Protocol data leak

In this document you will find the protocol to follow when a data leak takes place in your association and which steps you must take.
It is since the 1st of January 2016 recuired to report data leaks following to the Wet bescherming persoonsgegevens (Wbp). This obligation to report such cases applies both to the person (s) as at the Radboud University in Nijmegen.

The study association can determine for each data leak whether the procedure should be fully followed or that there can be deviated from this. The purpose of this procedure is to record which steps should be taken by Study Association Psychology in Nijmegen with the suspicion of, or taking note of, an incident that (possibly) can be considered as a data leak. It is hoped that the following results will be pursued:
Always following an unambiguous procedure.
Careful safeguarding of the interests of the study association, the individual or another organization involved in the incident, being (possibly) data leak.
Analysing an incident in a careful and systematic way, being a possible data leak, so that existing risk moments are visible during the process. The central idea here is that you can determine the imperfections in the (application of) technical and organizational security measures, which (possibly) could have led to the incident.
Promoting the taking of appropriate measures, improve them and structurally guaranteeing these improvement measures.
The appointment of a person within the board who is responsible regarding data leaks and the appointment of an instance you can contact when discovering a (possible) data leak. You can think of by example the privacy coordinator at Radboud University.

Approach to data leak

So when there is a (possible) data leak, the following process diagram can be used (After the schedule an explanation will be described per step).

1. Identify possible data leak
2. Board members judge the seriousness of the incident and let the rest of the board know
3. In case of a data leak: inform the designated organization and investigate the leak
4. Determine the data leak
5. Report the involved ones
6. Think of measures to improve and implement them
7. End

1. Identify possible data leak.

When there is a data leak the rest of the board will be notified. The responsible

one will determine whether he/she will do it alone or will ask for help in the board or older boards.

2.The responsible one will do research the data leak on its seriousness and where it came from.
The board member will then keep the whole board updated. When there really is a data leak the board responsible will check what information has leaked. He/she keeps the board updated during this whole process. During the research of this data leak the next points are important: is the case of loss of personal information; this means that the association lost this information; because it was destroyed or lost in another way; is this a case of unrightful use of personal information; this can be unlawfully destroying information, use of the information, changing the information or giving unauthorized access to information; protocol data leak
Is there a shortage of vulnerability in the security; it can be excluded that there is a case of data leak; when important personal information has been leaked; go to important personal information article 16 Wbp; information including financial or economic situation of the person; information that can lead to stigmatising the person; there logging in information; that can be used for identity fraud: can this leak lead to a big impact; take in account: the size of the process; did a lot of personal information leak per person and information of big groups- the impact of loss or unrightful processing; the sharing of personal information in chains; involvement of a fragile person or handicapped.

3. In case of a data leak; informing instances and investigation of data leak.
The authority of the Radboud University will be informed and based on this plans will be made. Also it is investigated how a data leak happened if this is not known yet.

4. Determine data leak
After consultation with the authority of Radboud University, research into the data leak will be completed and the entire board thinks about follow-up plans for this incident.

5. Reporting to the person (s)
The board decides whether the person (s) concerned should be informed about the data leak, if this is the case, the responsible board member contacts them. If a person is informed should depend on the following points:
If the association has taken appropriate technical protection measures, the personal data that is incomprehensible or inaccessible to anyone who is not entitled to have knowledge of the data, the report to the person (s) concerned may be omitted (Article 34a, paragraph 6, Wbp). In case of doubt about this, the data leak must be reported.
The data leak must be reported to the person (s) concerned if the infringement is likely to have consequences for his personal privacy (Article 34 (2) of the Wbp).
The report to the person (s) concerned may be omitted if there are serious reasons for doing so (Article 43, Wbp). In that case, however, the report may only be omitted by the person concerned if necessary in view of the interests mentioned in this article. On pursuant to Article 43 (e) of the Wbp, the notification may be waived for the person concerned if this is necessary in the interests of protecting the person concerned.

6. Design and implement improvement measures

In response to the data leak, the board draws up improvement measures for a similar situation. These are also introduced a.s.a.p. with all other possible data leaks are investigated and remedied.

7. End

This completes the process surrounding data leaks. If another (possibly) dataleak occurs, then the process is set in motion again.