LEWIS SILKIN

Data Breach Checklist

Inside

A guide to what to do when you have had a data breach

Introduction

Data breaches are becoming increasingly common as more staff have access to sensitive data, as hackers become more sophisticated and as IT and data security struggle to keep up with the pace of change.

To help deal with this challenging issue when it arises, and to prepare for when you do get a data breach, we have created this brief guide.

Set out in this guide is a checklist of the things that you will need to consider, and some of the questions you will need to be able to answer, in the event of a data breach.

Checklist

- What is the nature of the data that has been compromised?
  - Personal Data
  - Non-Personal Data
- What is the volume of data that has been compromised?
- Consider what external partners and stakeholders may be required to ascertain the causes and extent of the breach and its subsequent containment and rectification. These could include:
  - Your CTO
  - Enquiry Agents
  - Technical consultancies such as software tracing and analytics
  - Forensic consultancies
- If the data in issue is Personal Data are you the Data Controller or Data Processor of that data?
- Do you owe any contractual obligations to maintain the security of such data and/or mitigate and/or notify your counterparties of the breach?
- Are you a regulated body, or are you processing the data on behalf of someone who is?
- Consider whether any criminal offence has taken place. i.e. Computer Misuse Act, Section 55 of the DPA.
- Identify steps to contain the current breach and mitigate its effect.
- Notify your insurers
- Notify your regulatory body (such as the FCA or SRA) if applicable.
- Notify and brief your PR advisers (internal and external).
- Consider whether to notify the Police if criminal offence(s) are suspected.
- If a Personal Data breach consider strategy on whether to notify the ICO applying the ICO Guidance on Data Breach Notification.
- If Personal Data breach apply the ICO's Guidance on data breach management.
- Notify staff and control documents produced by you and your staff about the breach in view of possible Regulatory inspections and/or litigation.
- Consider notifying your customers/users/employees affected by the breach.
- Consider any causes of action against the perpetrators of the breach:
  - Injunctions to restrain abuse of confidential information
  - Employment sanctions
  - Civil claims such as breach of confidentiality, IP infringement, tortious claims and/or breach of contract
  - Criminal action
- Identify and implement remedial action to prevent re-occurrence of the breach.
- Conduct an audit of your collection and use of data and the security measures used by you and third parties with whom you share data in the handling of data.
- Consider staff training (targeted according to role and seniority).

For further information on this subject please contact:

Simon Morrissey
Partner
T + 44 (0)20 7074 8221
simon.morrissey@lewissilkin.com

LEWIS SILKIN

5 Chancery Lane – Clifford's Inn
London EC4A 1BL
DX 182 Chancery Lane
T +44 (0)20 7074 8000 | **F** +44 (0)20 7864 1200
www.lewissilkin.com