Learning from previous data breaches (Plan-Do-Check-Act)

It is important that organisations do not regard maintaining the data breach register as a mere administrative obligation, but also as a means of learning from previous incidents. The AP provides an example of a step-by-step plan that organisations can periodically implement as part of the Plan-Do-Check-Act (PDCA) cycle. They can use this step-by-step plan to monitor whether (certain types of) data breaches are increasing, what the possible causes are, whether previous measures to reduce the number of data breaches have worked and whether additional measures are needed. This allows organisations to continuously evaluate and improve the security of personal data.

STEP 1: Make an analysis based on the data breach register

- How many data breaches have occurred in the past period?
- What type of data breaches did it involve? What type of data breaches are most common?
- Which type of data breach poses the highest risk to victims?

Compare with previous periods: are there any notable trends emerging?

- Has the number of (serious) data breaches risen or fallen?
- Has the number of data breaches reported to the AP and to victims increased in the recent period?
- Can you see an increase or decrease in certain types of data breaches?
- What is the possible cause of the increase or decrease?

Note: an increase or decrease in the number of (reported) data breaches may also be caused by the fact that more or fewer data breaches have been reported/registered internally in the past period than before.

STEP 2: Check what measures you can take to limit the risk of the most serious and/or common data breaches

Prioritise mitigation measures aimed at data breaches that pose the highest risk and relatively easy-to-implement measures that are likely to have an immediate effect ('low-hanging fruit').

STEP 3: Monitor the implementation of the proposed (additional) security measures

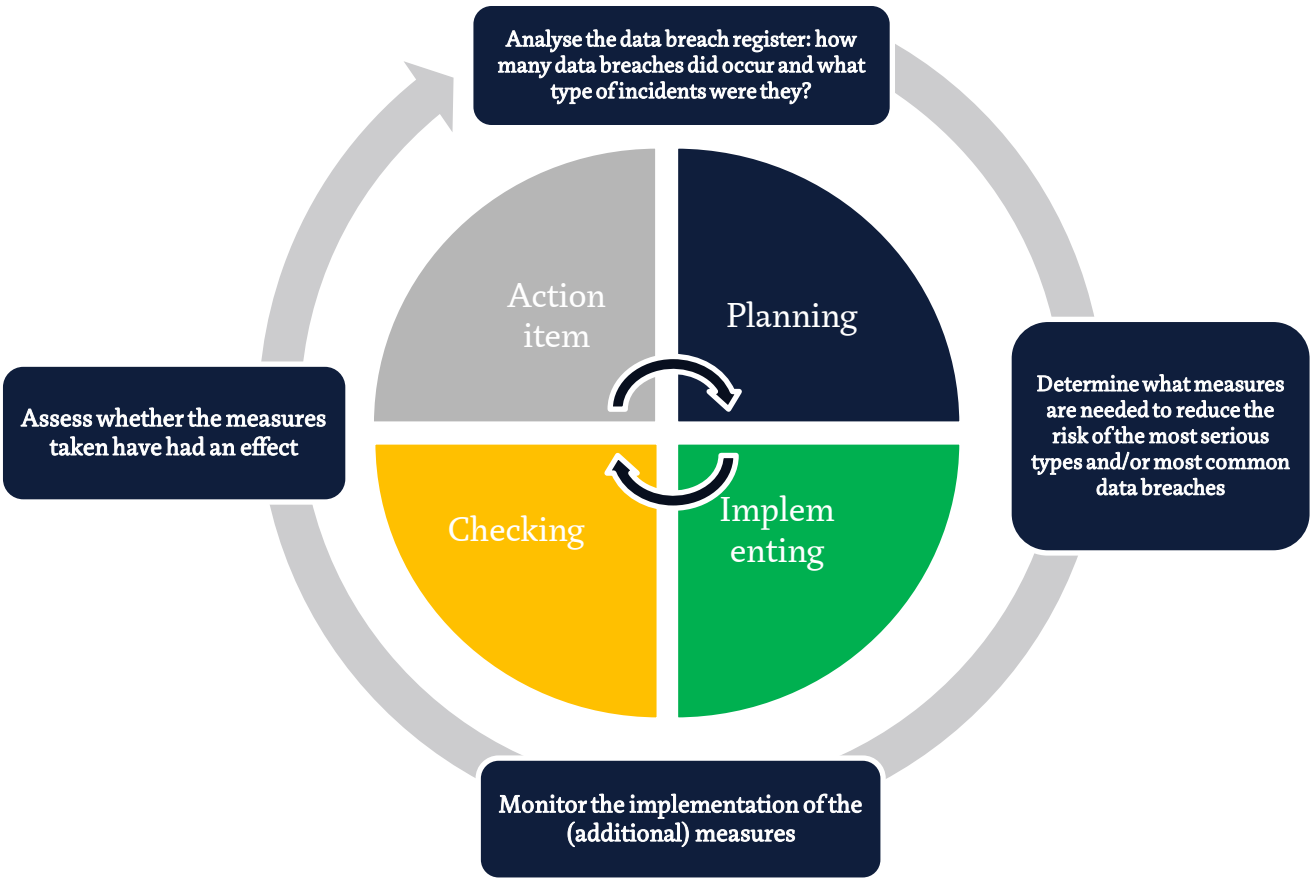
- Have the announced measures from the previous cycle been implemented?
- If not, why so? When will these measures be implemented?

Have the proposed security measures not been implemented within the agreed period? Hold the responsible management to account for this and enter into agreements about it.

STEP 4: Assess (say after six months) whether the additional measures taken have had an effect

- Have the measures introduced during the previous cycle led to a reduction in the number of data breaches (of a certain type)?
- If the measures have not proven effective, what was the reason for this? Are additional measures necessary?

Repeat steps 1 to 4 every 6 to 12 months and report to senior management.
The AP recommends involving the DPO and the CISO in the implementation of these steps.


Analyse the data breach register: how many data breaches did occur and what type of incidents were they?
Action item
Planning
Determine what measures are needed to reduce the risk of the most serious types and/or most common data breaches
Checking
Implem enting
Assess whether the measures taken have had an effect
Monitor the implementation of the (additional) measures