Revision of privacy statement

Dear General Members' Assembly,

The privacy documents on the website provide the members with information on how their personal data is handled and provides the board with guidelines on how work responsibly with the data of the members. Due to the implementation of the new website, the privacy related documents which are shown on the website have been subject to revision. Revision of the privacy statement is necessary since the documents include outdated information and legislation, and because the new website requests different personal data than the previous website.

The separate documents of the "privacy statement", the "picture terms and conditions", and the "data breach protocol" have been combined into one privacy statement document, which entails all relevant information. Parts of the privacy statement that have been highlighted in yellow are those that have been altered or added. These changes include:

- The addition of revision information in the document, including a version number.
- The addition of the full board having access to the general membership database, for the purpose of checking membership status for membership stickers.
- The addition of the website provider hosting the general membership database.
- The removal of a personal phone number being requested in the membership application form on the website.
- The update of the amount of contribution to the actual current amount, which is from 12 to 15 euros.
- The addition of a signature being requested in the membership application form on the website.
- The addition of a personal phone number and dietary preferences and allergies being requested in contracts.
- The addition of banners on the website as a location where pictures of members can be used.
- The change of the legislation that the data breach protocol is being based on, from the Wet Bescherming Persoonsgegevens (Wbp) to the General Data Protection Regulation (GDPR). This change further included:
    - A new flowchart for the data breach protocol.
    - Contact information of the data protection officer of the Radboud University.
    - A less active role of the Radboud University in the data breach protocol.
    - The addition of the department of personal data of the government, the Autoriteit Persoonsgegevens (AP), as a destination for data breach notifications.

The XVIth board is currently still working on establishing a processing agreement with the privacy department of the Radboud University. Therefore, the paragraph which is highlighted in red is still subject to change. The XVIth board expects no drastic changes in this part of the statement, and therefore plans on implementing these changes after the fact, with the permission of the General

Study association Psychology in Nijmegen
Thomas van Aquinostraat 4
Kamer 00.016
6525 GD Nijmegen
(024) 361 25 88
info@spin-nijmegen.com

Members' Assembly. In case these changes are drastic, a new privacy statement revision will be presented at a General Members' Assembly in the future.

To implement these changes a vote will be held at the general members' assembly. The XVIth board hopes to have properly informed you of the revisions made in this privacy statement and welcomes any questions during the General Members' Assembly. Questions may also be sent to Secretary@spin-nijmegen.com before Tuesday the 12th of May 2024 23:59 PM, these will then be discussed at the GMA.

Yours faithfully,

The XVIth board of Study association Psychology in Nijmegen.

Study association Psychology in Nijmegen
Thomas van Aquinostraat 4
Kamer 00.016
6525 GD Nijmegen
(024) 361 25 88
info@spin-nijmegen.com

PRIVACY STATEMENT

This document entails the explanation regarding data that 'Study association Psychology in Nijmegen (hereinafter referred to as SPiN)' collects from its members and beneficiary members. The two aforementioned groups will be further referred to as 'the members'. The association does not collect or use information for purposes other than the purposes described in these terms and conditions unless you have given permission in advance. This privacy statement is subject to change and members should regularly consult the privacy statement for this reason. Any adjustments and/or changes will be changed in this document and permission will be requested for this. Drastic changes in the privacy statement can therefore not be adjusted in the interim unless consent has been requested prior to the change, of members who have already signed the privacy statement.

1. The application form

Below is a list of the data collected on the registration form and for what purposes this data is used. This information is necessary to make use of the services of the association. The information provided through the registration form will be stored in the general membership file. These are stored on a secure server hosted by the website provider, to which only the board members of SPiN and the website provider have access. A processor agreement has been concluded with the website provider. In addition, these data are stored in a digital administration program. A processor agreement has been concluded with the administrators of this administration program. The personal data are stored up to and including September of the academic year in which the membership or donorship is terminated at SPiN through the usual procedure for termination, i.e. by completing a registration form offline or online before September 1st. The data is then deleted. If a person wants to become a member or a donor again, they must fill out a form again.

Data:	**Purpose:**
First and last names	To distinguish between members.
Date of birth	To indicate whether a member is 18 years or older, in importance with the law.
Address	For sending documents.
Email address	To get in touch for announcements or invitations, and to send the newsletter with relevant information for members
Student number	To indicate the type of member; it is required for scholarships

Study association Psychology in Nijmegen
Thomas van Aquinostraat 4
Kamer 00.016
6525 GD Nijmegen
(024) 361 25 88
info@spin-nijmegen.com

IBAN	To withdraw the annual membership fee of 15 euros through automatic collection and to make payments and declarations easier to process.
BIC	To withdraw the annual membership fee of 15 euros through automatic collection and to make payments and declarations easier to process.
Signature	To withdraw the annual membership fee of 15 euros through automatic collection.

Furthermore, Radboud University can request SPiN to provide certain information of members given through the membership registration. This is to check the student status of members and to check the member lists. The information includes the name of the member and the status of the student (RU-student). Through signing this privacy statement, one agrees with sharing the personal information mentioned above with Radboud University and the Radboud Fonds for scholarship requests.

By signing this statement, permission is given for processing personal information.

2. View and modify your data

It is always possible to view your collected personal data through the secretary and to submit a request to amend, supplement or delete the data. It counts for all data that when there is a change, addition, or removal, you should let this be known to the board.

3. Objection

It is possible to object to the collection of personal data. If the ground of SPiN outweighs the objection, SPiN can choose to continue the processing. If there is only objection to the provision of (certain) personal data to Radboud University, this can also be reported to SPiN. If SPiN has already provided personal data to Radboud University, SPiN will inform Radboud University of the restriction of personal data.

4. Reporting obligation for a data breach

SPiN has a duty to report in case of a data breach. This serves the purpose of ensuring that personal data is handled more carefully, and that security is in order. There is a data breach if loss or unlawful processing of personal data (as described above) takes place. Should a data breach take place, then SPiN is obliged to report this to its members. For more information on this, we would like to refer you to the data breach protocol.

Study association Psychology in Nijmegen
Thomas van Aquinostraat 4
Kamer 00.016
6525 GD Nijmegen
(024) 361 25 88
info@spin-nijmegen.com

5. Contracts

Additional data to the standard member file are requested on SPiN's contracts. This data is only collected from members who participate in the activity. Below is a list of the data collected for participation in the activity.

Data:	Purpose:
Date of birth	To determine whether a member is 18 years or younger.
Phone number	To get in touch in case of an emergency or clarification of other business.
Name emergency contact	To get in touch in case of emergency.
Phone number emergency contact	To get in touch in case of emergency.
Dietary preferences and allergies	To take into account for the activity.

6. Picture terms and conditions Study association Psychology in Nijmegen (SPiN)

During activities of SPiN, pictures will be taken that will include members on it. The association sees it as its responsibility to protect your privacy. Through this form, you will be informed where the pictures will be published. These terms and conditions are applicable to all services of SPiN. The association makes sure to take care of your personal information and that it will be handled and stored with confidentiality.

6.1 Website

The pictures that will be taken at activities will be published on the website of SPiN. These pictures are protected and can only be seen after logging into your personal account with a password. Only members are entitled to have an account. The pictures are therefore not publicly available, but only for members of SPiN. Pictures will be filtered before being uploaded to the website. These pictures will be online for up to two years.

Pictures can also be used on banners on the website. The use of pictures on banners happens automatically unless objections have been made by the specific member. Objections can also be made after publication, after which the pictures can still be taken offline.

6.2 (Social) Media

Pictures can also be put online on the social media channels of SPiN. The current existing social media accounts of SPiN are: Facebook, Instagram, LinkedIn, and TikTok. Furthermore, pictures can be published in the association magazine ‘HersenSPiNsels’, and in the almanac. In the magazine and

Study association Psychology in Nijmegen
Thomas van Aquinostraat 4
Kamer 00.016
6525 GD Nijmegen
(024) 361 25 88
info@spin-nijmegen.com

almanac, atmosphere pictures will be used and/or pictures with permission from the specific people in the photos. The (social) media channels are publicly accessible.

Publishing of the pictures happens automatically unless objections have been made by the specific member. Objections can also be made after publication, after which the pictures can still be taken offline.

7. Protocol data breach

This part will explain the protocol which is to be followed when a data breach takes place in the association and explains which steps to take. It is mandatory according to the General Data Protection Regulations (GDPR) to communicate data breaches. This obligation to notify is with regard to the data subject(s), to the Radboud University in Nijmegen (when the data are applicable to the Radboud University) and to the Autoriteit Persoonsgegevens (AP).

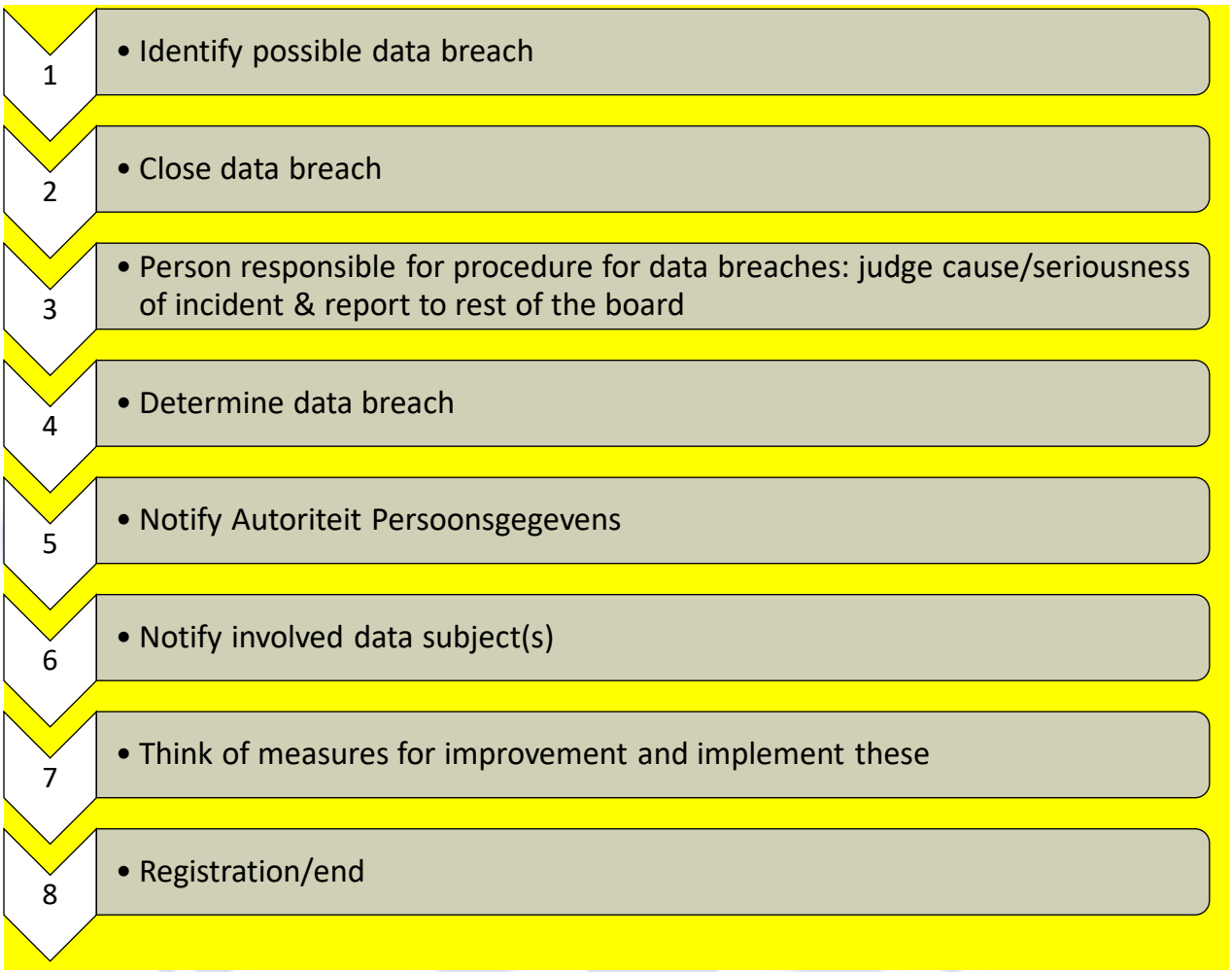
The study association can decide per data breach whether to follow the procedure completely or to deviate from the procedure. The goal of this procedure is to define which steps should be taken by Study association Psychology in Nijmegen (SPiN) when there is suspicion or knowledge of an incident that (potentially) can be defined as a data breach. Hereby the following the result should be strived for:

- To continuously follow a consistent procedure.
- To carefully guarantee the interests of the study association, the individual or another organisation that is involved in the incident, being a (potential) data breach.
- To analyse an incident, being a (potential) data breach, in a careful and systematic way, so existing risk moments in the process will become visible. The focus here is on the determination of imperfections in the (application of the) technical and organisational safety measures, which (potentially) could have given cause to the incident.
- To promote taking appropriate measures, to improve them and to structurally guarantee these improvement measures.
- To appoint a person within the board who is responsible for the procedure for data breaches and the appointment of an instance you can contact when discovering a (possible) data leak. In these instances you can think of the privacy coordinator at Radboud University.

7.1 Approach to data leak

When there is a (potential) data breach, the following process scheme could be used (After the scheme an explanation will be provided per step).

Study association Psychology in Nijmegen
Thomas van Aquinostraat 4
Kamer 00.016
6525 GD Nijmegen
(024) 361 25 88
info@spin-nijmegen.com



1. Identify possible data breach

When a data breach occurs, the rest of the board will be notified. The responsible board member for the procedure of data breaches will determine whether they will process it alone or whether they involve another board member (or potentially a former board member/active member).

2. Close data breach

If relevant, there will be immediate consultation by the board/available IT support to close the data breach as soon as possible. If the data breach applies to the Radboud University, it should be notified to the university through icthelpdesk@ru.nl and or +3124-3622222 within 24 hours after becoming aware of the breach, with the addition of urgence to close the data breach.

3. Person responsible for procedure for data breaches: judge cause/seriousness of incident & report to rest of the board

The responsible board member for procedure for data breaches (and potentially further assistance) will investigate the data breach to see if it actually is a data breach. The law (GDPR) uses the definition of 'infringement with regards to personal data' for a data breach. This is the case with an infringement of

Study association Psychology in Nijmegen
Thomas van Aquinostraat 4
Kamer 00.016
6525 GD Nijmegen
(024) 361 25 88
info@spin-nijmegen.com

the security which by accident or in an unlawful way leads to the destruction, the loss, the change, or the unauthorized sharing or the unauthorized access, storing, or other processing of personal data (article 4, part 2, GDPR).

If it is a data breach, there will be looking into the information which is leaked and the seriousness of the data breach. The responsible board member reports the result to the rest of the board. The following topics play a role in the assessment:

- Is there a loss of personal data; this included that the study association does not hold the data anymore, because these are destroyed or lost in a different manner;
- Is there unlawful processing of personal data; this includes the accidental or unlawful destruction, loss or change of processed personal data, or unauthorised access to processed personal data or the provisions of those;
- Is there a singular shortage of vulnerability in the security;
- Can it reasonably be excluded that a breach of the security could have lead to unlawful processing of personal data;
- Could the nature and extent of the breach lead to (a considerable risk of) serious negative consequences; mention the following factors:
    - De extent of the processing; is it about much personal data per subject, and about the data of large groups of subjects;
    - The impact of the loss or the unlawful processing;
    - The sharing of personal data within chains; this means that the consequences of loss and unauthorized altering of personal data could arise through the whole chain;
    - The involvement of vulnerable groups; think of mentally handicapped subjects

4. Determine data breach

After consult with the board (and with possible assistance), the investigation of the data breach will be concluded and the whole board thinks of follow-up steps regarding the incident.

5. Notify Autoriteit Persoonsgegevens

The GDPR demands that organisations notify the Autoriteit Persoonsgegevens in case of a data breach, within 72 hours after becoming aware of it, unless it is not probable that the data breach will form a risk for the 'rights and freedoms of the subjects' (Article 33, part 1, GDPR). You do not have to notify the AP or the subjects in the following cases:

1. Measures taken before

Fitting measures have been taken before the data breach. This makes the leaked personal data not understandable for the unauthorised. For example, because the data are well encrypted or replaced by hash values. Important: this only applies when:

- The data are still fully intact.
- You still have the full control over the data.

Study association Psychology in Nijmegen
Thomas van Aquinostraat 4
Kamer 00.016
6525 GD Nijmegen
(024) 361 25 88
info@spin-nijmegen.com

- The key that has been used for the encryption or hashing has not been in danger during the data breach. And that this key can also not be found by the unauthorised with the available technology.

2. The wrong recipient is trustworthy

Are the data sent to a wrong but trustworthy recipient? (Think of the Radboud University). This means that it is potentially not probable that the data breach still gives rise to risks. When that is the case, you do not have to notify the AP or the subjects anymore of the data breach.

6. Notify involved data subject(s)

The board considers whether the data subjects need to be informed of the data breach, and when this is the case, the responsible board member contacts the subjects. Whether the subjects need to be informed is dependent on the following factors:

- In case the association has taken fitting technical and organizational protective measures, which make the personal data unreadable or inaccessible for anyone who is unauthorized to get access to the data, then the communication to the data subjects is not necessary (article 34, part 3a, GDPR).
- In case the association takes measures after the fact to ensure that the high risk for the rights and freedoms of the subjects would not be present anymore, then the communication to the data subjects is not necessary (article 34, part 3b, GDPR).
- The data breach should be communicated to the data subjects, in case the breach holds a high risk for the rights and freedoms of the data subjects (article 34, part 1, GDPR). This is done in the form of a description, in clear and simple language, which explains the cause of the data breach. It also mentions a contact person for further information, it includes the naming of probable consequences of the breach, and the mentioning of measures against the current breach and potential negative consequences of these (article 34, part 2, GDPR).

In case the data breach involves data which are applicable to the Radboud University, then the data protection officer of the Radboud University will be notified immediately about the data breach. The data protection officer can be contacted via mail via fg@ru.nl.

7. Think of measures for improvement and implement these

Following the data breach, the board defines measurer of improvement to avoid similar situations in the future. These will be implemented as soon as possible, which also includes researching and processing other possible data breaches.

8. Registration/end

The notification of a data breach and the measures of improvement will be registered in the Register Datalek document. This document safeguards the following and evaluating of potential measurer of improvement. Registrations should be kept for a minimum of 2 years.

This concludes the process for data breaches. When another (potential) data breach occurs, then this process will start over again from the beginning.

Study association Psychology in Nijmegen
Thomas van Aquinostraat 4
Kamer 00.016
6525 GD Nijmegen
(024) 361 25 88
info@spin-nijmegen.com