SQUIRE PATTON BOGGS

EDPS-ENISA Conference: Towards assessing the risk in personal data breaches

April 04, 2019

Introduction

Law

Art. 33.1 GDPR - the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority (except when….)

Problem

72 hours – short time- !

Tip

BE PREPARED

- Incident Response Plan
- Training
- Contracts

Controller Incident Response Plan

SQUIRE PATTON BOGGS

1. Identify the response team;
2. Emails and telephone numbers of all team members;
3. Who will do what when a breach occurs -> specify it!;
4. How will the team be informed? (e-mail?, phone?);

   How will the person who “caught” the breach know whom to report it to/ or where?;
5. Who else will be informed? (CFO, Board, Legal, DPO, Communications Dep);
6. Clarity on who is the lead authority (cross-border cases);

   - local DPA’s notification form?
7. Templates documents ready (for notification to DPA’s);
8. Clarity on how to communicate to data subjects if required (e-mail)?;
9. Will you use forensic services? Lawyers? P.R. Companies? Or source help from other group entities?.

Contracts with service providers in place/retainers

SQUIRE PATTON BOGGS

1. Providers of forensic services – Or will you be able to carry out this task internally or source help from one of your group entities? [Pros and cons]

   Is a back up necessary?

2. Legal counsel ? – internal?
3. Is a PR company needed (e.g. , when communication of breach to data subjects is required)?

4. Insurance companies?

Notification Controller/Processor- Timing

SQUIRE PATTON BOGGS

Law

- **Art. 33.1 GDPR** - the **controller** shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority.
- **Art. 33.2 GDPR** – The **processo**r shall notify the controller without undue delay after becoming aware of a personal data breach.

Problem

When does the 72h time start for the controller whose processor's data processing operation was breached?

Tip

Reflect timing obligations in Art. 28 DPA

Make sure you have clear roles and responsibilities

(e.g., they do not notify on your behalf, release any unapproved statements)

Reporting obligations- processors

SQUIRE PATTON BOGGS

Law

- **Art. 33.1 GDPR** - the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority.
- **Art. 33.2 GDPR** – The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

Problem

a. What information shall be given to the data controller by the processor?

b. What if DPA wants more information (at a later stage)?

Tip

Reflect obligations in Art. 28 DPA

Liability – CAPS - Insurability

Law

Art. 82 GDPR – Right to compensation and liability

Problem

Art. 28 DP Agreements include liability caps - indemnities

a. Caps for administrative fines + other damages claims
b. Are caps enforceable?

Tip

Be mindful

Request

Clarification regarding penalities needed

When the breach happens

SQUIRE PATTON BOGGS

- Put **the incident response plan** in practice

→ **Contain the leak!!**

- If data has to be sent to forensic companies/ for internal analysis (e.g., to a centralized IT function), don't create more problems by
  - Sending too much information
  - Sending to third countries without safeguards

(if you have to notify supervisory authorities/ communicate to data subjects)

- Determining risk/ high risk to the righs and freedoms of data subjects

→ it will seldom be an exact assessment

After the breach

SQUIRE PATTON BOGGS

- Update **the incident response plan** and your internal technical and organizational measures in light of the lessons learned
- Trainings, for example
  - Changing or selecting passwords
  - Not to click on phishing emails and how to recognize them
- Record internally all the breaches
  - Prepare a record template
  - Records should not contain unnecessary information that could create additional exposure

SQUIRE PATTON BOGGS

Questions?

Contact Details

Ann J. LaFrance
Partner, London, UK
T +44 20 7655 1752
ann.lafrance@squirepb.com

Annette Demmel
Partner, Berlin, Germany
T +49 30 72 616 8226
annette.demmel@squirepb.com

Rosa Barcelo
Partner, Brussels, Belgium
T +322 627 1107
rosa.barcelo@squirepb.com

Monika Kuschewsky
Partner, Berlin, Germany
T +49 30 72 616 8220
monika.kuschewsky@squirepb.com

Stephanie Faber
Of Counsel, Paris, France
T +33 1 5383 7400
stephanie.faber@squirepb.com

Global Coverage

SQUIRE PATTON BOGGS

Abu Dhabi
Atlanta
Beijing
Berlin
Birmingham
Böblingen
Bratislava
Brussels
Budapest
Cincinnati
Cleveland
Columbus
Dallas
Darwin
Denver
Doha
Dubai
Frankfurt
Hong Kong
Houston
Leeds
London
Los Angeles
Madrid
Manchester
Miami
Moscow
Newark
New York
Northern Virginia
Palo Alto
Paris
Perth
Phoenix
Prague
Riyadh
San Francisco
Santo Domingo
Seoul
Shanghai
Singapore
Sydney
Tampa
Tokyo
Warsaw
Washington DC
West Palm Beach

Africa
Argentina
Brazil
Chile
Colombia
Cuba
India
Israel
Italy
Mexico
Panamá
Peru
Turkey
Ukraine
Venezuela

Office locations
Regional desks and strategic alliances