Data breach protocol for V.C.M.W. Sigma

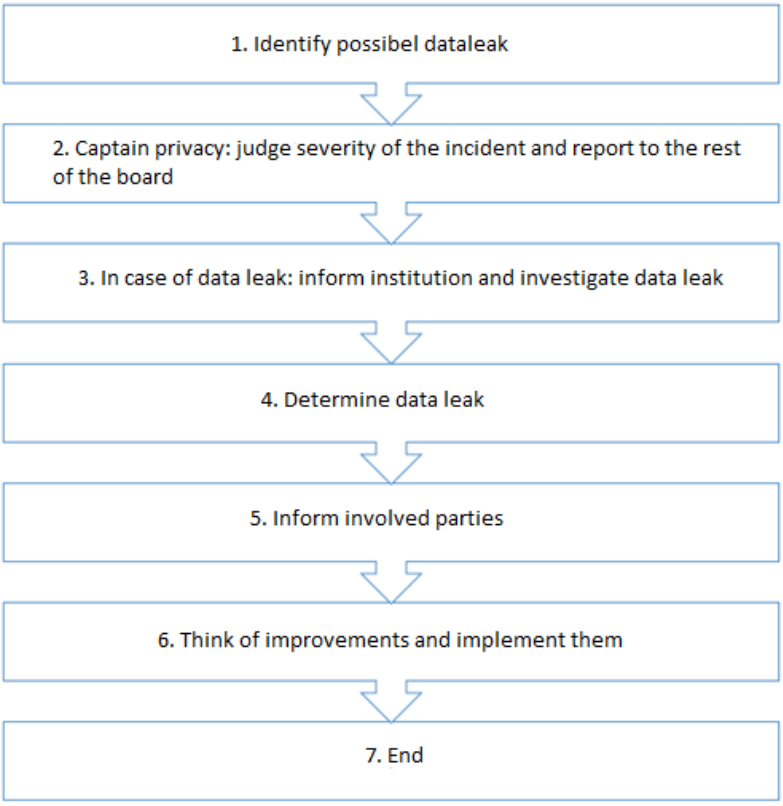
This document contains the protocol for what to do when there is a data breach within the association, and which steps you should take. Since the 1st of January 2016, for the General Data Protection Regulation, you're obligated to report all data breaches. This applies for every person involved, as well as the Radboud University Nijmegen.

V.C.M.W. Sigma can determine per data breach whether the protocol should be followed completely, or you can divulge. The goal of this procedure is to determine which steps should be taken at Sigma in the event of a suspicion or knowledge of an incident that (possibly) could be a data breach. With this we hope to achieve the following result:

- Following the same, clear procedure.
- Thoroughly protect the interests of the association, the individual or other organization involved in the incident that might be a data breach.
- Carefully and systematically analyse the incident that might be a data breach, so that the present risks in the process can be identified. The most important thing is to identify the imperfections in the technical and organizational security measures, that possibly lead to the incident.
- Stimulate taking appropriate improvements and implementing these structurally.
- Indicate a responsible board member for data breaches (captain privacy) and indicate the institution to go to when discovering a possible data breach. Keep the privacy coordinator in of the RU in mind.

What to do with a data breach

When dealing with a possible data breach, the following scheme should be used (after the scheme, every step will be explained in detail.)



1. Identify possible data leak

When a (possible) data breach is found, the (rest of) the board must be notified. Captain privacy then determines if he/she will handle it alone or ask for the help of another board member or active member.

2. Captain privacy: judge the severity of the incident and report to the rest of the board

Captain privacy (and possibly other help) research the data breach to see if it's really a data breach. If this is the case, they look at the information that is leaked and the severity. Captain privacy reports the results to the board. Take the following things into account with your judgement:

- Are you dealing with the loss or personal data; this means the association does not have them anymore, because they have been destroyed or got lost some other way;
- Are you dealing with unlawful processing of personal data; this includes accidental or unlawful destruction, loss or editing of processed personal data or unauthorized access to processed personal data, or the supplying thereof;
- Are you dealing with a lack of security measures;
- Can you reasonably exclude that a breach in security lead to the unlawful processing;
- Was sensitive personal information leaked;
  - Special personal data as listed in article 9 of the GDPR (article 16 of the Wbp);
  - Data about the financial or economic situation of the involved person;
  - Data that could lead to stigmatization or exclusion of the involved;
  - Usernames, passwords and other login data;
  - Data that could be used for identity theft;
- Could the size and nature of the data breach lead to severe disadvantageous consequences; think of factors like:
  - The size of the processing; does it concern lots of data per person, or data of large groups;
  - The impact of the loss or unlawful processing;
  - The sharing of personal data through a chain; this means the consequences of the data breach could be felt throughout the entire chain;
  - The involvement of vulnerable groups; think of mentally handicapped people.

3. In case of data breach; inform designated institution and research data breach

The designated institution of the Radboud University will be informed, and together you will make plans. You will research how the data breach could happen, in case this was not known yet. In 2018 the faculty privacy manager of the faculty of Science was Bjorn Bellink, the head of C&CZ. You can contact the university via dpm@science.ru.nl (FNWI) and privacy@ru.nl (central).

4. Determine data breach

After consulting the the designated institution of the RU, the investigation will be finished, and the board will think of what measures to take to improve the situation

5. Report to involved parties

The board judges whether or not involved parties need to be informed about the data breach. When this is the case, captain privacy will contact them. Whether involved parties must be notified depends on the following:

- If the association took fitting technical security measures, that made the leaked data inaccessible or incomprehensible to anyone who should not have access to them, the notification is not obligatory (article 34a, section 6 Wbp). When in doubt, they should be notified.

- Σ The data breach has to be communicated to the involved parties when it has possible disadvantageous consequences on their personal life (article 34, section 2 Wbp).
- Σ Notification is not necessary, if there are substantial reasons for that (article 43 Wbp). This only counts if not notifying them is *necessary* considering the interests mentioned in this article. Based on article 43e Wbp, it is allowed to refrain from notifying the parties if it is considered necessary for the sake of the protection of the involved parties.

6. Think of improvements and implement them.

In response to the data breach, the board makes a list of improvements to prevent a similar situation. These have to be implemented as soon as possible. You then also have to look at other possible data breaches.

7. End

This is the end of the process. Should another data breach occur, the whole procedure will be started again.