Data Security Breach Action Plan

Assemble the security breach team

- Dealing with a breach quickly can limit the potential damage that it causes.
- Put in place a security breach management team or appoint / task appropriate staff / senior management (SB Team) and nominate deputies (as appropriate).
- **Data controllers** dealing with **personal data** security breach incidents may need input from specialists to the size of the business. These specialists may be derived from areas such as Human Resources, IT, security (IT and physical) as well as legal and compliance officers. If necessary, contact with external stakeholders and suppliers may also be required.
- The SB Team should include at least one senior officer, so that decisions can be made and acted on swiftly. Senior level ownership of information is a key factor in success, demonstrates the importance of the issue and is critical in obtaining resource.
- Members of the SB Team should be aware of any sector-specific guidance on the actions to take in the event of a data security breach.

Investigate the facts

The data security breach should be investigated to determine:

- The nature and cause of the breach.
- The extent of the damage or harm that results or could result from the breach.

Stop or mitigate the breach

- Take action to stop the data security breach from continuing or recurring and mitigate the harm that may continue to result from the breach.
- If the ICO is notified or becomes involved in a data security breach, he will want to know what has been done to stop or mitigate the breach and what the data controller will do to ensure future compliance with Principle 7 of the Data Protection Act 1998 (DPA) (Security Principle).

Data controller(s)

- Determine the identity of the data controller for the purpose of the data security breach. The data controller is the party that determines the purpose for, and manner in which, personal data is processed.
- There may be more than one data controller, particularly where, for example, **shared services** are involved.
- Where there is more than one data controller, both parties may be liable for breach of the Security Principle.

Consider who needs to be notified

The data controller will need to consider which parties should be notified. These could include:

- **The ICO**. There is no express obligation in the DPA to notify the ICO in the event of a data security breach. However, the Information Commissioner believes that serious breaches should be brought to the attention of the ICO, so that the nature of the breach or loss can then be considered, together with whether the data controller is properly meeting his or her responsibilities under the DPA.
- The term "**serious breaches**" is not defined, but this ICO guidance gives some high level examples of what would or would not constitute a serious breach. Such instances include situations where:
  - A large volume of personal data is involved and there is a real risk of individuals suffering some harm.
  - The breach concerns information that, if released, could cause a significant risk of individuals suffering substantial detriment, including considerable distress. This is most likely to be the case where that data is **sensitive personal data**.
- **Sensitive Personal Data** is data consisting of information about the data subject's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life, or commission of or proceedings for any offence committed or alleged to have been committed by the data subject.
- **Determine if there are any legal or contractual notification requirements.**
- **Other data controllers.** If there are other data controllers of the personal data in question, you may want to notify them (although this is not a legal obligation under the DPA).

- **Insurers.** Notification of potential claims may be an insurance policy requirement.
- **Data subjects.** In the Breach Management Guidance, the ICO cautions against the dangers of "over notifying" **data subjects**, since not every incident will automatically warrant notification and this may well cause a disproportionate level of enquiries and increase in workload. Data controllers should instead consider how notification could help the individual by allowing individuals to act on the information to mitigate risks, for example by cancelling a credit card or changing a password. Data controllers may wish to consider providing data subjects whose personal data security is at risk with assistance in dealing with practical issues, such as identity fraud checking services. The Breach Management Guidance urges organisations to consider which is the most appropriate way to notify affected data subjects, bearing in mind the security of the medium as well as the urgency of the situation. If notifying, the notification should at the very least include a description of how and when the breach occurred and which data was involved. Details of actions the organisation has already taken to respond to the risks posed by the breach should also be included.

Check the contract

- Consider whether the data security breach has been caused by another data controller (for example, where personal data has been made available to another data controller for the purposes of joined up or shared services) or whether it has been caused by a **data processor**. If so, consider whether there are contract terms in place.
- Where the data security breach has been caused by a data processor, contractual issues / remedies may arise, in particular:
  - Are the data protection and data security obligations in the contract appropriate for the purposes of compliance with the Security Principle?
  - Does the data controller have a claim or any liability for breach of a specific data protection or security obligation?
  - In the absence of any specific data security provisions, consider whether there may be a claim or any liability for breach of confidence or a failure to take reasonable skill and care.
  - Does the breach give rise to a right to claim damages? If so, is the value of the claim limited by the contractual limit of liability? Many contracts carve out claims for loss of data and damage to reputation from the limitation and exclusions of liability provisions.
  - How will the claim for damages be quantified? Will liquidated damages be payable or will a party be granted service credits? Are the costs incurred as a result of the breach recoverable? Is the data controller able to pass on any liability?
  - Does the breach give rise to a right to terminate the contract? In many contracts the breach of data security clauses will give rise to an express right to terminate.
  - In the absence of an express right to terminate, consider whether the breach is sufficiently serious to give rise to the right to terminate the contract at common law for repudiatory breach. Whether such a right can be exercised will depend upon how serious the security breach is and its impact upon the parties' ability to continue to perform their contractual obligations.
  - Does the data security breach trigger any other aspects of the contract, such as audit rights or the implementation of business continuity and disaster recovery plans?
  - Are there are any specific contractual administration matters that need to be observed to preserve rights, such as compliance with notice provisions or prescribed alternative dispute resolution procedures?

Does disciplinary action need to be taken?

- Data controllers will need to review the actions of employees who cause data security breaches and then decide whether disciplinary action is appropriate. This will involve consideration of:
  - Any constitutional requirements of the organisation or any statutory requirements that may affect the way that the disciplinary process is conducted.
  - The organisation's own disciplinary policies and other relevant policies, such as data protection policies, IT and internet use policy and security policies. This will allow determination of the extent to which the employee has breached their express contractual provisions.
  - Whether the employee had received adequate training and guidance on data protection and security responsibilities and ought reasonably to have been aware of the employer's expectations and the consequences of breaching them.
  - Whether there has been any breach of statute that could justify immediate suspension or summary dismissal. Where disciplinary action is appropriate, this must be conducted in accordance with the statutory dismissal and disciplinary procedures and the organisation's own disciplinary procedure.

Audit of security appropriateness and the need to make necessary improvements

- An investigation should take place and include a review of whether appropriate security policies and procedures were in place and if so, whether they were followed.
- Where one or more data processors may have caused the breach, consider whether adequate contractual obligations were in place to comply with the Security Principle and if so, whether the data processor or processors is or are in breach of contract.
- Where security is found not to be appropriate for the purpose of the Security Principle, consider what action needs to be taken to raise data protection and security compliance standards to those required by the Security Principle. If the ICO is notified or becomes involved in a data security breach, he or she is likely to request this information.