EDPS-ENISA CONFERENCE ON PERSONAL DATA BREACHES

Stibbe

Panel Discussion III

Supporting data controllers on assessing the risk of a personal data breach

1. Immediate actions

- **Quick scan: malicious or not?**
- **Manage communications (instruct employees)**
- **Contain the risk as much possible and mitigate**
- **Strategic decision: restore v not contaminating**

2. Fact finding - forensics

- **Collect relevant information about the context of the data breach and impact**
- **Assistance from external forensic experts/auditors with effective tools (DPA)**
- **Document steps undertaken (log)**
- **Territorial aspects of the attack: where did the breach occur?**

2. Fact finding - forensics

- **Nature of the data breach: human error, technology failure, malicious intent …**
- **Data involved: which databases, which types, sensitive, volumes, etc.**
- **Categories/number of data subjects affected: suppliers, customers, employees, website visitors, etc.**
- **Time of the data breach**

2. Fact finding - forensics

- **Likely consequences**
- **Name and contact details (DPO, legal, risk, CISO?)**
- **Measures taken or proposed to address the breach, including to mitigate adverse effects**
- **Attach the form to be submitted to the DPA**

3. Notification obligations

- **Notification of the DPO/data protection team**
- **Notifying data protection authority (article 33 GDPR)**
  - “likely to result in a risk to the rights and freedoms of data subjects” (low threshold)
  - “ Without undue delay and where feasible within 72 hours after becoming aware of the breach” (be pragmatic, but notify even when only partial information)
  - It is recommended to only provide the information that is required
  - Which authority? Principle of “leading supervisory authority” for all cross-border processing of personal data: the authority of the place where the data controller has its main establishment
  - Who is data controller? (can be tricky – file on behalf of all entities involved)

3. Notification obligations

- **Notifying data subjects (article 34 GDPR)**
  - “Without undue delay”, but no strict time limit
  - “breach is likely to result in a high risk to the rights and freedoms of natural persons”
  - Can be cross-checked with DPA
- **Notification of CERT**
- **Notifying customers, suppliers and other stakeholders**
  - Under specific contractual obligations (to check) but also general contract law
- **Notification of sector specific regulators (Financial, Telco, Aviation, …)**

4. Filing a criminal complaint (if malicious)

- **Public prosecutor (IT forgery, IT fraud, hacking and IT sabotage are criminally sanctioned)**
- **Safeguard your interests vàv other stakeholders (shareholders, business partners,…)**
- **Ideally in the jurisdiction of the place where it is easiest to collect the required evidence**
- **Can be in multiple jurisdictions**
- **No strict time limit for such complaints, best once a first level of analyses has**

Thank you!

Erik Valgaeren
Partner
T +32 2 533 53 43
M +32 477 50 62 92
erik.valgaeren@stibbe.com

Thank you

Stibbe

Stibbe.com