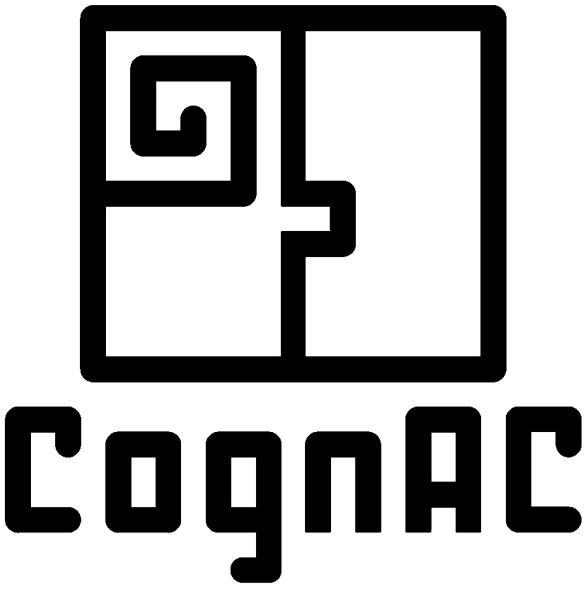


Study Association CognAC

Data Leak Protocol

Established on 5th February of 2019
Altered on 11th of June 2019

1 Introduction

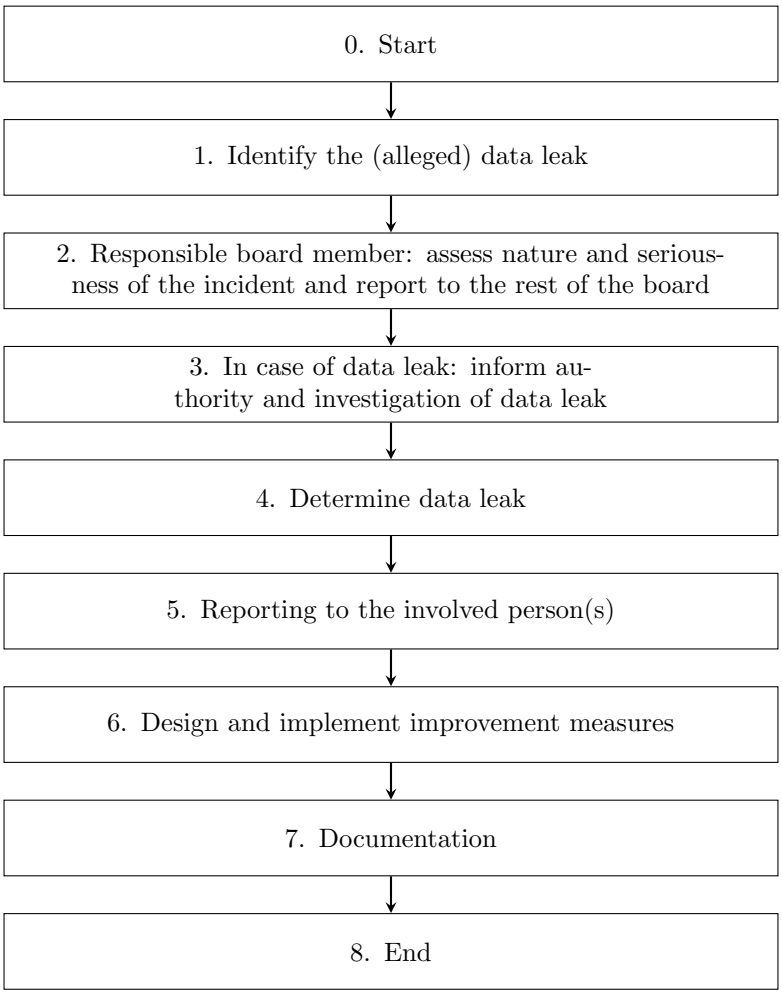
This document specifies the protocol that will be followed when a data leak occurs and which steps will be taken. Since the 1st of January 2016, the Dutch Personal Data Protection Act (Wbp) obliges to report data leaks. This duty to report applies to both the involved person(s) and the Radboud University in Nijmegen.

The study association can determine for each data leak whether the procedure has to be followed completely or whether it can be deviated from. The purpose of this procedure is to establish which steps are recommended by the study association when there is suspicion or knowledge of an incident that could be considered a data leak. Following the below mentioned protocol intends to pursuit the following goals:

- The followed procedure is clear, transparent and unambiguous.
- The interests of the study association, individuals or another organisation that is involved in the incident are being carefully safeguarded.
- The incident is analysed in a careful and systematic way, such that possible risks become visible in the process. The central goal is the determination of deficiencies in (the application of) technical and organisational security measures, which (allegedly) could have led to the incident.
- Promoting that appropriate improvement measures are taken and structurally guaranteeing these improvement measures.
- The appointment of a board member responsible for data leaks and an institution that can be approached when discovering a(n) (alleged) data leak. For example, a privacy coordinator from Radboud University.

2 The Protocol

When there is a(n) (alleged) data leak, then the following diagram can be used. After the diagram, an explanation will be given for the relevant steps.



1. **Identify the (alleged) data leak**

   If a(n) (alleged) data leak is detected, the rest of the board and the chair of the WebC will be informed. The board member responsible for data leaks determines whether they accept the problem alone or involves another board member (or possibly a former administrator/active member) in the process.

2. **Responsible board member: assess nature and seriousness of the incident and report to the rest of the board**

   The board responsible (and any other help) will investigate the alleged data leak to see if a data leak actually occurred. If it occurred, the information that has been leaked and the severity of the data leak will be examined. The board member reports the result to the rest of the board. The following points have to be considered in the assessment:

- Is there a loss of personal data: this means that the study association no longer has the data, because it has been destroyed or has been lost in another way;
- Is there unlawful processing of personal data: this includes the unintentional or unlawful destruction, loss or alteration of processed personal data, or unauthorised access to processed personal data or provision thereof;
- Is there a single shortcoming or vulnerability in security;
- Can it be reasonably ruled out that the data leak has resulted in unlawful processing;
- Has personal data of sensitive nature been leaked;
  - special personal data in accordance with Article 9 of the AVG (GDPR);
  - information on the financial or economic situation of the person concerned;
  - data that may lead to stigmatisation or exclusion of the person concerned;
  - usernames, passwords and other log-in data;
  - data that can be used for (identity) fraud;
- The nature and extent of the infringement can lead to (a considerable chance of) serious adverse consequences; consider factors such as:
  - the extent of the processing; it involves a lot of personal data per person, and data from large groups of persons
  - the impact of loss or unlawful processing;
  - the sharing of personal data within chains: this means that the consequences of loss and unauthorised modification of personal data can occur throughout the chain;
  - involvement of vulnerable groups: think of mentally disabled people.

3. **In case of data leak: inform designated authority and investigate data leak**

   The authority of personal information (Autoriteit persoonsgegevens) will be informed within 72 hours to make a plan. It is investigated how the data leak could have occurred if this was not yet known. If the report is made after 72 hours, it must be provided with a motivation for the delay.

4. **Determine data leak**

   After consultation with the authority of personal information (Autoriteit persoonsgegevens), research into the data leak will be completed and the entire board will consider follow-up plans for this incident.

5. **Reporting to the involved person(s)**

   The board takes the assessment whether it is necessary to inform the involved person(s) about the data leak. If this is the case, the responsible board member contacts them. Whether the person(s) concerned should be informed depends on the following points:

   - If the association has taken appropriate technical protection measures, as a result of which the personal data in question is incomprehensible or inaccessible for anyone who is not entitled to access the data, then the notification to the data person(s) may be omitted. In case of doubt, the data leak must be reported.
   - If the association has taken measures afterwards that prevent the expected risk, then the notification to the concerned person(s) may be omitted.

- If informing the concerned persons would require disproportionate effort, then general, public communication suffices, whereby the concerned person(s) will be informed equally effectively.
- The data leak must be reported to the concerned person(s), if the infringement is likely to have adverse consequences for their privacy.

6. **Design and implement improvement measures** As a result of the data leak, the board draws up improvement measures to prevent a similar situation from happening in the future. These are then introduced as soon as possible and all other possible data leaks are also investigated and remedied.

7. **Documentation** After completion of the above steps, the data leak must be documented. This documentation has to be stored next to all other board documents. It is necessary to state at least the nature of the data leak, the course of events and the reasons why certain decisions were made.