**Protocol Data Breach**

In this document you will find a protocol for when a data breach has been established in your study association and which steps need to be taken. Since January 1st of 2016, it is obligated to report data breaches according to the *Wet bescherming persoonsgegevens* (in English: Law of protection of personal data). This obligation is applicable to both those implicated as well as the Radboud University in Nijmegen.

The study association can decide for each individual data breach whether this procedure needs to be followed in its entirety, or whether a deviation from it is appropriate. The goal of this procedure is to establish which steps need to be taken by the study association in case of suspicion or knowledge of an incident that can (possibly) be considered a data breach. Here, the aim is to achieve the following results:

* The continuous following of an unambiguous procedure.
* The careful safeguarding of the interest of the study association, the individual or another organisation that is involved with the incident, which is (possibly) a data breach.
* The careful and systematic analysis of an incident, which is (possibly) a data breach, causing the risk moments during the process to become visible. The establishment of the deficiency in the (execution of) technical and organisational security measurements, which could (possibly) have led to the incident, are central here.
* The promotion of appropriate improvement measurements and securing these improvement measurements.
* To appoint a board member regarding data breaches and to appoint a company that can provide help or information when discovering a (potential) data breach. This could e.g. be a privacy coordinator at the Radboud University.

Approach of the data breach

When there is a possible data breach, the following process steps can be taken.

**Step 1: Identifying the potential data breach**

If a (possible) data breach is found, the rest of the board will be notified. The board person responsible for data leaks determines whether s/he deals with the problem individually or whether alerting another board member (or possibly a former board member or active member) is necessary to deal with the issue.

**Step 2: Board member responsible for data leaks; determining the nature and severity of the incident & reporting to the rest of the board**

The board member responsible (and possible additional helpers) investigate the data breach to find out if there has indeed been a data breach. If that is the case, the leaked information and the severity of the data leak are inspected. The board member responsible reports the conclusion to the rest of the board. In the conclusion, the following issues play a role:

* Is there a loss of personal data; this means that the study association does not have these data anymore, because they have been destroyed or lost in another way;
* Has there been unauthorised processing of personal data; in other words, has there been accidental or unlawful destroying, loss, or change of processed personal data, or non-authorised access to processed personal data or the supply thereof;
* Has there been flaws of vulnerability in security;
* Can it reasonably be excluded that the breach in security has led to unauthorised processing;
* Is there sensitive personal data among the leaked data;
	+ Special personal data (according to Art. 9 AVG [English: GDPR]);
	+ Information regarding the financial or economic situation of the concerned;
	+ Information that could lead to stigmatisation or exclusion of the concerned;
	+ Usernames, passwords, and other sign-in data;
	+ Information that can be used for (identity)fraud;
* Do the nature and extent of the breach lead to (a considerable chance of) severe negative consequences, including factors such as:
	+ The extent of the processing; are large quantities of personal data of a person or data concerning large groups implicated;
	+ The impact of the loss or unauthorised processing;
	+ Sharing of the personal data within the chains of processing; this means that the consequences of the loss or unauthorised change of personal data can occur throughout the chain;
	+ Implication of vulnerable groups, such as mentally atypical groups

**Step 3: If a data breach has been established; notifying designated authority and investigation into data leak**

Authoriteit persoonsgegevens (English: Authority on personal data) is notified within 72 hours, and subsequent plans can be made on this basis. The causes of the data breach are investigated if these are not known so far. If the notification is made after 72 hours, it must be accompanied with a motivation for its delay.

**Step 4: Determining data leak**

After consultation with authoriteit persoonsgegevens (English: Authority on personal data), the investigation into the data breach is completed and the entire board discusses follow-up plans regarding this incident.

**Step 5: Reporting to the concerned people**

The board decides whether the people implicated in the data leak must be notified about the data leak. If this is the case, the board member responsible will contact them. Whether those concerned should be notified, depends on the following points:

* If the association took adequate technical protection measures that made the personal data in question unintelligible or inaccessible for anyone who is not authorised to see these data, notifying the implicated person(s) is not needed. If there is doubt about this, the data leak must be reported.
* In case the association took measures after the fact that prevent the expected risk, notifying the implicated person(s) is not needed.
* In the case that notifying the implicated person(s) would require disproportionate effort, a general public notification will suffice where those concerned are effectively informed.
* The data leak must be reported to those concerned if the breach has probable negative consequences for their personal life.

**Step 6: Thinking of and implementing improved measures**

The board proposes measures to improve based on the data leak to prevent similar situations to occur. These are implemented as soon as possible, whilst other possible data leaks are investigated and mitigated.

**Step 7: Documentation**

After finishing the above steps, the data leak must be documented. Here, the nature of the data leak, the subsequent course of events and a justification for certain choices are described.

**Step 8: End**

With the above, the process surrounding data leaks is finished. If there is another (possible) data leak, the process is initiated again.