Management of a Data Breach under the GDPR

Presenter: Hugh Jones

SYTORUS
DATA PROTECTION SPECIALISTS

In the headlines….

Details of online Sony video game players stolen

Insurance Company Staff caught spying on Celebrities' Records

Sony Hackers Hit Up To 250,000 Irish Users in Data Theft

Protecting privacy - A victory for us all

Top telecoms firms fined for cold calling customers

PlayStation Users on high alert after hacking

Customer "harassed" by 225 calls from UPC

40% of tech firms view potential staff on Web

Telecoms companies plead guilty to data protection offences

Insurers to discuss Code after Report identifies breaches of data law

PlayStation fans hit by Credit Card hacker

Telecom companies plead guilty in unsolicited calls case

Celebs in Insurance Spy Probe

Telecom firms prosecuted for sales methods

What constitutes a Data Security Breach?

- “a breach of security…
- leading to the accidental or unlawful
  - destruction,
  - loss,
  - alteration,
  - unauthorised disclosure of, or
  - access to,
- personal data being transmitted, stored or otherwise processed.

(GDPR Article 4.12)

- Remember: A Breach is not automatically an Offence!

SYTORUS
DATA PROTECTION SPECIALISTS

Data Management Considerations

- Security v's Access
- Creative and Compliant
- Users – Ambassadors v Assassins
- Protecting the Brand
- Processing Efficiency
- Retention Schedule – Keep? Destroy? Take the risk?
- Use of Test Data
- Formal engagement of third party Processors
- Policies and Procedures
- Staff Awareness-raising

SYTORUS
DATA PROTECTION SPECIALISTS

How to respond to a Breach

- GDPR outlines specific obligations (Art. 33, 34)
- Controller must report to ODPC within 72 hours of becoming aware
- Breach Notification Report now available on ODPC web-site
- 38-question form must be completed – 22 are mandatory
- New breach v update on existing reported incident
- (Indications of a public register of all those firms who have reported a breach)

SYTORUS
DATA PROTECTION SPECIALISTS

Reporting a Breach to the ODPC

Report should include at least:

- a description of the nature of the personal data breach…
- the categories and approximate number of data subjects concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach;
- whether or not the impacted data has been recovered;
- a description of the measures taken or proposed to be taken by the Controller to address the personal data breach, and, where appropriate,
- measures to mitigate its possible adverse effects and prevent recurrence.

SYTORUS
DATA PROTECTION SPECIALISTS

Liaison with the DP Commission

- Guidance now available on the Commission's re-branded website
- Indication that the DP Commission will issue a Case Reference for each Breach reported
- Telecomms firms continue to use existing reporting forms, guidance
- Alternative 'Raise a Concern' option for members of the public
- Guidance on impact – low, medium, high, severe
- Consideration of the vulnerability of the data subjects – minors, elderly, patients, etc.
- Separate consideration for breach involving law enforcement data

SYTORUS
DATA PROTECTION SPECIALISTS

Reporting a Breach to the Data Subject

- "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay." (Art. 34)
- Provide information on the following *at least*:
  - the name and contact details of the data protection officer or other contact point where more information can be obtained;
  - a description of the likely consequences of the personal data breach;
  - a description of the measures taken or proposed to be taken by the Controller to address the personal data breach, and, where appropriate,
  - measures to mitigate its possible adverse effects and prevent recurrence
- The ODPC may *instruct* the Controller to report to the Data Subjects

SYTORUS
DATA PROTECTION SPECIALISTS

So why comply with the Reporting obligation?

- ‘It’s the law of the land!’
- Principle of Transparency
- Protection of Brand
- Risk of losing control of disclosure
- Reduce risks to reputation
- Protection of public trust
- Failure to report is an offence (Art 83)
- Prosecution for failure to report is capped at €10m or 2% of GAT
- *Report early, clearly, honestly*

SYTORUS
DATA PROTECTION SPECIALISTS

Thank You!

Your Questions?

SYTORUS
DATA PROTECTION SPECIALISTS