**Protocol personal data breaches**

In this document you will find the protocol in the case that a personal data breach takes place in Maizena and which steps Maizena has to take. Since 25th May 2018, the General Data Protection Regulation (GDPR) makes it obligatory to report personal data breaches. This duty to report personal data breaches applies to both the person(s) and the Radboud University in Nijmegen.

The study association has the authority to decide for each personal data breach whether the procedure should be fully or partially followed. The purpose of this procedure is to establish which steps must be taken by Maizena when there is a suspicion or knowledge of an incident that could be regarded as a personal data breach. Therefore, Maizena aims to target the following results:

- Follow an unambiguous procedure.

- Carefully safeguard the interests of the study association, the individual or another organization that is involved in the incident, which caused the personal data breach.

- Analyse an incident in a careful and systematic manner so that existing risk moments become visible in the process. The central issue here is the determination of the deficiencies in the (application of) technical and organizational security measures, which could have led to the incident.

- The appointment of a management responsible for personal data breaches and the designation of a body that can be called upon to discover a (possible) data breach. This could include a privacy coordinator at Radboud University. In the case of Maizena, that would be the FG-Bureau of the Radboud University.

**Approach following a personal data breach**

When there is a (possible) data breach, the following process diagram can be used.



3. In the case of a personal data breach inform the designated body (e.g. a privacy coordinator at Radboud University) of the personal data breach

7. End

6. Think about ways to better improve data protection and implement them

5. Report to those involved

4. Determine the exact nature of the personal data breach

2. Board President: assess the nature/ seriousness of the incident and report to the rest of the board

1. Identify the possible personal data breach

**1. Identify the possible personal data breach**

If a (possible) personal data breach is detected, the rest of the board should be informed. The board member responsible for personal data breach determines whether he / she is solely responsible for the problem or involves another board member (or possibly a former administrator / active member) in the process.

**2. Board President: assess the nature/ seriousness of the incident and report to the rest of the board**

The Board President (and any other drafted in to help) will investigate the personal data breach to see if there is a personal data breach. If it is determined that a personal data breach has occurred, then the information that has been leaked and the severity of the personal data breach will be examined. The Board President reports the result 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 these details, because they have been destroyed or have 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 unauthorized access to processed personal data or provision thereof?

- Is there a single shortcoming or vulnerability in security?

- Can it be reasonably ruled out that a breach of security has resulted in unlawful processing?

- personal data of a sensitive nature has been leaked;

- special personal data in accordance with article 9 of the AVG;

- information about the financial or economic situation of the person concerned;

- data that may lead to stigmatization or exclusion of the person concerned;

- user names, passwords and other log-in data;

- data that can be used for (identity) fraud;

- The nature and extent of the infringement leads to (a considerable chance of) serious adverse consequences? Involving factors such as:

- the extent of the processing; it involves a lot of personal data per person, and data from large groups of subjects

- the impact of loss or unlawful processing;

- the sharing of personal data within chains; this means that the consequences of loss and unauthorized modification of personal data can occur throughout the chain;

- involvement of vulnerable groups e.g. mentally disabled people

**3. In the case of a personal data breach inform the designated body (e.g. a privacy coordinator at Radboud University) of the personal data breach**

The designated authority of Radboud University is informed about the plans that are made to correct the personal data breach. It examines how the personal data breach could have occurred if this has yet to be identified. The designated body for this is the CERT-RU, available on 024-36 2 22 22 (ICT Helpdesk). Outside office hours you can contact the CERT-RU on 024 361 08 18.

**4. Determine the exact nature of the personal data breach**

After consultation with the designated body of Radboud University (ICT-helpdesk/ CERT-RU), research into the personal data breach will be completed and the entire board will consider follow-up plans for this incident.

**5. Reporting to those involved**

The board decides whether those involved should be informed about the personal data breach, if this is the case, the Board President is responsible for the contact. Based on article 34 paragraph 1 of the AVG, any involved data subject must be informed when the personal data breach probably forms a high risk for the rights and freedoms of this person. The information provided to subjects at least entails a description, in simple and clear language, of the nature of the data that has been breached as well as the details mentioned in article 33 paragraph 3 of the AVG. Involved subjects do not need to be informed when one of the following criteria are met:

- If the association has taken appropriate technical protection measures, as a result of which, the personal data relating to it are incomprehensible or inaccessible to anyone who is not entitled to the data, such as encryption (Article 34, paragraph 3, sub a AVG).

- If the processor took adequate measures after the breach to ensure that there is no longer a risk for the in article 1 mentioned rights and freedoms of the subjects.

- If contacting the subjects requires disproportionate effort. In this case, a public announcement or equally effective measure to inform subjects will instead be given (article 34, paragraph 3, sub c AVG).

**6. Think about ways to better improve data protection and implement them**

As a result of the personal data breach, the Board draws up improvement measures to prevent a similar situation from occurring in the future. These measures should be introduced as soon as possible, and all other possible personal data breaches will be investigated and remedied.

**7. End**

This completes the personal data breach protocol. If a personal data breach occurs again, the process should be started again.