AVG declaration

Hereby, the AVG for Associations Foundation declares that E.S.V.V. Pusphaira has completed all or part of the AVG program. E.S.V.V. Pusphaira hereby declares that the efforts have been made as arose from the General Data Protection Regulation (AVG).

If not all program components have been completed and the declaration is nevertheless requested, then the requirements of the legislator have not been fully implemented. The AVG Association for Clubs recommends that the outstanding points be processed as quickly as possible and in any case make a note in the program when this will happen.

The following statement lists all parts / steps that E.S.V.V. Pusphaira has gone through to comply with the AVG legislation. For each part it is clearly indicated which data and parts of the law apply and how they have been complied with. Where necessary, additional information has been provided to clarify the situation.

E.S.V.V. Pusphaira understands that AVG legislation is continuously applicable and that we must regularly check and update the data.

With the full completion of the AVG program of the AVG Association for Clubs, E.S.V.V. Pusphaira received knowledge about the matter that is affected by the AVG, and declares to comply with the law in good conscience. The parts of the self-declaration by E.S.V.V. Pusphaira can be found on the following page (s) of this statement.

Drawn up in Gorinchem,

dated 8/19/2018,

by the AVG Association

located at Stephensonweg 14 in Gorinchem.

2.3 Checklist personal data stored within your association.

Please indicate below which personal data are used within the organization.

Normal personal data

☒ Name/ initials/ insert

☐ Titles

☒ Adress

☒ Postal code

☒ City

☐ Province

☐ Country

☒ City of residence

☒ Phone number

☐ Fax number

☒ Email adress

☐ Website

☒ Gender

☒ Date of birth

☐ Place of birth

☐ Date of death

☐ Marital status

☐ LinkedIn

☐ Facebook

☐ Twitter

☐ Employed at organisation

☒ Bank account number

☐ Login details (username/password)

☐ Vehicle license plate

☐ Branch of sport

☒ Membership number

☐ Race number / start number

Special personal data

☐ Ethnic origin

☐ Political views or preference

☐ Religious opinion or belief

☐ Trade union membership

☐ Genetic or biometric data for unique identification

☐ Health data

☐ Data on sexual orientation

☐ Criminal data or convitions / related security measures

☐ Salary details

☐ Passport copy, on which passport photo is visible (copied without a cover)

☐ BSN-number

☐ Handicap classification code

Explenation of special personal data:

 Education / profession

 Sportspecific diploma’s

Other normal personal data:

Type of identification (ID, Passport, Driver’s license)
Identification number

3.2 Inventory purpose limitaion

For the inventory of the different purposes within the associations, we have made the diagram below. For purposes that often occur with some associations, we have already filled in the scheme and you can tick it as quickly as possible. (Example: telephone numbers in WhatsApp groups at sports clubs). If there are other purposes within your association, you can note these in the open form at 3.3.
NOTE: It is wise to use as little personal data as possible. So only ask for the data that you really need for the proper functioning of your club.

(N = Name, A = Address, C = City, T = Telephone, E = E-mail adress)

☒ **Membership**

Personal information NACTE + birth date

Agreement	Membership agreement (paper or form on the website);
Processing	Member administration, contribution levy, information and invitations to meetings
Processing by whom	Member administration department and communication department;
Retention period	Starting point: two years after termination of the membership, subject to the tax retention obligation of seven years (if relevant).

Briefly describe your situation below:

☐ **Membership and additional profile intormation**

Personal data	NACTE + profile intormation such as: shoe and/or clothing size, dietary requirements, Membership agreement (paper or form on the website)
Processing	Member administration, contribution levy, information and invitations to meetings
Processing by whom	Member administration department and communication department
Retention period	Starting point: two years after termination of the membership, subject to the tax retention obligation of seven years (if relevant).

Briefly describe your situation below:

☐ **Membership and medical data**

Personal data	NACTE + medical information
Processing	Member administration, contribution levy, information and invitations to meetings
Processing by whom	Member administration department and communication department
Retention period	Starting point: two years after termination of the membership, subject to the tax retention obligation of seven years (if relevant).

Briefly describe your situation below:

☐ **Sign up for newsletter**

Personal data	Name and e-mail address;
Agreement	Newsletter subscribtion (form on the website);
Processing	Information provision in the form of newsletters;
Processing by whom	Communications department;
Retention period	During the registration period.

Briefly describe your situation below:

☐ **Stakeholder / lobby contacts, donor and interested party**

Personal data	NACTE;
Agreement	Oral consent, issuing of business card and / or via LinkedIn;
Processing	Provision of information in the form of newsletters or targeted contacts;
Processing by whom	Communication department, management, specialist knowledge departments and / or relationship manager;
Retention period	During the period that people are in contact and thereafter a maximum of 2 years.

Briefly describe your situation below:

☐ **Stakeholder / lobbying contacts with political preference**

Personal data	NACTE + political preference;
Agreement	Oral consent, issuing of business card and/or LinkedIn
Processing	Personal contacts and news provision;
Processing by whom	Communications department, management;
Retention period	During the period that people are in contact and thereafter a maximum of 2 years.

Briefly describe your situation below:

☐ **Employees**

Personal data	NACTE + date of birth, copy ID and bank details;
Agreement	Employment agreement;
Processing	Salary;
Processing by whom	HRM-Department;
Retention period	Depending on which data is involved.

Briefly describe your situation below:

☐ **Employee photos on the website**

Personal data	Name and photo;
Agreement	Additional personnel agreement;
Processing	Employee photos on website;
Processing by whom	Administration, communications department;
Retention period	Starting point: subject to permission, photos are deleted after a person leaves employment.

Briefly describe your situation below:

☐ **Volunteers**

Personal data	NACTE;
Agreement	Volunteer agreement;
Processing	Information provision;
Processing by whom	Communication department, specialist knowledge departments and / or relationship manager;
Retention period	Starting point: two years after termination of the membership, subject to the tax retention obligation of seven years (if relevant).

Briefly describe your situation below:

☐ **Direct marketing (calling or paper only)**

Personal data	NACTE;
Agreement	No agreement required;
Processing	Sending (or calling about) information about the association and / or products / services;
Processing by whom	Communications department
Retention period	During the period that people are seen as prospects for the association or its services / products

Briefly describe your situation below:

 Digital direct marketing (e-mail, facebook, LinkedIn, fax, SMS etc.)

Personal data	NACTE;
Agreement	Digital permission agreement in advance, e.g. when requesting information or registering for a newsletter;
Processing	Digital sending of (or access to) information about the association and / or products / services;
Processing by whom	Marketing / Communications Department;
Retention period	During the period that people are seen as prospects for the association or its services / products.

Briefly describe your situation below:

3.3 Description of additional goal binding.

If you have more personal data, processing and / or agreements than described in 3.2, add this below. Add the additional description about goals and goal retention below so that we can include them in the AVG statement.
Purpose: Event photos on website and Facebook Personal data: photos
Agreement: Permission given through membership form Processing: Photos on website and Facebook
Processing by whom: the board of E.S.V.V. Pusphaira and / or photo / website committee
Retention period: Subject to permission, photos will be deleted after you unsubscribe

4.2 Privacy policy findable, reference in documents.

The privacy policy of the association must be findable for everyone. The easiest way is to put it on the website of the association and to place a link to it on every page (below).

☒ We as an association have made our privacy policy visible on the association's website.

☐ We as an association have not made our privacy policy findable on the association's website.

Briefly describe your situation below:

All agreements (documents requesting personal data) must contain a reference to the privacy policy.

☒ We refer as an association in all our documents (membership agreement, registration form, etc.) in which personal data are contained in our privacy policy on the association's website.

☐ We as an association refer to documents (membership agreement, registration form, etc.) in which personal data are not included in our privacy policy on the association's website.

Briefly describe your situation below:

5.2 Working with processor agreement

☒ We, as an association, declare that we will never pass on personal data to other parties with whom we have not concluded a processing agreement if this is necessary for the purposes for which we received it.

☐ We as an association declare that we also pass on personal data to other parties with whom we have not concluded a processing agreement.

☐ We as an association declare that we do not pass on any personal data to other parties.

We have a processor agreement with the following parties: Google, Dropbox, Hostnet, the KNVB and Sportlink.

6.1 Software up-to-date.

To make systems as safe as possible, you must keep them up-to-date. You do this by turning on automatic retrieval and installation of software updates. Also provide good antivirus software. Ensure that all software is set to automatically retrieve and perform updates. Make good agreements with all your software suppliers.

☒ We as an association have stored personal data only on computers / servers with security software where both the security software and the operating system are set to automatically retrieve and install updates.

☐ We as an association have not only stored the personal data on computers / servers with security software where both the security software and the operating system are set to automatically retrieve and install updates.

☐ We as an association have no personal data stored electronically and therefore have no software updates.

Briefly describe your situation below:

6.3 Data back-up.

To protect the personal data against loss or theft you have to make backups. It is necessary to do that regularly. Ensure that this backup is stored safely.

☐ We as an association have secured the stored personal data with a back-up.

☒ We as an association have not protected the personal data with a back-up.

☐ We as an association have no personal data stored electronically and therefore have no back-up.

Briefly describe your situation below:

6.4 Beware of storing personal data outside the EU.

The legislator is extra strict if you want to store personal data outside the EU. So check whether your service provider (printer, distributor, etc.) stores the entrusted personal data within the EU. For example, that can be the member list. In the processor agreement you can determine whether or not a processor may store personal data outside the EU.

☒ We, as an association, declare that we never transfer or store personal data with parties established outside the EU.

☐ We, as an association, declare that we also transfer or store personal data to parties established outside the EU.

Briefly describe your situation below:

7.3 Accessibility.

☒ In our association, only authorized persons have access to the personal data of the association.

☐ In our association also unauthorized persons have access to the personal data of the association.

Briefly describe your situation below:
Only the board has access to personal data of the association.

We as an association have authorized 5 people to view and process the personal data of the association if necessary for the performance of their duties.

We as an association have registered the personal data of 222 people.

8.4 Destroy personal data.

Indicate below that your association will destroy all personal data by, for example, deleting a rule in Excel and / or shredding the registration form if there is no longer an agreement. Personal data may not be stored for longer than for the purpose for which it is processed. So: after termination of the membership, the personal data of that member will be destroyed.

Identify who is responsible for destroying personal data or checking for destruction. Note: Shredding and throwing away is insufficient. Therefore, purchase a shredder.

Note: In the financial administration (or actually: must!) These personal data may still remain, because there is a (legal) retention obligation of 7 years.

☒ We as an association declare that we will destroy all personal data if the agreement on the basis of which they were obtained has expired or the consent has been withdrawn.

☐ We as an association declare that we will not destroy any personal data if the agreement on the basis of which they were obtained has expired or the consent has been withdrawn.

Briefly describe your situation below:

At the time of deregistration and indicating the deletion of data, all personal data will be destroyed.

9.6 Security measures taken.

We have taken the following security measures:

☒ Software is protected with username and password.

☒ Computers are protected with username and password.

☒ Telephones are protected with a code or finger recognition.

☒ All network folders are only accessible with a username and password.

☒ We have entered multiple authentication.

☐ Only encrypted data carriers are applied

☒ All our (private) websites are set to use a secure connection (= green lock = HTTPS).

☐ The private website is only accessible from countries that we have allowed (whitelist).

☐ We have an authorization procedure for issuing access to our data.

☐ We have trained employees and had a confidentiality agreement signed.

Briefly describe your situation below:

9.7 Access security.

To be sure that only authorized persons can view and edit the personal data, they must always be protected with a password and if possible also with a username. For example, you can protect an Excel file with a password and a PC with a username and password. So make sure that you always have to know a password at least once before you view or edit the personal data of your association.

If you use special personal data, ensure extra security for access security. Hereby you first have to map out which special personal data you have and who is authorized to process it.

Make sure that this data is protected with a username and password. If the association uses special personal data, it is advisable to also take one or more of the following measures:
change password regularly;
apply a second authorization method such as an additional code via SMS; automatic screen lock after 3 minutes of inactivity;
closing off spaces where this data is processed; no guests on the WIFI network.

SO: The more sensitive the special personal data is, the better the measures must be.

☒ We as an association have always stored the personal data behind the security of at least a username and password.

☐ We as an association have not always stored personal data behind the security of at least a username and password.

☐ We as an association have no personal data stored electronically and therefore do not have access security.

Briefly describe your situation below:

9.8 Paper documents and security.

If personal data is also fixed on paper (such as registration forms), then those papers with personal data must be stored under lock and key. Practical: keep all papers with personal data in a cupboard that you always lock. Only persons who have permission to do so for their work for the association may enter that cupboard.

TIP: Locking a cupboard is one thing, but if the keys are lying around, the effect of secure storage is lost. Our tip is to record that one person manages the key (set) on behalf of the association. Also make sure that the key cabinet itself (where you keep all keys to cupboards) is not visible from outside the building.

☐ We as an association have paper documents on which the personal data are stored, stored under lock and key.

☐ We as an association do not have all paper documents on which the personal data are stored, stored under lock and key.

☒ We as an association do not have any paper documents containing the personal data.

Briefly describe your situation below:

We do not store any personal data on paper

10.2 Permission for direct marketing.

The legislator distinguishes between normal direct marketing (calling and sending mail) or digital marketing (via e-mail, Facebook, LinkedIn or SMS).

☐ We as associations always ask permission before we approach someone via digital direct marking.

☐ We as associations do not request permission before we approach someone via digital direct marking.

☒ We as associations do not use digital direct marking.

Briefly describe your situation below:

11.1 Permission for children.

When registering with the association in the case of children under the age of 16, extra attention is required. In that case, the parent / guardian must sign.

But the obligation also applies to:
sign up for a newsletter; register for a meeting; sign up for an outing.

If this type of registration / registration is also used, then you must also check there for permission from children. So make sure you always ask permission from children.

With children (younger than 16 years)

If you have personal details of persons younger than 16 years of age, you must always have a written signature (on paper!) For approval from the parent, guardian or legal representative. Indicate below that your association always does the same.

☐ We as an association declare that we will only process personal data of minors if written permission has been given by the parent, guardian or legal representative.

☐ We as an association declare that we process personal data of minors without written permission from the parent, guardian or legal representative.

☒ We as an association declare that we do not process any personal data of minors.

Briefly describe your situation below:

As a student sports association we do not process any personal data of minors.

12.3 Signature.

By submitting this step-by-step plan, I hereby declare that I have completed this step-by-step plan on behalf of the association.

Explained by:

Name association:	E.S.V.V. Pusphaira
Name person:	James Loos
City:	Eindhoven
Date:	19-08-2018