The Data General
Mar 2019

BRIDGING THE COMMUNICATION GAP

IN THIS ISSUE

What is a Breach?

A breach is not just about someone hacking your computer systems. In fact if you have your Cyber Essentials in place then this is the least likely type of breach.

The GDPR and UK Data Protection Act 2018 (DPA) define what constitutes a Breach and when you would need to report it.

Types of Breach?

The most common type of breach is simply not being compliant with the legislation. Privacy Policies referring to the out dated 1998 Act and charging for Subject Access Requests are classic indicators that the organisation does not have all the parts of the puzzle.

Significant changes were implemented with the UK DPA 2018, not just changes to Privacy Policy requirements.

A breach is defined in the GDPR Article 4(12) :- "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;"

A breach is an incident that breaches **Security, Confidentiality, Legislation or Regulation.**

Here are some examples of a Breach.

▷ Security Confidentiality – accidental or intentional leaking of data, usernames and passwords to unauthorized persons either internal or external to the company.

▷ Data Integrity – accidental or intentional disruption or inaccuracies with data held.

▷ Availability – accidental or intentional disruption to system availability or access to data.

▷ Policy – accidental or intentional breach of company policies, procedures and standards.

▷ Legislation / Regulation – accidental or intentional breach of legislation and / or regulation.

▷ Operational – day to day access to systems and data required to fulfil role. Physical security controls such as door locks, key safes and key cards.

The Human element is the biggest risk factor for organisations, which is why training is essential. The cost to the organisation in terms of fines and reputational damage are significant. The organisation is always accountable regardless of who made the mistake.

As a Data Controller you are also liable for the transgressions of your suppliers. Contractual arrangements, processes and due diligence review of your suppliers (Processors) is critical in mitigating the risks to your organisation.

PrimeConduct has a number of training programmes for organisations can help them understand their responsibilities and how to "Spot the Breach".

A well documented process ensures how you respond to a breach is consistent and well prepared. This must of course include self reporting to the ICO regulator where appropriate.

Being prepared and organised is the best approach to mitigating the damage caused by a breach. It also demonstrates to any investigator that you have taken protection of Personal Data seriously.

Don't forget that as a Data Controller you are accountable for the actions or inaction of your supplier processors. Contract carefully and select only those that are compliant.

We are here to help and you can find us at PrimeConduct or Contact Us . We happy to assist in evaluating suppliers for compliance.

.

FAST FACTS

50%

According to Forrester 50% of companies had a data breach in 2017.

62%

Of data breaches were paper based compared to 32% electronic.

28%

Although 72% of breaches were by malicious outsiders a staggering 28% were avoidable insider accidents or errors.

69%

Of data breaches were Identity Theft.

22%

Of breaches involved financial information such as accounts and cards

50%

Of companies are not compliant at all and only 30% have full compliance.

FOR MORE INFORMATION

We are pragmatic, helpful and ethical.

We belong to the IAPP

PRIMECONDUCT
Contact us at PrimeConduct or Contact Us

Breach Management Process

Breach Discovered

When a breach or incident is discovered it is important to act quickly and carefully. If it is a reportable incident the ICO must be informed within 72 hours. If that discovery is down the chain of suppliers every party needs to act together.

Take Notes and Report

The most important aspect is to take notes. Write down what has happened, what Personal Data is involved, who may be affected, and time and date of discovery.

Management Action

As everyone is accountable you must inform your line management and they must act. Action could involve involving the assigned DPO, department heads and IT security.

Assess Severity

Understanding the level of severity of the incident is paramount in determining what actions to take next. It may be minor or major. For example, the loss of a phone that has the contact details of many people and perhaps access to an organisations CRM system is high risk.

Incident Log Entry

The Incident needs to be logged. Everyone is familiar now with the Health and Safety Accident log. A Data Privacy Incident log is a very similar concept. If you are investigated, clear management of your processes will mitigate the actions a regulator may wish to take against your organisation.

Resolve and Mitigate

In the example of a phone that has been lost, a first step could be to inform the mobile operator the phone is attached to. Rapid mitigation of an issue stops it getting worse and minimises impact.

Inform Director or Board

The Management Board or Directors of an organisation are ultimately accountable so they must be informed of what has happened and what has been done to manage the incident.

Escalate to ICO?

Depending on the severity and extent of the breach and the likely impact on individuals, the Directors or Management team must decide whether to inform the ICO and/or people impacted. If you don't when you should then that is also a breach.

Risk Register Update

The Risk Register will need updating in the light of the incident including mitigating actions taken and methods of resolution or fix.

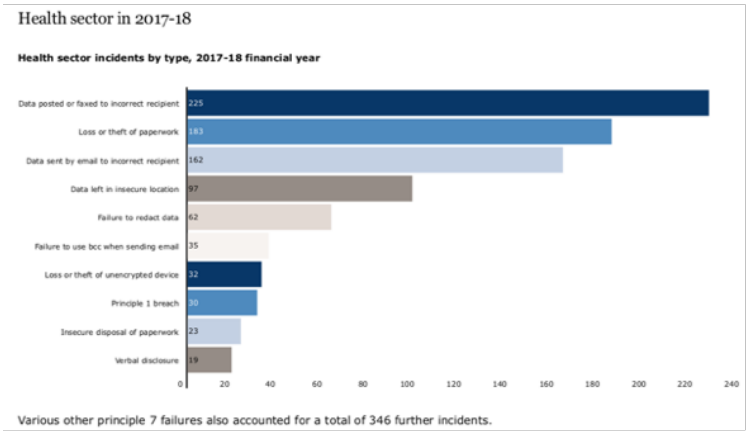
Resolution Report

In any professionally managed process there needs to be a close to the incident which could involve technical changes or process changes and training. This report documents the outcomes and decisions taken.

Close

Close the incident in the log with an outcome and report to everyone involved.

Breaches are a serious issue



- 22% increase Q2 to Q3
- 21% increase Q3 to Q4
- Paper 65%
- Electronic 31%
- Verbal / Visual 4%
- From 2013 to Today
  - UK
  - **141 million breaches**
  - Globally
  - **9.8 billion breaches**

Principle 1 Breach – Where Personal Data is not being used for the purpose it was collected, not accurate, held beyond the retention period or not secure. *(GDPR Article 5)*
Principle 7 Breach - Where Personal Data is not being held or used securely. *(GDPR Article 5 (f))*