AP

Handling of data breaches in youth care

Looking after youth care patients also means protecting their personal data

Summary

The Autoriteit Persoonsgegevens (AP), the Dutch data protection authority, has conducted an investigation into (the handling of) data breaches in youth care. With this investigation, the AP wants to draw attention within the Youth Care sector to the importance of carefully reporting and registering data breaches. The basic principle is that if data breaches are handled carefully and lessons are learned from previous incidents, the protection of personal data of youth care patients can be structurally improved. At the same time, the AP wants to accommodate youth care centres with recommendations, thus giving them concrete tools to raise the protection of personal data within their respective organisations to a higher level.

The investigation by the AP demonstrates, among other things, that all centres that were investigated have drawn up an internal reporting policy for data breaches. In most cases, this policy is also actively brought to the attention of employees. All centres do also have an internal data breach register. However, in about half of all cases this register is not complete. In addition, one in three of all centres investigated does not (yet) have plans for improvement to tackle recurring data breaches. This creates the risk that these centres will not take important additional security measures (in time) and that similar recurring data breaches will arise in the future, causing youth care patients to be unnecessarily exposed to the risk of their personal data falling into the wrong hands.

Recommendations from the AP

It is important that youth care centres do not view maintaining a data breach register solely as an administrative obligation, but primarily as a means of learning from previous incidents and preventing those in the future. Centres can use the data breach register to reflect on past mistakes, assess the effectiveness of security measures and implement improvements where necessary. The register can therefore make an important contribution to realising better protection of personal data.

Following the investigation, the AP comes up with the following recommendations:

- Learn from previous data breaches, create an improvement plan and include it in the PDCA cycle

Use every data breach to improve your processes. Carefully analyse what went wrong, identify the causes and implement concrete measures to prevent recurrence. Also record these measures in the data breach register, so that you can periodically evaluate their effectiveness.

Make this evaluation part of the Plan-Do-Check-Act (PDCA) cycle. If your organisation already has an internal procedure for handling incidents and emergencies, you can align the handling of data breaches with the general process or method for improvement following an incident. This enables you to not only handle incidents, but also structurally strengthen your security strategy and risk management in the long term.

Example of PDCA cycle for data breaches

As an appendix to this report, the AP has added an example of a step-by-step plan that can be carried out periodically as part of the PDCA cycle. You can use this step-by-step plan to track 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 you to continuously evaluate and improve the security of personal data.

- Always involve the DPO in the handling of data breaches

Ensure that the Data Protection Officer (DPO) is always closely involved in the handling of data breaches from the outset. The DPO is vital in monitoring compliance with the privacy rules and plays an advisory and supervisory role therein.

Therefore, involve the DPO so that he or she can provide advice, and then let the board, as the party ultimately responsible, decide whether a data breach should be reported to the AP and the victims of the data breach (the data subjects whose personal data has been compromised).

- Make sure you can demonstrate that data breaches have been handled adequately

Make sure that you clearly record the following in the data breach register: (1) what exactly happened; (2) what the consequences are for the victims; and (3) what measures you have taken following the data breach. This provides transparency about the steps that have been taken. This in turn ensures that both internal and external stakeholders can see whether a data breach has been properly sealed and whether there are any further risks. In any case, state the following: the cause of the data breach, what exactly happened, which group(s) of people was or were affected and what type of personal data is involved. This allows you to subsequently check whether a proper risk assessment was made and whether informing the victims or not was the correct decision.

Example of a data breach register

To help organisations properly maintain a data breach register, the AP has created an example of a data breach register. This example can be downloaded from the AP website. All organisations can use this example, including organisations operating outside the Youth Care sector. See our website: Voorbeeld-datalekregister (in Dutch).

- Make sure employees know what a data breach is and how to act

Well-informed employees can respond to incidents better. Therefore, pay attention to the topic of data breaches when onboarding new employees, discuss/evaluate data breaches within the team in which they occur and regularly organise (mandatory) training courses, workshops and awareness campaigns.

1. Introduction

1.1 Reason for the investigation

In 2019 and 2020, several major data breaches occurred within the Youth Care sector in the Netherlands. These data breaches led to Parliamentary questions[1] and an investigation by the Health and Youth Care Inspectorate (IGJ)[2]. The main conclusion of this investigation was that knowledge of IT and information security in youth care remains wanting, which in turn means a lack of insight into the risks. The IGJ further found that the sector does not have sufficient funds. In recent years, youth care has been a regular topic in the news media due to financial issues. More than 40 percent of youth care centres made a loss in 2022.[3] In addition, Statistics Netherlands (CBS) found that in 2022, no less than 50 percent of youth care workers experienced '(much) too high a workload'.[4] These circumstances contribute to the risk of data breaches at youth care centres.

In order for youth care to be effective, it is important that young people who receive youth care (hereinafter referred to as youth care patients) can trust that the (sensitive) personal data that they have provided to the youth care centres is handled with due care, as well as that youth care workers do not breach their legal duty of confidentiality. Data breaches in youth care can damage this trust. This may lead to youth care patients becoming reluctant to share sensitive information about their private situation with youth care centres. This in turn impedes the implementation of youth care. In addition, data breaches in youth care can lead to significant emotional damage for those affected. After all, a large part of personal data of vulnerable minors processed in this sector is sensitive data.

1.2 Purpose of the investigation

Autoriteit Persoonsgegevens (AP) decided to conduct an exploratory investigation into (the handling of) data breaches within the Youth Care sector. The investigation aimed to gain more insight into how 'GDPR mature' this sector is in terms of dealing with data breaches and to make recommendations and provide examples based on the insights obtained during the investigation. In doing so, the AP seeks to encourage youth care centres to properly protect the personal data of youth care patients and that they report data breaches to the AP and the victims of the data breach (the data subjects whose personal data has been compromised) when necessary. Informing the victims is important because it enables them to protect themselves against the adverse effects of the data breach. Transparency about data breaches is also important for the trust of youth care patients in the careful handling of their personal data.

1.3 Method of the investigation

The investigation was conducted by analysing information and documentation requested from fifteen selected youth care centres, including:

- the data breach register;
- the internal reporting policy for security incidents;
- information about general technical or organisational measures that the centre takes to limit the risk of data breaches;
- information about measures the centre takes to ensure that employees know how to carefully handle data breaches, including how to report security incidents internally.

[1] https://www.tweedekamer.nl/debat_en_vergadering/plenaire_vergaderingen/details/activiteit?id=2019A01711
[2] https://www.igj.nl/publicaties/publicaties/2020/06/18/extra-aandacht-nodig-voor-ict-in-de-jeugdzorg
[3] https://www.jeugdzorgnederland.nl/actueel/zorgbarometer-seinen-voor-jeugdzorg-op-rood/
[4] https://www.cbs.nl/nl-nl/nieuws/2022/46/helft-zorgwerknemers-vindt-werkdruk-te-hoog

Selection procedure

The fifteen youth care centres that were contacted were selected based on size[5] and the number of data breach reports they have made to the AP since 1 January 2020. The AP mainly selected centres that, given their size, made relatively few data breach reports. Centres where the AP identified many points of attention were invited for an interview. This occurred in three cases. The AP entered into agreements with these centres to improve a number of issues.

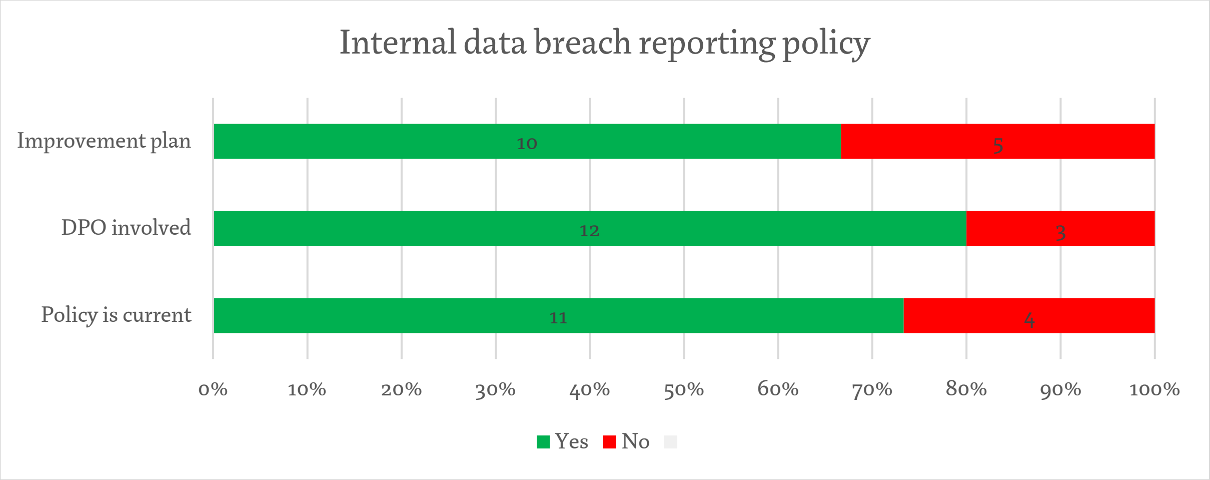
2. Internal reporting policy for data breaches

2.1 Importance of an internal reporting policy

It is important for organisations to have a documented data breach reporting procedure in place that the organisation adheres to once a data breach is discovered. This procedure can also specify how the organisation must contain, manage and recover from the data breach, assess the risk and report the data breach. This way, the organisation ensures that the correct steps are always taken in the event of a data breach. Youth care centres may already have an internal procedure for handling (cyber) incidents[6] and emergencies in place. In those cases the internal data breach reporting policy can be aligned with existing processes. In order to properly implement the reporting policy, it is also important for the employees to be informed of these procedures and that they know how to respond to data breaches, thus enabling them to provide good and privacy-friendly care to their patients.[7]

2.2 Assessment of the internal reporting policy

The AP has asked fifteen youth care centres for their internal policy on registering and reporting data breaches. The findings are shown in this table:



At most centres (ten out of fifteen), implementing improvement measures after a data breach, or investigating them, is already an integral part of the data breach policy. This is not yet the case at five of the fifteen centres. These organisations have not yet learned enough from previous data breaches. This increases the risk of certain types of data breaches reoccurring.

[5] Measured in number of employees and/or number of youth care patients.

[6] See: NEN 7510-2:2017 Chapters 16 and 17 including Appendix C. See also: Guidelines for information security in youth care centres Recommendations for safer IT in youth care, Feature: HB/dd/20-1875a, Chapter 7 "Incident response".

[7] See also: Guidelines 9/2022 on Personal Data Breach Notification under the GDPR, Version 2.0 (hereinafter referred to as Guidelines 9/2022), p. 31.

Recommendation: Learn from previous data breaches and evaluate measures
It is important to learn from previous incidents as much as possible and take measures to reduce the risk of future data breaches occurring. The AP recommends including this in the Plan-Do-Check-Act (PCDA) cycle and reporting to the board at least twice a year on data breaches in the past period. The board paying regular attention to this is important, because this way privacy becomes part of the organisational culture. If your organisation already has an internal procedure for handling incidents and emergencies, you can align the handling of data breaches with this procedure. This allows you to track whether (certain types of) data breaches are increasing, what the possible reasons are, whether previous measures to reduce the number of data breaches worked and whether additional measures are needed. For example, you can delegate this to the Data Protection Officer (DPO) in collaboration with the Chief Information Security Officer (CISO). The DPO and/or the CISO can also use the data breach register to monitor whether proposed improvement measures are implemented in a timely manner. It is important that the data breach register is complete and carefully maintained.

The role of the DPO

Most centres (twelve out of fifteen) actively involve the DPO in the handling of data breaches. The other three centres do not involve the DPO at all, in accordance with their internal policy. In one case, the policy was designed in such a way that the DPO decided whether the centre had to report a data breach to the AP and the victims of the data breach. However, such a role is not compatible with the independent position of the DPO. DPOs cannot properly monitor compliance with the General Data Protection Regulation (GDPR) if they themselves play an active role in the implementation of GDPR obligations, such as the data breach notification obligation. These operational tasks can be assigned to, for example, the Privacy Officer.

Reporting policy is sometimes outdated

Most centres (eleven out of fifteen) also recently evaluated or renewed their internal reporting policy. Four centres have not evaluated or renewed their policies since 2020. The interviews showed that this can lead to the process in practice deviating from the established reporting policy. This in turn can lead to confusion about the allocation of roles, especially when there is a high turnover of staff, which is the case in many youth care centres.

3. Data breach register

3.1 Importance of the data breach register

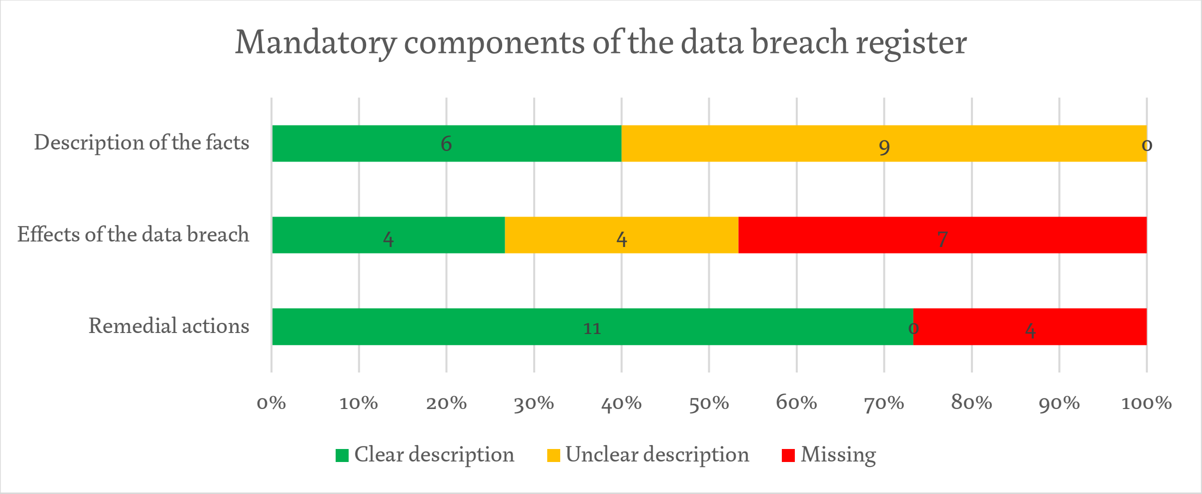
In order to be able to perform analyses that provide a complete picture, it is important to document all data breaches, regardless of whether organisations report a data breach to the AP or not. In addition, it is crucial to better protect youth care patients involved from potential consequences. Moreover, it is part of the duty of accountability under the GDPR.[8] Organisations must record all details of each data breach. This includes the cause, what exactly happened, which personal data is involved, what the consequences of the data breach are and what remedial actions the organisation has taken. This allows organisations to demonstrate that they report data breaches to the AP and to victims when necessary.

However, it is important that organisations do not regard maintaining the data breach register as a mere administrative obligation, but primarily as a means of learning from previous incidents. Organisations can use the data breach register to reflect on past mistakes, assess the effectiveness of security measures and make improvements where necessary. The register can therefore make an important contribution to realising better protection of personal data.

[8] See also: Guidelines 9/2022, p. 30 and 31.

3.2 Data breach register assessment

The AP requested fifteen youth care centres to submit their data breach registers[9] containing all registrations from 1 January 2020 to 30 April 2024. The AP assessed, among other things, whether these data breach registers contained the legally required components: a clear description of the facts relating to the personal data breach, its effects and the remedial action taken. The results are shown in this table:



When assessing the requested data breach registers, a number of things stood out. Some registers contained only very limited information and unclear descriptions. In some cases, these registers were also incomplete and/or did not contain all legally required components, such as the effects of the data breach and the remedial action taken. Since these registers were unclear or incomplete, the AP was unable to properly assess the extent to which the centres concerned report data breaches to the AP and the victims when necessary. Furthermore, the incompleteness of these registers makes it difficult for the centres concerned to properly report on data breaches to stakeholders within the organisation and to evaluate the effectiveness of previous measures.

Description of the facts

The AP came across very short and unclear descriptions of data breaches in various data breach registers. One such example was:

- *"Accidentally emailed documents to the lawyer who was still registered, but has since been replaced by the mother."*

Due to the use of abbreviations and short descriptions of the facts, it is not always clear what type of personal data has been affected. As a result, the centre concerned cannot subsequently determine whether a proper assessment has been made of the seriousness of the data breach and its effects. In addition, the board and/or the AP cannot properly assess (in retrospect) whether a correct risk assessment has been made of the possible consequences of the data breach for the victims, and whether reporting the data breach to the AP and the victims or not was the correct decision.

Description of the effects

In four registers, the AP came across unclear descriptions of the effects of a data breach. For example, reference to a 'negligible risk', 'low risk', 'medium risk', or 'high' risk, without an explanation of why a data breach falls into a particular risk category. If the consequences of the data breach are not clearly described, the centre concerned cannot subsequently assess whether the appropriate remedial action have been

[9] This concerns the documentation as referred to in Article 33, paragraph 5 of the GDPR.

taken. This in turn means that the AP cannot properly assess in retrospect whether the decision to report the data breach to the AP and the victims was correct.
Furthermore, in seven out of the fifteen data breach registers, the consequences of the data breach are not described separately. Although in some cases the consequences of the data breach could be deduced from the description of the incident. However, it is important to record the consequences of the data breach separately in the data breach register, as prescribed by the GDPR. The same violation can have more serious consequences in one situation than in another.

Remedial action

In four out of the fifteen data breach registers, remedial actions were not recorded. Some centres only recorded the preventive measures taken to prevent future data breaches, but did not state whether the data breach ended and, if so, how. As a result, the centre (and the AP) cannot properly assess in retrospect whether enough has been done to limit the negative consequences for the victims. It is therefore unclear whether the data breach is still ongoing or has already ended. For example, in the case of a postal item having been sent incorrectly, it would be unclear whether the letter was destroyed or returned by the incorrect recipient, and therefore whether the violation has ended or is still ongoing.

Recommendation: Ensure data breach registrations are clear and complete
In order to properly handle data breaches, and to be able to demonstrate this, it is important that your data breach register contains at least the legally required components: a clear description of the facts, the effects of the data breach and the remedial action taken. Register these components separately. Above all, make sure that the description of a data breach clearly shows what happened. In any case, state the following: the cause of the data breach, what exactly happened, which group(s) of victims was/were affected and what type of personal data is involved. This way you can check in retrospect whether the risk assessment you made was correct.

In addition, the AP advises to also include these components in your data breach register:

- the measures you have taken to prevent new, similar data breaches;
- whether or not you reported the data breach to the AP and the victims;
- why you did or did not report the data breach to the AP and the victims;
- if you reported a data breach to the AP too late: why this is the case.
- In addition, it is important to regularly analyse the register and report to the board at least twice a year about the data breaches in the past period.

Example of a data breach register
To help organisations get started, the AP has created an example of a data breach register.
This example can be downloaded from the AP website:
https://autoriteitpersoonsgegevens.nl/documenten/voorbeeld-datalekregister

3.3 Bad practices

At several of the youth care centres investigated the AP identified two bad practices.

Data breach register also contains other types of incidents

A number of centres use one register for different types of incidents. In this register they also record security incidents other than data breaches, such as physical incidents and incidents that do not involve personal data. This makes it more difficult to establish how many data breaches occurred at the relevant centre within a certain period. This in turn makes internal and external reporting on data breaches and evaluating the measures taken more difficult.

The AP therefore recommends that data breaches must always be recorded in a separate, dedicated register (as well).

Inappropriate software systems used as data breach register

A number of centres used separate systems for recording reports of incidents, including data breaches. These are systems that are designed to manage and process notifications ('tickets'). Some centres also used these systems as an internal data breach register, even though the systems are not properly set up for this. During the investigation, the AP found that these centres experience difficulty exporting data breach registrations from these systems and submitting them to the AP. These exports further contain a lot of unnecessary information, such as the personal data of the initial person reporting the data breach and the names of the employees who handled the report. This makes it difficult for the relevant centres to obtain a clear overview of the type and number of data breaches occurring within the centre and to assess the effectiveness of the measures taken.

The AP therefore recommends using a separate system or overview for registering data breaches, i.e. one that is easily searchable and easy to export. Alternatively, it is possible to opt for a system that can be linked to the existing processing register, so that it is easy to determine which processing involved the data breach and what consequences the data breach may have (which types of personal data and groups of data subjects are affected).

3.4 Other notable matters

In addition to the bad practices mentioned, the AP noticed several other things.

More data breaches reported to the AP than recorded in the data breach register

At five youth care centres, the number of data breaches reported to the AP according to the data breach register did not correspond with the number of reports actually received by the AP. All these centres reported more data breaches to the AP than they had recorded in their registers. Furthermore, a number of reports received by the AP could not be found in the data breach register of the centre concerned. If organisations do report data breaches to the AP, but fail to register them in their own data breach register, they will not be able to properly check in retrospect whether improvement measures have been taken. Nor will they be able to properly report on the number of data breaches in a specific period based on the register.

Common type of data breach: emails and postal items sent incorrectly

A letter or email containing personal data that ends up with the wrong recipient is a common data breach at youth care centres. For example, a file is accidentally emailed to the wrong person, or a letter is sent to the wrong address because a change of address was not recorded properly. In the case of such types of data breaches occurring, it is important to specify the consequences for the victims in the register, because the consequences can vary greatly from situation to situation. Furthermore, it is important to keep track of how future incidents are prevented.

The AP recommends considering the following, among others:

- Is handing over sensitive documents in person instead of sending them by post or email an option?
- If the document needs to be sent digitally: can a secure email system or a secure online portal be used instead?

4. Security measures and awareness

4.1 Security measures

All centres that the AP investigated have software for sending secure emails. However, due to human error, employees still send emails incorrectly. The interviews show that this is sometimes because employees find the secure email systems impractical and therefore do not (always) use them. When secure email systems or online portals are user-friendly, it will be easier and more accessible for employees to use them.

4.2 Employee awareness

A number of centres are not yet doing enough to make employees aware of the importance of compliance with the GDPR. Data breaches must be prevented as much as possible. And if data breaches occur, it must be possible to recognise them and handle them with due care. Some centres only pay attention to this topic during the onboarding of new employees (for example with a privacy checklist), but do not organise additional training or awareness sessions thereafter. However, repetition of this theme is important given the level of staff turnover.

Do employees not know how to recognise a data breach? And are they not aware of the internal reporting policy? If so, it creates the risk of data breaches going unnoticed and not being reported and recorded internally. Consequently, centres run the risk of failing to report data breaches, whereas victims and the AP should have been notified. Do centres wrongly fail to report data breaches to the AP? In that case, the AP will not be able to check whether the victims have been properly notified and whether the remedial actions taken are effective.

Recommendation: Pay attention to raising awareness among employees

Make sure your employees know what a data breach is and what they should do when they discover or cause a data breach. This prevents data breaches from going unnoticed and not being reported and recorded internally. Only a complete register allows for all data breaches to be analysed, which in turn can improve the protection of personal data of youth care patients. Looking after youth care patients also means protecting their personal data. If not all data breaches are reported and registered internally, you run the risk of wrongly failing to report data breaches to victims and the AP. And as such you run the risk of violating the GDPR. Pay attention to this when onboarding new employees, discuss/evaluate data breaches within the team in which they occur and regularly organise training courses, workshops and awareness campaigns. It is important to not only draw attention to this in case of new employees, but to continue to repeat this theme. For example, in the form of mandatory annual e-learning sessions.

APPENDIX - 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

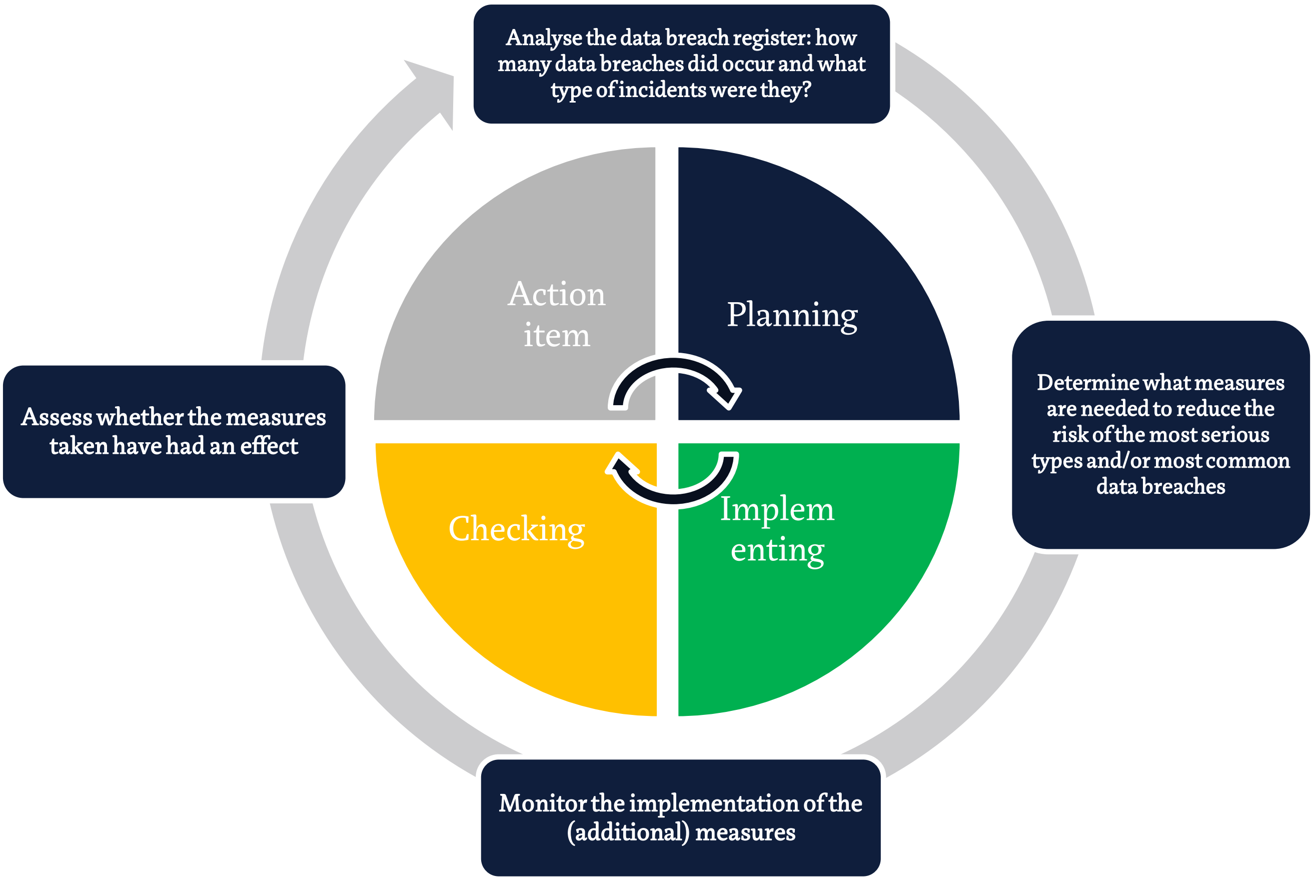
- Have the announced measures from the previous cycle been implemented?
- If not, why so? When will these measures be implemented?

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?

Determine what measures are needed to reduce the risk of the most serious types and/or most common data breaches

Monitor the implementation of the (additional) measures

Assess whether the measures taken have had an effect