**SamenwerkingsOverleg Faculteitsverenigingen**
**Heyendaalseweg 141, N-1.280, 6525AJ Nijmegen**
**info@sofv.nl www.sofv.nl**

# Data breach protocol of the association SamenwerkingsOverleg Faculteitsverenigingen

This document contains the protocol for when a data breach occurs in your association and what steps you should take. It has been mandatory since 1 January 2016 by the Personal Data Protection Act (Wbp) to report data breaches. This reporting obligation applies both to the data subject(s) and to Radboud University Nijmegen.

For each data breach, the study association can determine whether the procedure must be followed in full or whether it can be deviated from. The purpose of this procedure is to lay down which steps must be taken by **Study Association X** when it suspects or becomes aware of an incident that (potentially) qualifies as a data breach. With this, it is hoped that the following result will be pursued:

- Always following an unambiguous procedure
- Carefully safeguarding the interests of the study association, the individual or another organisation involved in the incident, being a (possible) data breach
- Carefully and systematically analysing an incident, i.e. a possible data leak, so that any risk moments in the process become visible. Central to this is determining the deficiencies in the (application of) technical and organisational security measures, which (may) have led to the incident
- Promoting the taking of appropriate improvement measures and structurally securing these improvement measures
- Appointing a board responsible for data breaches and appointing an authority to which one can turn when discovering a (possible) data breach. This could include a privacy coordinator at Radboud University

## Approach to data breach

So when there is a (possible) data breach, the following process diagram can be followed.

**Step 1. Identify possible data breach**

If a (possible) data breach is identified, the rest of the board is informed. In doing so, the board data breach manager decides whether he/she will take on the problem alone or involve another board member (or possibly a former board member/active member) in the process.

**Step 2. Board leader; assess nature/seriousness of incident & report to rest of board**

The board leader (and any other help) investigates the data breach to see if there is in fact a data breach. If it is a data breach, the information leaked and the severity of the data breach are considered. The board leader reports the outcome to the rest of the board. The following points play a role in the assessment:

- Is there a loss of personal data; this means that the study association no longer has this data because it has been destroyed or otherwise lost;
- Is there unlawful processing of personal data; this includes the inadvertent or unlawful destruction, loss or alteration of processed personal data, or unauthorised access to or disclosure of processed personal data;
- Is there a single security vulnerability failure;
- Can it reasonably be ruled out that a security breach led to unlawful processing;
- Have personal data of a sensitive nature been leaked;
    - special personal data in accordance with Art. 9, AVG;
    - data relating to the financial or economic situation of the data subject;
    - data that could lead to stigmatisation or exclusion of the data subject;
    - usernames, passwords and other login data;
    - data that can be used for (identity) faude;
- Do the nature and extent of the breach lead to (a significant likelihood of) serious adverse consequences; consider factors such as:
    - the scope of the processing; does it involve a lot of personal data per person and data from large groups of data subjects;
    - the impact of loss or unlawful processing;
    - sharing of the personal data within chains; this means that the impact of loss and unauthorised modification of personal data may occur throughout the chain;
    - involvement of vulnerable groups; think of mentally disabled people.

**Step 3. If data breach; notify designated authority and investigate data breach**

Authority personal data is notified within 72 hours with which plans are made on that basis. This involves investigating how the data breach could have occurred if it was not already known. Should the notification take place after 72 hours, it should be provided with a motivation for the delay.

**Step 4. Determining data breach**

After consultation with the Personal Data Authority, investigations into the data breach are completed and the entire board considers follow-up plans regarding this incident.

**Step 5. Report to data subject(s)**

The board considers whether data subject(s) should be notified about the data breach; if so, the board responsible will contact them. Whether data subject(s) 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 concerned are unintelligible or inaccessible to anyone who does not have the right to inspect the data, then notification to the data subject(s) may be omitted. If in doubt, the data breach should be reported.
- If the association has subsequently taken measures, which prevent the expected risk, the notification to the data subject(s) may be omitted.
- If notifying the data subject(s) would require disproportionate effort, a general, public notification, in which the data subject(s) are informed equally effectively, is sufficient.

The data breach must be notified to the data subject(s) if the breach is likely to adversely affect their privacy.

**Step 6. Devise and implement remedial measures**

Following the data breach, the board devises improvement measures to prevent a similar situation. These are then also implemented as soon as possible whereby all other possible data breaches are also investigated and remedied.

**Step 7. Document**

After completion of the above steps, the data breach should be documented. This should include the nature of the data breach, the course of events and why certain choices were made.

**Step 8. End**

This concludes the data breach process. If a (potential) data breach occurs again, the process is started again.