

# Privacy Policy

2018-2019



Version 5.0

Enschede, 1 February 2019

Privacy policy: 2018/2019  
Cas van der Kuil  
Patrique Westerweel  
Tristan van Haaren  
Enschede, 2018  
SV IManage

## Table of Contents

<b>1.</b>	<b>INTRODUCTION .....</b>	<b>5</b>
1.1	REQUIREMENTS FOR THE PROCESSING OF DATA BY ASSOCIATIONS.....	5
1.2	ADDITIONAL DEMANDS.....	5
1.3	SYSTEMS .....	5
1.3.1	<i>Members file</i> .....	6
1.3.2	<i>Money box and Bank account</i> .....	6
1.3.3	<i>svimanage.nl</i> .....	6
1.3.4	<i>@svimanage.nl mail addresses for board members through Transip</i> .....	6
1.4	UPDATES PRIVACY POLICY .....	6
<b>2.</b>	<b>REGISTRATION AND VISIBILITY OF PERSONAL DATA IN THE MEMBER FILE.....</b>	<b>7</b>
2.1	DATA MATRIX .....	7
2.2	REGISTRATION OF ADDITIONAL INFORMATION .....	7
2.3	REGISTRATION OF SPECIAL INFORMATION .....	7
2.3.1	<i>Definition of special data</i> .....	8
2.3.2	<i>Medical data</i> .....	8
2.3.3	<i>Confidentiality</i> .....	8
2.3.4	<i>Expiry date</i> .....	8
2.3.5	<i>Safekeeping</i> .....	8
2.4	SYSTEM- AND DATA MANAGEMENT .....	8
<b>3.</b>	<b>DISTRIBUTION, EXCHANGE AND USAGE OF PERSONAL DATA .....</b>	<b>9</b>
3.1	GENERAL .....	9
3.1.1	<i>Who processes?</i> .....	9
3.1.2	<i>Conditions for usage of personal data</i> .....	10
3.2	EXTERNAL PARTIES .....	10
3.3	MAILING .....	10
<b>4.</b>	<b>MUTATION OF PERSONAL DATA.....</b>	<b>11</b>
4.1	MUTATIONS IN PERSONAL DATA .....	11
4.1.1	<i>Ability to mutate</i> .....	11
<b>5.</b>	<b>ARCHIVING OF PERSONAL DATA.....</b>	<b>12</b>
5.1	LISTS.....	12
5.2	COPY .....	12
5.3	PUBLISHING .....	12
5.4	REMOVAL .....	12
5.5	ALUMNI .....	12
	EDITING THE MEMBER FILE .....	13
<b>6.</b>	<b>SENDING MESSAGES.....</b>	<b>14</b>
6.1	OPT IN/OUT.....	14
<b>7.</b>	<b>ONLINE MEDIA .....</b>	<b>15</b>
7.1	IMAGES TAKEN DURING ACTIVITIES .....	15
7.2	DISCLAIMER SVIMANAGE.NL AND SOCIAL MEDIA ACCOUNTS .....	15
7.2.1	INFORMATION RELATED TO THIRD PARTIES, PRODUCTS AND SERVICES .....	15
7.2.2	PERSONAL DATA .....	15
7.2.3	EXCLUSION OF LIABILITY .....	15
7.2.4	APPLICATION OF LAW .....	16
7.2.5	CHANGES .....	16
7.2.6	DOCUMENTS, ILLUSTRATIONS, (IMAGE) MATERIAL AND CONTENT .....	16
<b>7.3</b>	<b>DATA BREACH .....</b>	<b>16</b>

7.3.1 PROCEDURES DETECTION DATA BREACH .....	16
7.3.2 PROCEDURE DATA BREACH .....	16
7.3.2.1 <i>Communication to the supervisor</i> .....	16
7.3.2.2 <i>Communication to members</i> .....	17
7.4 SUPERVISOR .....	17
<b>8. UNAUTHORISED USE OF PERSONAL DATA.....</b>	<b>18</b>
8.1 PREVENTING UNAUTHORISED USE OF PERSONAL DATA.....	18
8.1.1 <i>No-Disclosure Agreement</i> .....	18
8.2 REPORTING ABUSE .....	18
8.3 MEASURES .....	18
<b>9. QUESTIONS, COMPLAINTS OR REPORTS .....</b>	<b>19</b>

## 1. Introduction

As a student association with international business students, student association IManage (here after called 'S.V. IManage') understands the importance of properly storing and processing personal information of its members, partners and other relations. Personal information is handled with the greatest amount of care and is properly protected by S.V. IManage. Furthermore S.V. IManage abides to all the demands stated within the General Data Protection Law (here after referred to as GDPR).

In this policy plan S.V. IManage aims to give adequate information regarding the handling and storage of personal information by S.V. IManage. This will be done by explaining how personal information and data files are registered, processed and saved. S.V. IManage also aims to give information regarding related topics, such as consultation, mutation and the exchange of personal information of its members, partners and other relations. This privacy policy contains all on- and offline systems used by S.V. IManage that handle various types of personal information.

### 1.1 Requirements for the processing of data by associations

The GDPR has various demands for organizations that utilize administration files. These demands are as followed:

- Permission from a member to process their personal data;
- Keeping a correct and exact record of all member data;
- Security of data;
- If requested, the possibility to view all stored information related to a member;
- The data only to be used for the goal of which it was initially gathered.
- Financial information is kept for 7 years after a member cancels his or her membership with S.V. IManage, in accordance with Dutch laws.

In accordance with the GDPR S.V. IManage has permission to process personal data; *Categorie Bijzondere vereisten, vrijgestelde categorieën van verwerkingen (paragraaf 1): verenigingen, stichtingen en publiekrechtelijke beroepsorganisaties.*

### 1.2 Additional demands

In addition to the current demands stated within the GDPR, S.V. IManage has set out to formulate some additional demands regarding the processing of personal data. This policy also contains information for members, users, administrators and designers of our systems to ensure that in the future S.V. IManage acts according to the privacy laws.

### 1.3 Systems

S.V. IManage processes personal data using the following systems. For most of its storage S.V. IManage uses Dropbox. Dropbox fully works according to the demands set within the GDPR. The remainder of our systems work with either European servers or local storage.

### 1.3.1 Members file

The members file is a custom designed Excel sheet where all the data regarding membership information is stored. This file is stored in Dropbox, locally on a computer and occasionally a backup is made on a thumb drive. This file can only be viewed by the board members of the current year. All board members of the current year are allowed to insert new membership information and mutate existing data.

### 1.3.2 Money box and Bank account

IManage SV has a bank account in Rabobank, a Dutch multinational banking and financial services company headquartered in Utrecht, Netherlands. Rabobank is completely compliant with the GDPR law. Direct access to the bank account have only the chairlady and the treasurer (for online banking as well). The online banking is secured via the option of using Rabo reader.

IManage also has a money box, which stays in the office. It is used to collect cash payments when necessary. The money box is locked with a key and the internal and treasurer have access to it. For security purposes the amount of money in the box is small.

### 1.3.3 svimanager.nl

The website [www.svimanager.nl](http://www.svimanager.nl) has multiple purposes for which it is used. Mostly it is used to display information regarding the association. Furthermore, it is used to display events that S.V. IManage is organising as well as pictures of past events.

### 1.3.4 @svimanager.nl mail addresses for board members through Transip

Every board member has a @svimanager.nl email address in accordance to their function. These emails are sent through Transip webmail. Transip is conform according to the GDPR.

## 1.4 Updates privacy policy

S.V. IManage retains full permission to make changes to this policy document. It is recommended to regularly check this document to know about any changes that might occur. The privacy policy can be found at [www.svimanager.nl](http://www.svimanager.nl)

## 2. Registration and visibility of personal data in the member file

### 2.1 Data matrix

The following personal information is registered in the member file of S.V. IManage. Each *record* in the database is connected to a unique index number.

	Required	Visible for Board	Visible for Committees	Mutable
First Name	x	x	x	
Last Name	x	x	x	
Nationality	x	x	x	
Mobile phone number	x	x		x
E-mail Address	x	x	x	x
Address	x	x		x
Date of Birth	x	x		
Study	x	x		x
Payment information	x	x		x
Membership status		x	x	x
Other information		x		x

Information will only be supplied to committees when this is necessary for activities. Payment information contains either the IBAN or BIC or both, of a specific member.

### 2.2 Registration of additional information

A commission connected to S.V. IManage can require additional information for its activities (Dietary wishes for example). This might be necessary when an activity, such as an international excursion is organized. The data collected is kept for as long as necessary for organizing this excursion. This data will be deleted after completion of the activity which it was obtained for.

### 2.3 Registration of special information

Special information will only be processed if it is explicitly required. Within an association it is allowed to keep track of health related information to be able to properly care for a member.

All other types may not be registered, unless it is clearly necessary and the member gave approval for the registration.

Some information should be handled with extra care. Examples of this are religion and health related information. This kind of data could lead to unwanted risks. It could, however, be necessary to have access to this kind of information in certain circumstances.

### 2.3.1 Definition of special data

Classified as special data is:

- Religion
- Race
- Political leaning
- Sexuality
- Membership of an association
- 'Burger Service Nummer' (BSN)

### 2.3.2 Medical data

It might be necessary to collect some medical data for the safekeeping of members during activities, especially for our annual Study Trip abroad. This data must be destroyed when it is no longer necessary for the activity for which it was originally collected. Data specified under this article may not be collected as 'medical data'.

### 2.3.3 Confidentiality

Individuals who have permission to register and look into personal data are obliged to keep all data secret unless they are by law required to share it. We enforce this rule by having anyone who might come in contact with personal data sign a Non-disclosure agreement (NDA).

### 2.3.4 Expiry date

Special data may only be kept for a pre-determined term. After this period, the data will be destroyed. It should be clear to a member why this data was collected and for how long it will be kept.

### 2.3.5 Safekeeping

A standard sign up form does not contain any type of special information. When for a special occasion one needs to deviate from the standard forms and collect special data a few steps should be taken. A request should be send out by those responsible in the association (= the board). This request should contain at least: Which data is required, why this data is required and for how long it is to be kept by the association. Unanimous approval of the board is needed before commencing with the collection.

## 2.4 System- and data management

Data and applications used within SV IManage are all locked with a password. The member file is only accessible by board members, filled paper sign-up sheets are kept in a locked closet. All board members have individual mail addresses with personal passwords. Next to that, our website is maintained by the board.



### 3. Distribution, exchange and usage of personal data

As an addition to the strict privacy laws imposed on S.V. IManage, there are also several decisions formulated by the board on the exchange of data.

#### 3.1 General

##### 3.1.1 Who processes?

- Board members  
*In practice a board member is able to view, edit and register all data contained within the member file and the Dropbox. Specific board members are assigned to the various tasks surrounding all administration.*
- Treasurer  
*The treasurer is in charge of all the financial tasks required for running the association.*
- Secretary  
*The secretary is in charge of the social media surrounding the association. (Facebook, LinkedIn & Instagram). He or she is also in charge of sending out mails via MailChimp.*
- External affairs  
*The external is in charge of all the personal data that is communicated with third parties (which will be further explained later in this document).*
- Internal (Deventer) affairs  
*The internal is in charge of the registering and mutating of all information related to members within the administration.*
- Committee members  
*Within the committees committee members have reason to access personal data. This access is needed for organising activities. The committee members have to sign a NDA to access the personal data.*

### 3.1.2 Conditions for usage of personal data

Usage of data must meet the following requirements:

1. A clear goal needs to be formulated before data can be collected. Beforehand it should be clear for how long the data is kept;
2. It is only allowed to collect relevant information;
3. A permission model needs to be designed which shows which person is able to access what data. In addition to this, adequate security measurements need to be applied;
4. Data may not be shared with third parties unless a member gave explicit approval or it has to be required by law;
5. Data may only be kept for a pre-determined amount of time and needs to be removed after that. A member has the possibility to get his or her data removed at all times;
6. It is only allowed to save special data if this is explicitly required and explicitly allowed by the individual in question. This data needs to be fully removed at the end of the event for which it was gathered, unless the individual gives permission to keep their information for an extended period of time;
7. The collecting of data happens in accordance with the privacy policy and the GDPR.

### 3.2 External parties

- Providing personal data, addresses and e-mail addresses of members of the associations to third parties is not allowed in any occasion. With the exception of the member cards, which are issued in collaboration with Khalid Oubaha.
- Koepel Overleg Studenten Saxion (hereafter KOSS) is an association within Saxion of which S.V. IManage is a member. KOSS has an agreement with Studystore, in which Studystore sends KOSS personal data regarding new sign ups to S.V. IManage through Studystore. KOSS then sends this data back to S.V. IManage so we can complete the sign up to S.V. IManage. The data that will be received from KOSS contains:
  - Names of Members
  - Emails of Members
- S.V. IManage gives its sponsors the possibility to advertise through various communication channels of the association. These advertisements are critically evaluated before being sent out to the members. It is important to know that these e-mails/messages will always be sent through us, a third party will not receive access to your personal data unless there is permission from that individual.

### 3.3 Mailing

S.V. IManage will never send a physical letter to your home address unless this is necessary for financial reasons. This will always happen in consultation with the specific individual.

## 4. Mutation of personal data

As previously mentioned, the Internal (and Internal Deventer) affairs will be the ones in charge of registering and mutating information of members. If other board members want to change or add something to this file, they have to ask one of the internals to do it. Other board members won't ever have authority over the member file and are not allowed to edit it.

### 4.1 Mutations in personal data

It is currently not possible for a member to view who edited his personal data, one can assume that this editing has been done by the Internal affairs officer/Internal Deventer.

#### 4.1.1 Ability to mutate

Upon request, a member is able to ask to update his or her personal data (phone number, e-mail address and payment information). It is not possible to change first/last name, date of birth or student number. Officially the Internal affairs officer/Internal Deventer will be responsible for updating the database.

Sign-up sheets used to sign up for activities can only be removed and are not available for editing.

It is not possible for a member to directly update his or her personal data.

## 5. Archiving of personal data

The 'Member file' is the file in which the members data is stored. Therefore it is prohibited to pass on any information found within this file to individuals who normally would not have access to it. It is only stored on the personal computers of board members when they are updating the file. It is to be removed from a board members personal computer when the relevant individual is no longer a board member, this is to be done in the presence of a current board member. It is prohibited to copy and/or save any information found within the Member file on an external computer (exception being a board member's personal computer).

### 5.1 Lists

It is prohibited to export data from the Member file to another document. Excursions and activities however, do sometimes require data to organise the activity. To ensure that committees are not hindered in organising their activities, they are able to export data that is gathered to a sign up point for that specific activity. This data will be exported by a member of the specific committee to another file (which is not the Member file), in order to create an overview of who is participating, has paid and is a member of S.V. IManage.

When an external or physical list is made, it will be kept for a minimal amount of time as described above. Saving data on a different location than on a specific S.V. IManage location or the board members personal computers is deemed a potential security risk. Therefore we have put in place a Non-Disclosure Agreement, which you can find in Appendix 1.

### 5.2 Copy

As mentioned before it is prohibited to make external copies of the Member file. In compliance with the previous statement, it is prohibited to make any copies of the lists as mentioned under *6.1 lists* on external computers. An additional exception for this being the personal computers of the committee members responsible for this specific activity.

### 5.3 Publishing

The data stored within the Member file is strictly personal. Therefore, it is forbidden to publish any data found here outside of the Member file unless explicitly approved by the member whose data is to be published.

### 5.4 Removal

Exported data must be kept as short as possible. The individual who exports data from sign up forms as is approved under *6.1 lists* is fully responsible for proper destruction of the data after the activity.

### 5.5 Alumni

Data stored within the Member file is kept for as long as an individual is a member or donator of the association. This entails personal data and payment information.

When an individual decides to leave as a member, most of his data is removed. We will only keep their names, e-mail addresses and the years in which they were a member, in order to organise reunions. We will also keep financial data according to GDPR ruling.

Data filled in through an activity sign-up form are kept for a maximum of six months; after this period the data has to be destroyed.

Data of ex-members may only be viewed by board members. The data saved pertaining to ex-members cannot be altered and are only used for statistical, historical purposes and in order to organise reunions.

#### [Editing the Member file](#)

Editing the Member file requires it to be downloaded by a board member. This may only be done on a personal computer. Editing is done when someone subscribes as a member or wants to be removed as a member. The editing is done by the Internal Affairs Officer for members in Enschede, and by the Internal Deventer for members in Deventer.

## 6. Sending Messages

### 6.1 OPT in/out

S.V. IManage is allowed to send its members e-mails containing information related to membership fees, General Member Meetings, newsletters and information related to the participation in activities. These e-mails may be send out without the approval of the receiver. Usually members will only be contacted through e-mail. If however, it is necessary for financial related information it is also allowed to send letters to the registered home addresses. An OPT out request can be send to the board, whom will then ensure that this individual will no longer receive these e-mails or letters.

It is however, not possible to OPT out of system messages, which contain critical information pertaining to the membership (such as a General Membership Meeting) and financial messages. The only way to OPT out of these messages is to leave S.V. IManage as a member.

## 7. Online Media

In the modern world we cannot go without the usage of online media. All online media channels association with S.V. IManage work in accordance with this written statement and guidelines.

### 7.1 Images taken during activities

During activities organised by S.V. IManage, several pictures will be taken in order to be published on our website, Facebook page or Instagram page. These pictures will be published without any names relating to the individual in the picture.

### 7.2 Disclaimer SVimanager.nl and social media accounts

The website utilized by S.V. IManage is created and maintained with the greatest care. Even though S.V. IManage attempts to give factual, exact and actual information from creditable sources, we cannot give any guarantee that information provided through the website is any anyway factual, exact or actual. Decisions based on the available information on our website is entirely the responsibility of the user.

S.V. IManage cannot guarantee that the website will always run without any hiccups.

#### 7.2.1 Information related to third parties, products and services

If S.V. IManage places a hyperlink to a third party website we cannot promise that the information found on the website is factual or recommend the website. The usage of such hyperlinks is entirely to the risk of the user. S.V. IManage takes no responsibility for the content, usage or availability of such websites.

#### 7.2.2 Personal Data

In order for an individual to sign up through the website, a registration form has to be filled in. When you send the filled in registration form it is automatically send to all the board members to see that the individual has signed up for S.V. IManage. This data will be processed according to the earlier made statements in this policy.

#### 7.2.3 Exclusion of liability

S.V. IManage takes no liability for any direct, indirect, special, incidental or immaterial damage, regardless of the fact that S.V. IManage was information about the possible damage that could be caused by;

- Defects or viruses connected to the machine or software used to gain access to the website
- Information which has been published through the website
- The interception, mutation or in any way changing any information received from the website
- The working or the lack of availability of this website
- Abuse of this website
- Loss of data
- The usage of software downloaded through the website
- Claims of a third party in relation to the website

This exclusion of liability is extended to board members, voluntary commission members and the person(s) updating the website.

#### 7.2.4 Application of law

Dutch law applies to this website and its disclaimer.

#### 7.2.5 Changes

S.V. IManage has the right to change any information found on the website and within this disclaimer without any form of announcement. We recommend to regularly check the information on our website and in this disclaimer for the latest information.

#### 7.2.6 Documents, illustrations, (image) material and content

Content, documents, images, logos and pictures found on S.V. IManage website or any of the S.V. IManage social media accounts are owned by S.V. IManage, photographers and its partners. If you want to make use of any of the content provided through this website you can contact [secretary@svimanage.nl](mailto:secretary@svimanage.nl).

### 7.3 Data breach

S.V. IManage does everything in its power to ensure stored personal data does not fall into the hands of a third party. When this does happen, article 34a of the law protection of personal data (Dutch law) act is set in motion and this data breach will be reported. The law explicitly states that this entails personal data leaked through security problems. A data breach must always be reported to the Authority Personal Data (AP), previously known as CBP.

#### 7.3.1 Procedures detection data breach

A data breach can be detected in several ways. Generally this breach is first detected by a board member or a website committee member. We constantly strive to find vulnerabilities within our software and systems.

#### 7.3.2 Procedure data breach

##### 7.3.2.1 Communication to the supervisor

When a data leak is detected, S.V. IManage is required to report this leak to the supervisor.

This report contains at least:

- Type of breach
- Who to contact for information regarding the breach
- Actions to minimize the negative effects of the breach
- A description of the possible effects of the breach in relation to the processing of personal data
- Actions taken by the organisation to prevent breach in the future



#### 7.3.2.2 Communication to members

After a breach has been detected and there is reasonable cause to assume that the leak will have negative implications to the personal life of a member, this member needs to be informed about the leak. This notification should at least contain the following:

- Type of breach
- Who to contact for information about the breach
- Recommended actions to minimize the effects of the breach

#### 7.4 Supervisor

S.V. IManage will use of the GDPR official (Data Protection Officer) of the board of Saxion University of Applied sciences in order to ensure proper proceedings after a data Breach.

You can reach the supervisor at [e.j.a.vandenbeld@saxion.nl](mailto:e.j.a.vandenbeld@saxion.nl).

## 8. Unauthorised use of personal data

### 8.1 preventing unauthorised use of personal data

Unauthorised use of personal data is seen as usage of personal data in any way which is not stated within Dutch law or in this GDPR policy. Unauthorised usage might happen by accident, if someone is not aware of the rules. It is also possible this happens with premeditation. For this reason we have classified both accidental as premeditated 'misuse' of personal data, as this can lead to damage to individual members as to S.V. IManage.

Misuse is seen as:

- A person who is not authorised accessing and using data he or she is not supposed to use or access.
- Using data which is not registered or may not be used

To prevent misuse it is important to set up rules and guidelines.

#### 8.1.1 No-Disclosure Agreement

A Non-Disclosure Agreement (NDA) has been made (see appendix), in order to ensure that individuals who have access to the Memberfile or any other form of access to personal data of members, will be careful when using personal data. This NDA has to be signed by the individual before they are allowed to access any personal data. By refusal to sign this NDA, the individual will not be allowed to access personal data of any form.

### 8.2 Reporting Abuse

When someone suspects the misuse of personal data in any way, one is obligated to report this abuse to any member of the board of S.V. IManage to ensure action is taken. One can contact either [chairperson@svimanage.nl](mailto:chairperson@svimanage.nl) or [secretary@svimanage.nl](mailto:secretary@svimanage.nl).

### 8.3 Measures

Misuse of data will lead to one of the following measures, dependant on the level of misuse:

- A warning
- Removal of access rights to data
- Ending of the function and if necessary the termination of (board) membership
- There is always going to be a research conducted to check whether the type of misuse can be prevented in the future

## 9. Questions, complaints or reports

Questions or complaints related to privacy within S.V. IManage can be send to [secretary@svimanager.nl](mailto:secretary@svimanager.nl)

To correctly handle each question, complaint or report we will register information. Using this information we can get in touch with the individual who send in the question, complaint or report.