Personal Data Breaches

4th April 2019
EDPS-ENISA Conference
Panel Discussion 1 – Experience in Ireland
Introduction –

- Legislative Frameworks
- Data Breaches – definitions, statistics
- *Notification and Communication* of Personal Data Breaches
- Consequences
- Key Messages from the DPC

Niall J. Cavanagh
Assistant Commissioner
The Data Protection Commission

Legislative Frameworks

• General Data Protection Regulation
• Law Enforcement Directive
• Data Protection Act 2018
• [Data Protection Acts 1988 and 2003] – s.8 of 2018 Act
• Statutory Instrument No. 336 of 2011 (e-Privacy Regulations)
Technical and organisational measures

• Secure the ICT

• Secure the environment/paper based systems
What is a Breach?

Legislative Frameworks

• **General Data Protection Regulation & LED**

  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

• **Statutory Instrument 336 of 2011 (e-Privacy Regulations)**

  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 in connection with the provision of a publicly available electronic communications service in the European Union;
Personal Data Breaches

Breaches by Framework since 25 May 2018

- GDPR: 4430
- LED: 348
- Pre-GDPR: 17
- Telcos (e-privacy): 117
Personal Data Breaches

Unauthorised Disclosure

Cyber Incident

Device Lost or Stolen

Paper Lost or Stolen
Personal Data Breaches

Breach Outcome

- Concluded: 4085 (90%)
- Concluded -Non Breach: 304 (7%)
- Live Cases: 165 (3%)
Personal Data Breaches

<table>
<thead>
<tr>
<th>Sector</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private</td>
<td>2947</td>
<td>65%</td>
</tr>
<tr>
<td>Public</td>
<td>1607</td>
<td>35%</td>
</tr>
</tbody>
</table>
Notification to DPC

• General Data Protection Regulation (Art. 33)
• Law Enforcement Directive (s.86 Data Protection Act 2018)
• e-Privacy Regulations
  (S.I. No. 336 of 2011 and
  Commission Regulation (EU) No 611/2013 )
Notification/Communication
Risk Assessment (all frameworks)

Two steps

1. **Notify DPC**
   - GDPR & LED: *unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons*
   - ePrivacy: Always

2. **Communicate with Data Subject** – (exceptions apply)
   - GDPR & LED: *if there is likely to be a high risk to the rights and freedoms*
   - ePrivacy: *if the breach is likely to adversely affect the personal data or privacy of a subscriber or individual*
Verification of Risk Assessment (GDPR)

Case Officer evaluates the self declared risk using

- Qualitative Checklist
- Quantitative Risk Assessment tool
Verification of Risk Assessment (GDPR)

**Qualitative Check list**

Informed by fields of web based notification form:

<table>
<thead>
<tr>
<th>Description of the breach incident:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Was the breach reported within 72 hours of awareness?</td>
<td>Yes / No</td>
</tr>
<tr>
<td>If not, is the explanation given for the late notification feasible / reasonable?</td>
<td>Yes / No / Questionable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Is the possibility of the above processing:</th>
<th>Tick as appropriate ✔</th>
</tr>
</thead>
<tbody>
<tr>
<td>Giving rise to...</td>
<td>Revealing...</td>
</tr>
<tr>
<td>Discrimination</td>
<td>Racial or ethnic origin</td>
</tr>
<tr>
<td>Identity theft</td>
<td>Political opinions</td>
</tr>
<tr>
<td>Reputation damage</td>
<td>Trade union membership</td>
</tr>
</tbody>
</table>
## Verification of Risk Assessment (GDPR)

<table>
<thead>
<tr>
<th>Loss of confidentiality</th>
<th>Health data</th>
<th>Reliability / behaviour / health</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of data protected by official secrecy</td>
<td>Religion or philosophical beliefs</td>
<td>Personal preferences / interests</td>
</tr>
<tr>
<td>Other significant economic or social disadvantage</td>
<td>Criminal convictions / offences</td>
<td></td>
</tr>
<tr>
<td>Loss of rights or freedoms</td>
<td>Related security measures</td>
<td></td>
</tr>
<tr>
<td>Loss of control over data</td>
<td>Genetic data</td>
<td></td>
</tr>
<tr>
<td>Financial loss</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Are vulnerable people affected? | Yes / No |
- Number of persons affected? | [Insert] |
- Large amount of data affected? | Yes / No |
- Have the risks to the DS as identified been mitigated... | Yes / No / Questionable |
  - Sufficiently |
  - In a timely manner |
  - Have data subjects been informed? | Yes / No / Questionable |
## Verification of Risk Assessment (GDPR)

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has the DC/DP identified the organisational / technical deficiencies which led to breach?</td>
<td>Yes / No / Questionable</td>
</tr>
<tr>
<td>Have sufficient organisation / technical measures been implemented to address deficiencies identified?</td>
<td>Yes / No / Questionable</td>
</tr>
<tr>
<td>Are additional organisational / technical measures to be implemented?</td>
<td>Yes / No If yes, insert date and set reminder to secure an update</td>
</tr>
</tbody>
</table>

**Free text box for additional comments:**

**Has this DC reported similar breaches in the past?**

**Free text box for additional comment:**

**Recommendation:**

[Close, follow-up action or commence inquiry]

**Rationale for recommendation:**

**Taking into consideration all of the responses given to the questions on this form do you agree with risk rating of DC**

Yes / No
Verification of Risk Assessment (GDPR)

Quantitative Check list

• Applies weighting factors to volume, type of data to achieve a score
• Still requires Case Officer experience and knowledge
• Determines whether there is
  o No risk
  o Risk
  o High Risk
Risk Rating of GDPR Notified Breaches

Risk Rating

- **Severe**: 23 (1%)
- **High**: 6 (0.4%)
- **Medium**: 191 (14.2%)
- **Low**: 3797 (27.7%)
- **TBC**: 895 (6.6%)

Middle

Low

High
Risk Rating of GDPR Notified Breaches

Risk Rating:
- High or Above: 4%
- Less than High: 96%
- To be Confirmed: 0%
Case Studies

- Highly sensitive data about sexual assault – postal delivery error
- Human error – wrong address on letter
- Loss of unencrypted USB key – health data
- Unauthorised disclosure of data to a journalist
- Financial Institution classed a mis-signed cheque as high risk
- Government body handling grant applications had webshell on server
- Creche sent personal financial data of employees and children’s data to 32 individuals
- Consulting firm disclosed staff salaries to an employee
Key Messages to controllers

In the event of a personal data breach:

• Report on Time
• Contact data subjects without undue delay
• Clearly describe the issue, the steps taken and the planned steps
• Have a Breach Playbook and train your staff
• Retain your Logs, Record of Processing, Breach Records