SESSION ID: SEM-MO1

A PRACTICAL GUIDE TO GDPR BREACH NOTIFICATION AND SECURITY REQUIREMENTS

Mahmood Sher-Jan  
CEO and President  
RADAR, Inc.  
@msherjan

Julia Jacobson  
Partner  
K&L Gates, LLP
Overview

- Key definitions for breach notification requirements and GDPR
- 5 phases of an effective breach response lifecycle
- Questions
Key Definitions for GDPR Breach Notification

Personal data

GDPR regulates all forms of personal data which is defined as “any information relating to an identified or identifiable natural person.”

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.”

Art. 4. (12)
Key Definitions for GDPR Breach Notification

Types of data breach

- **Availability breach**: Accidental or unlawful destruction or loss of personal data.
- **Integrity breach**: Alteration of personal data.
- **Confidentiality breach**: Unauthorized disclosure of, or access to, personal data.
Having become aware

“...a controller should be regarded as having become “aware” when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.” - WP29 Guidance

- A short initial investigation period may be required to determine if personal data has been compromised.
- What constitutes a reasonable degree of certainty?
- Key difference to US regulations: assumption of breach
Key Definitions for GDPR Breach Notification

Having become aware – benchmarking data from US organizations show the average timeframe to be:

- Occurrence > Discovery – 13.21 days
- Discovery > Notify – 29.1 days

*From RADAR metadata: https://www.radarfirst.com/blog/from-incident-to-discovery-to-breach-notification-average-time-frames*
Key Definitions for GDPR Breach Notification

Risk vs High Risk

- The standard for notification to supervisory authorities is a breach that is likely “to result in a risk to the rights and freedoms of natural persons.” Article 33 (1)

- The standard for notification to data subjects is a breach that is likely to result in a “high risk to the rights and freedoms of natural persons.” Article 34 (1)
Key Definitions for GDPR Breach Notification

Considerations when determining severity and likelihood of risk:

- Form of data
- Data protection measures such as pseudonymization
- Nature of the incident
- Recipient of the data
- Risk mitigation

<table>
<thead>
<tr>
<th>Data elements</th>
<th>Cultural or social</th>
<th>Financial</th>
<th>Health</th>
<th>Reputation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank account number without access code</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit history</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employment history</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>National identification number</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Important to note: This risk assessment is different from a DPIA, which is theoretical in nature.
Phased notifications
After making an initial notification, a controller could update the supervisory authority if a follow-up investigation uncovers evidence that the security incident was contained and the breach did not pose a high risk.

Delayed notifications
If notice is not provided to supervisory authority within 72 hours, you must provide a reason for the delay.
## Key Definitions for Breach Notification under GDPR

### Roles in US vs GDPR

<table>
<thead>
<tr>
<th>US</th>
<th>GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Covered Entity:</strong></td>
<td><strong>Controller:</strong></td>
</tr>
<tr>
<td>Responsible for notice to affected individuals &amp; regulatory agencies</td>
<td>Responsible for notice to data subjects &amp; supervisory authorities</td>
</tr>
<tr>
<td><strong>Business Associates:</strong></td>
<td><strong>Processor:</strong></td>
</tr>
<tr>
<td>Responsible for notice to CE / Data Owner (timeline for notice specified in the agreement)</td>
<td>Responsible for notice to controller.</td>
</tr>
</tbody>
</table>
Key Definitions for GDPR Breach Notification

Entities with EU establishments
- Single member state vs. cross-border breaches
- Notice to lead supervisory authority
- Notice to individuals in applicable member states
- Voluntary report to applicable member state DPAs

Entities without EU establishments
- Single member state vs. cross-border breaches
- Notice to lead supervisory authority of the entity representative
- Notice to member state of affected individual (?)
Providing notification in 72 hours

Racing the clock to determine...

- Who must be notified? How?
- Can you ensure consistency and manage risk?
- Can you demonstrate compliance?

...*do you even need to notify?*
Before a Breach Takes Place....

**Operational:**
- Data mapping and inventory, data workflows
- Identify core and extended teams
- Establish organizational controls & breach response plan
- Have cyber insurance & know what it covers/what the process is to report
- Practice, practice, practice – hold regular tabletop exercises

**Data Security:**
- Data Storage
- Disaster Recovery, Business Continuity
- Integrated systems passing information from a GRC, SIEM, ticketing system, or privacy monitoring software
5 phases of an effective breach response lifecycle

Operationalize breach notification

1. Timely incident intake and escalation
2. Consistent risk assessment
3. Providing notification
4. Reporting and trend analysis
5. Staying current with changing regulations
Timely incident intake and escalation

- Single channel of escalation
- Integrations and APIs with detection systems
- Avoid duplicate data entry
- Complete documentation of required incident details
- Automated alerts to privacy & security teams
Consistent assessment

- Defensible, compliant multi-factor risk assessment
- Enables cross-functional collaboration
- Legal oversight
- Documentation & audit trail
Scenario: Confidentiality Breach

A website hosting company acting as a data processor identifies an error in the code which controls user authorization. The effect of the flaw means that any user can access the account details of any other user.

Data compromised: Name and Financial Account Number

...do you have to notify?

# Sufficient Risk Mitigation

### Risk factors

<table>
<thead>
<tr>
<th>What is the incident category? *</th>
<th>Incident subcategory *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic</td>
<td>Website</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What is the nature of the incident? *</th>
<th>Compromise description *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unintentional or inadvertent</td>
<td>Unauthorized access</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Who was the recipient of the data? *</th>
<th>Recipient description *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized person or organization, or unknown</td>
<td>Customer</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What is the risk mitigation outcome? *</th>
<th>Risk mitigation description *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sufficient risk mitigation</td>
<td>Forensic analysis determined that data integrity or confidentiality was not compromised</td>
</tr>
</tbody>
</table>
Sufficient Risk Mitigation

- **GDPR lead supervisory authority**: Low
  - **Data Sensitivity**: High
  - **Incident Severity**: Low

  **Notifications**
  - **Name**: Netherlands Data Protection Authority (A/P)
  - **Guidance**: No
  - **Decision**: No
  - **Due**: 06/09/2018 6:12 PM
  - **Notified**
    - **Regulation**: Notify without undue delay and, where feasible, not later than 72 hours after becoming aware, by Monday, June 4, 2018 at 6:12 PM.

  **Data elements**
  - Financial account information
  - Name

- **Ireland**: Low
  - **Data Sensitivity**: High
  - **Incident Severity**: Low

  **Notifications**
  - **Name**: Affected Individual(s)
  - **Guidance**: No
  - **Decision**: No
  - **Due**: 06/09/2018 6:12 PM
  - **Notified**
    - **Data Protection Commissioner (DPC)**

  **Data elements**
## Insufficient Risk Mitigation

### Risk factors

<table>
<thead>
<tr>
<th>What is the incident category? *</th>
<th>Incident subcategory *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic</td>
<td>Website</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What is the nature of the incident? *</th>
<th>Compromise description *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unintentional or inadvertent</td>
<td>Unauthorized access</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Who was the recipient of the data? *</th>
<th>Recipient description *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized person or organization, or unknown</td>
<td>Customer</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What is the risk mitigation outcome? *</th>
<th>Risk mitigation description *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient or unknown risk mitigation</td>
<td>Unknown</td>
</tr>
</tbody>
</table>
Insufficient Risk Mitigation
Provide notification

- Counsel approved notification templates
- Content, format & contact requirements
- Generating notifications
- Central repository of all notifications
Real-time reporting, trend analysis

- Track program key performance indicators
- Establish benchmarking metrics:
  - Volume, source, type
  - Initial vs. Complete vs. amended notifications
  - Average time to provide notice
  - Frequency of missed deadlines or delays
Remain current with changing regulations

- Considerations:
  - Monitor pending regulations
  - Analysis of impact on existing workflow and decision making
  - Implementation of any resulting changes to workflow, who to notify, notice content, etc.
Apply what you have learned today:

- Establish benchmarking metrics and KPIs
- Identify areas of your privacy program that can be automated or streamlined
- Begin building a model to demonstrate ROI of investments in your program, assigning value of reducing *overall risk* and *operational costs*. 
ANY QUESTIONS?

Thank you!