: All information must be provided at the same time.
    - Exceptionally: In phases, without undue further delay.

Documentation Requirements

Article 33(5) GDPR

SQUIRE PATTON BOGGS

- The controller shall **document** any personal data breaches, comprising:
  - the facts related to the breach,
  - its effects and
  - the remedial action taken.

- The documentation shall **enable SAs to verify compliance** with the notification requirement.

Communication to the Data Subject (cont.)

Article 34 GDPR

SQUIRE PATTON BOGGS

- **What triggers** the obligation?
  - When the personal data breach is likely to result in a *high* risk to the rights and freedoms of natural persons.
  - SA might order the controller to communicate the personal data breach to the data subject.

- **Exceptions**:
  - The controller has implemented **appropriate technical and organisational protection** measures, and those measures were applied to the personal data affected by the personal data breach (e.g., encryption).
  - The controller has taken **subsequent measures** which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.
  - A communication would involve **disproportionate effort**.
    - In such a case, a public communication or similar measure is required.

Communication to the Data Subject (cont.)

Article 34 GDPR

SQUIRE PATTON BOGGS

- **Deadline**
  - Without undue delay.

- **Who** must communicate **to whom**?
  - The controller must communicate the breach to the data subject.

- **How to** communicate the breach?
  - Same content as notification to the SA, but in clear and plain language.

Non-compliance with the Personal Data Breach Requirements

Articles 77-84 GDPR

SQUIRE PATTON BOGGS

- Constitutes a serious violation, subject to a fine up to **Euro 10 million** or up to **2%** of the total worldwide turnover of the preceding year.

- May lead to:
  - Complaints to the SA;
  - Claims for damages;
  - Ban or suspension of the underlying processing by a SA;
  - Injunctions or interim measures by individuals or works councils;
  - Loss of reputation and customer trust;
  - Further data loss, etc.

How to Prepare a Data Breach Response Plan?

SQUIRE PATTON BOGGS

- Breach **prevention**
  - Identify, assess and amend existing technical and organisational security measures (Art. 32 GDPR).
  - When using vendors:
    - Implement/amend existing due diligence procedures to cover data protection/security.
    - Check existing contractual terms and incorporate new mandatory GDPR requirements, including specification of the mandatory breach reporting obligation and specific security measures.
    - Audit and monitor for non-compliance.
  - Operate awareness campaigns/training for the organisation's employees.
  - Review the organisation's insurance policies to ensure they sufficiently cover the costs of a data breach.

How to Prepare a Data Breach Response?

SQUIRE PATTON BOGGS

- Breach **management**
  - Assign responsibilities:
    - Consider setting up a multi-departmental team, comprising, for example, General Counsel, Privacy/Compliance, IT, Security, HR, Communications/Media relations.
    - Contact information for team members, competent SA and other authorities.
  - Consider contractual arrangements with public relations firms, credit monitoring service providers, forensic investigation firms, external counsel, public communications firms in advance.
  - Set up policies/procedures to detect, stop and respond to data breaches, including the capability to assess the risk and risk levels in light of statutory requirements and especially the tight reporting deadlines.
  - Ensure proper documentation right from the start.
  - Plan for notifying affected individuals.
  - Involve legal counsel (legal privilege).
  - Create guidance, FAQs, checklists and templates, including for documentation purposes.
  - Regularly review, test and update/improve the data breach response plan.

SQUIRE PATTON BOGGS

Questions and Answers

Thank you!

Dr. Annette Demmel

Partner, Berlin
T +49 30 7261 68 108
annette.demmel@squirepb.com

Monika Kuschewsky

Partner, Brussels
T +32 2 627 11 11
monika.kuschewsky@squirepb.com