Compliance Institute

BETTER BUSINESS ETHICS

Data Breaches and Data Subject Access Requests

Chris Bollard Partner, A&L Goodbody
Andrea Lawler Partner, A&L Goodbody
Tom O'Connor Head of Compliance, KB Associates

CPD CODE: 2022-0013

27th January 2022

compliance.ie

Welcome & Introduction

- Thank you for registering
- Questions
  - Please use the question box on the right of your screen to send the questions for our speaker
- Today's session will be recorded and will be on our website later today
- The CPD code is noted below and will be sent out directly after this session has concluded

CPD CODE: 2022-0013

Upcoming **Webinars**

World Data Protection Day – FREE EVENT

28th January @ 1pm

1 Hour LCOI, FCOI (Compliance), CDPO

Doing the Right Thing: Embedding Business Ethics – FREE FOR MEMBERS

9th February @ 1pm

CPD TBC

Central Bank of Ireland: Speaking Engagement – FREE FOR MEMBERS

21st February @ 1pm

CPD TBC

Compliance Institute

BETTER BUSINESS ETHICS

Panel

Chris Bollard
Partner, A&L Goodbody

Andrea Lawler
Partner, A&L Goodbody

Tom O'Connor
Head of Compliance, KB Associates

CPD CODE: 2022-0013

Compliance Institute

BETTER BUSINESS ETHICS

Data Breaches and Data Subject Access Requests

Andrea Lawler
Partner, A&L Goodbody

CPD CODE: 2022-0013

Data Breaches

- EDPB Guidance on Examples regarding Personal Data Breach Notifications

- Top Tips / Best Practice to ensure you are ready for a Personal Data Breach incident

EDPB Guidance

An overview

- Relevance of the Guidance
- Useful Case Studies that provide a frame of reference and clarity
- Recommends technical and organizational measures to prevent or limit risks that give rise to personal data breaches

Case Studies

- Ransomware
- Data Exfiltration
- Internal Human Risk Source
- Lost or Stolen Devices
- Mispostal
- Social Engineering

Some Key Takeaways

- Controllers should have a *Handbook on Handling Personal Data Breaches* and a robust *Incident Response Plan*.
- While the obligation to notify the SA is "without undue delay and where feasible not later than 72 hours", there may be circumstances where notification within 72 hours may not be satisfactory.
- When uncertain about the specifics of illegitimate access to personal data a controller should assume the worse scenario and assess risk accordingly.
- Even if no notice obligation arises – controller should record remediation steps that need to be taken. The experiences drawn from the breach should be utilized in updating the IT infrastructure

Are you prepared ?

Have a checklist of the steps you need to go through

- What steps need to be taken to ensure the incident has been contained?
- Have you arrangements in place to obtain forensic / security support?
- What points need to be considered to determine whether the breach triggers a notification requirement?
- Do you have any other notification obligations- e.g. under NIS Directive, the ePrivacy Regs or to another regulator?
- Is there a requirement to notify law enforcement?
- Do you have any insurance policies that require the insurer to be informed?
- Have you developed a communication strategy?
- Be mindful of the risk of litigation / risk of statutory inquiry !

Compliance Institute

BETTER BUSINESS ETHICS

Data Breaches and Data Subject Access Requests

Chris Bollard
Partner, A&L Goodbody

CPD CODE: 2022-0013

DSARs

Professional emails, market practices and predictions

DSARs

- Case Study

An employee is subject to a disciplinary investigation which may lead to the termination of their employment. They have been employed by the company for 10 years. They submit a broad DSAR (for “all personal data”) and refuse to reduce its scope. IT estimate that their name appears in about 75,000 documents (mostly emails).

DSARs

Written Rules

- "*The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data […].*"
- *"The controller shall provide a copy of the personal data undergoing processing."*

Developed Practices Rules

- Search for personal data must be "*reasonable and proportionate*".
- Statutory exemptions should be applied at the civil standard of proof.
- Application of exemptions should be explained.
- Redactions are fine – but so too are summaries.
- Opinion given in confidence rarely applicable to a manager's comments

Relevant case law?

EU

- Joined Cases C-141/12 and C-372/12 (YS & Oths)
  - > Data not documents

- C-434/16 (Nowak v Data Protection Commissioner)
  - > Scope of “personal data” is wider than you think

UK

- Deer v Oxford (2017 – England & Wales)
  - > Data not documents
  - > Obligation to conduct a “*reasonable & proportionate search*”
- Rudd v Bridle (2019 – England & Wales)

2022 – The Year of Clarity….?

- EDPB Guidance on the right of access.
- Number of CJEU referrals related to data protection – 7 (2019), 14 (2020) and 26 (2021).
- 15.5 months to produce a decision (on average).
- Trend at CJEU level – expansion of data subject rights.
- Ones to watch in 2022:
  - Case C-154/21 (Austrian Postal Service)
  - C-579/21 (Pankki) (Finnish Bank)
  - C-487/21 (Österreichische Datenschutzbehörde and CRIF)
- UK solo run?

Compliance Institute

BETTER BUSINESS ETHICS

Questions & Answers

Chris Bollard
Partner, A&L Goodbody

Andrea Lawler
Partner, A&L Goodbody

Tom O'Connor
Head of Compliance, KB Associates

CPD CODE: 2022-0013

Thank You For Attending Data Breaches and Data Subject Access Requests

A recording of this webinar and the CPD code will be available on our website later today.

CPD CODE: 2022-0013

Compliance Institute

BETTER BUSINESS ETHICS

compliance.ie