Risk control

Personal Data Breaches in the Public Sector

In partnership with

GALLAGHER BASSETT
GUIDE. GUARD. GO BEYOND.

Risk Management Partners
rmpartners.co.uk

Personal Data Breaches in the Public Sector

Introduction

An organisation may collect data about individuals through many different work processes. The Data Protection Act 2018[1] controls how an individual's personal information is collected and used by organisations. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation[2] (GDPR).

According to the Information Commissioner's Office, Local Government organisations have accounted for approximately 9% of all reported data breaches in 2024. 'Data emailed to the wrong recipient' being the most reported type of data breach (18%)[3].

GDPR

Every organisation has strict rules it must follow when using personal data called 'data protection principles'. They must make sure the information is:

- Used fairly, lawfully, and transparently
- Used for specified, explicit purposes
- Used in a way that is adequate, relevant, and limited to only what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Managed in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction, or damage

Data Breach

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity, or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted, or disclosed.

A breach can have a range of adverse effects on individuals, which includes emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. Organisations need to assess this on a case-by-case basis, looking at all relevant factors.

If a breach is likely to result in a substantial risk to the rights and freedoms of individuals, then the organisation must inform those concerned directly as soon as possible and without undue delay.

Breach Response

Organisations need to describe, in clear and plain language, the nature of the personal data breach and, at least:

- Provide the name and contact details of any data protection officer employed, or other contact point where more information can be obtained
- Give a description of the likely consequences of the personal data breach; and
- Give a description of the measures taken or proposed to deal with the personal data breach and, where appropriate, a description of the measures taken to mitigate any possible adverse effects

Organisations should also give specific and clear advice to individuals on the steps they can take to protect themselves, and what the organisation is willing to do to help them. Depending on the circumstances, this may include such things as:

- Forcing a password reset
- Advising individuals to use strong, unique passwords
- Encouraging individuals to look out for phishing emails or fraudulent activity on their accounts

Erasing Data

The regulations are clear that an organisation should set clear limits about data retention.

Organisations:

- Must not keep personal data for longer than needed
- Need to think about – and be able to justify – how long personal data is kept. This will depend on the purposes for holding the data
- Should produce a policy setting standard retention periods wherever possible, to comply with documentation requirements
- Should periodically review the data being held, and erase or anonymise it when it is no longer needed
- Must carefully consider any challenges to the retention of data. Individuals have a right to erasure if the data is no longer needed.
- Can keep personal data for longer if it is only kept for public interest archiving, scientific or historical research, or statistical purposes.

An Individual's Rights

Under the Data Protection Act 2018, individuals have the right to find out what information an organisation stores about them.

Individuals maintain the right to:

- Be informed about how their data is being used
- Access personal data
- Have incorrect data updated
- Have data erased
- Stop or restrict the processing of their data
- Data portability
- Object to how their data is processed in certain circumstances

Liability

Not only could an organisation be fined under data protection law, but an entitlement is also created for the individual to take their case to court to:

- Enforce their rights under data protection law if they believe those rights have been breached
- Claim compensation for any damage caused by any organisation if they have broken data protection law, including any distress they may have suffered

If the person can credibly prove that they have suffered loss or harm because of their personal data being breached (such as experiencing depression) then they may be able to claim more compensation. The court would require evidence that the suffering and loss has occurred. The values involved in any claim will in any event be unlikely to exceed the self-insured retention of an organisation.

Review

Any prudent and responsible organisation will regularly review their GDPR arrangements to make sure that they are doing everything they can to comply with the requirements placed upon them with a view to reducing the potential for a data breach occurring.

References

1. The Data Protection Act 2018
2. The GDPR Regulations
3. ICO Data Security Incident Trends

Further information

For access to further RMP Resources you may find helpful in reducing your organisation's cost of risk, please access the RMP Resources or RMP Articles pages on our website. To join the debate follow us on our LinkedIn page.

Get in touch

For more information, please contact your broker, RMP risk control consultant or account director.

contact@rmpartners.co.uk

Risk Management Partners

The Walbrook Building
25 Walbrook
London EC4N 8AW

020 7204 1800
rmpartners.co.uk

FP396-2025