Data Breach Protocol

PLEASE NOTE: this English version is a translation of the original document titled *Datalekprotocol*. It is merely a courtesy translation and does not hold any legal value in its own right.

In the event of a (potential) data breach, the following steps may be taken.

1. **Identifying a potential data breach**

If a (potential) data breach is detected, the board (or the remaining board members) are informed.

2. **Assessing the nature and severity of the incident**

The board investigate the potential data breach to determine whether a data breach has actually occurred. If it has, the information that has been leaked and the severity of the breach are assessed. The following points are taken into account in the assessment:

- Has there been a loss of personal data? That is, does the association no longer hold this data because it has been destroyed or has been lost in some other way?
- Has there been unlawful processing of personal data? This includes the accidental or unlawful destruction, loss or alteration of processed personal data, or unauthorised access to or disclosure of processed personal data.
- Are there any security shortcomings or vulnerabilities?
- Can it be reasonably ruled out that a security breach has led to unlawful processing?
- Has any sensitive personal data been leaked? Examples include:
    - Special categories of personal data as defined in Article 16 of the Personal Data Protection Act (WBP);
    - Data concerning the data subject's financial or economic situation;
    - Data that could lead to prejudice or exclusion of the data subject;
    - Usernames, passwords and/or other login details;
    - Data that could be used for (identity) fraud.
- Do the nature and scale of the breach lead to (a significant risk of) serious adverse consequences? Take into account factors such as:
    - The scale of the processing: does it involve a large amount of personal data per individual and data relating to large groups of data subjects?;
    - The impact of loss or unlawful processing;
    - The sharing of personal data within (hierarchical) chains. This means that the consequences of loss and unauthorised alteration of personal data can affect the entire chain;
    - The involvement of vulnerable groups, for example, people with intellectual disabilities.

3. **If the data breach is serious: notify the Dutch Data Protection Authority**

If the data breach is serious, there may be an obligation to report it to the Dutch Data Protection Authority (*Authoriteit Persoonsgegevens, or AP*) within 72 hours. If such is the case, the AP will be notified. Plans to close the breach and inform those whose data was involved will then be drawn up

based on that notification. This will involve investigating how the data breach could have occurred, if this was not already known.

4. Notifying the data subject(s)

The board will assess whether the data subject(s) should be informed of the data breach. If this is the case, the board will contact them. Whether the data subject(s) should be informed depends on the following factors:

- If the association has taken appropriate technical safeguards, rendering the personal data in question unintelligible or inaccessible to anyone who is not entitled to access the data, then report to the data subject(s) may be omitted (Section 34a(6) of the WBP). In case of doubt, the data breach must be reported.
- The data breach must be reported to the data subject(s) if the breach is likely to have adverse consequences for their privacy (Section 34a(2) of the WBP).
- Report to the data subject(s) may be omitted if there are compelling reasons for doing so (Section 43 of the WBP). However, report to the data subject(s) may only be omitted if this is necessary in view of the interests referred to in this Article. Pursuant to Article 43(e) of the WBP, report to the data subject may be omitted to the extent that this is necessary in the interests of protecting the data subject(s).

5. Devising and implementing improvement measures

Following the data breach, the board will draw up improvement measures to prevent a similar situation from occurring. These will therefore be implemented as soon as possible, whilst all other potential data breaches are also investigated and rectified.

Possible improvement measures to prevent a data breach include:

- Carrying out an internal clean-up. For example, delete emails or files that are no longer needed and clean up address books, as these often contain personal data. This prevents a data breach from affecting an unnecessarily large amount of personal data. When deleting personal data, check whether this data is still present in a backup. If so, delete the data from the backup as well.
- Setting ‘send in bcc’ as the default option for sending emails in email programs. This reduces the risk of a data breach caused by accidentally making the email addresses in a group email visible to everyone.
- Ensuring that personal data can only be accessed by authorised persons. Keep a close eye on who has access to personal data and check periodically for unauthorised access.
- Changing passwords regularly. Store passwords in a secure location to which only the appropriate persons have access.

6. End

This concludes the data breach protocol. Every data breach is recorded in the relevant register. Should another (potential) data breach occur, the protocol is restarted.

7. **Further information?**

Visit Data breach? This is what you have to do | Autoriteit Persoonsgegevens for more information on what to do in the event of a data breach.

This document was last updated on 12-08-2026