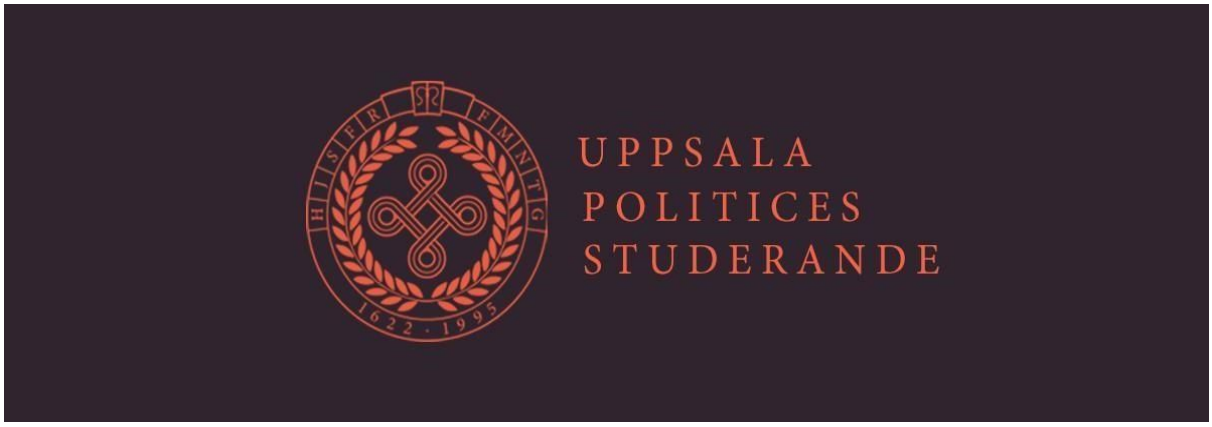

Manual for Personal Data Management

The purpose of this manual is to clarify routines and guidelines for the associations' personal data management, a legislated requirement according to GDPR. The manual can be seen as a compliment to the privacy policies' general description of how and what personal data are being managed. All members who hold a position of responsibility shall take part of and know how to access this manual to be able to secure a personal data management that respects all members integrity and rights regarding their personal data.

Changes in the manual can be made by a decision of the board. The purpose of this is to not aggravate or delay necessary changes or improvements but rather that all members of the board will have an updated and uniform version that members can access upon request. The board is responsible for keeping the manual up to date according to current data protection regulations or correspondent regulations. Members who hold a position of responsibility are responsible for documenting committee-specific routines in their routine manual.

1. What is personal data?

Personal data is all sorts of information that could be tied to a living, physical person. It could be a personal number (date of birth), name and e-mail address. Photos of people and audio recordings that are stored electronically, even though no names are mentioned are personal data. Some of the personal data that are viewed as extra sensitive is health information such as allergies.

2. When do we manage personal data?

Every measure or series of measures taken regarding personal data, whether it is happening automatically or not, for example, collecting, registering, organizing, storing, managing or

changing, recycling, using, distributing etc. In other words, if we have personal data - we are managing it.

3. When may we manage personal data?

Personal data may only be gathered for "specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes", according to the regulation. This means that the personal data we collect must have a specific purpose and may not be used for other purposes than that.

We must also have support in the regulation for our personal data management. There is a couple of legal grounds our association could use. One important is *informed consent.* We ask the person in question if we may register his or her personal data. Consent is described in the regulation as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

When we collect personal data we need to *inform* the person in question. In the regulation GDPR, there is a long list of what information that shall be given, in short, we shall inform about the collection of personal data, what data is being collected and why we are collecting the information. If we will be furthering the data to others we must inform about that as well. We must, as an example, be clear about our transmission of personal data to UPS's national organization, PolRiks.

The regulation also states that we may not *save personal data* for too long. When the purpose of storing the data no longer upholds, the data shall be removed. For UPS that means for example that when a person no longer is a member, his or her personal data must be removed. Before GDPR, the custom was that personal data about an earlier member normally could be used in marketing purposes up to one year after the membership expired.

Keep in mind to *protect* the personal data we manage so that they are not stolen, unintentionally changed or comes astray. If we happen to have a personal data incident we must report it to The Swedish Data Protection Authority (Datainspektionen). A personal data incident could be a lost USB with personal data content, a hacking incident or unauthorized access by UPS members of personal data.

Routines

Member register

If a member who holds a position of responsibility needs access to the member register or a members' personal data during the operational year, he or she may contact the secretary. Sending the whole register should be avoided and another solution is preferred. If the member register is sent to another member who holds a position of responsibility, the secretary states when the receiver must delete the register.

Google Drive

The association uses the cloud service Google Drive to store documents with content that might include personal data. The main rule is to not store or have documents with personal data if there are no legal grounds for doing so. When the operational year is over, before handing over to the next person who holds a position, the member who holds a position of responsibility shall remove documents who include personal data if there is no legal ground for passing it on to the next with the same position. Head of committees and trustees are only responsible for their own, closed folders. The presidium has the responsibility to look over the folder "Arkivet" (the archive).

Every post in UPS has a routine manual from earlier position holders. Only the latest version of the routine manual is saved.

Protocol

During board meetings, the participants first- and last names are written down and saved on a copy kept on Google Drive. The protocol is also uploaded to the associations' website. The purpose of this is the transparency towards the members of the association. If a member or other adjunct person participates during a board meeting, he or she shall be notified about his or her name being written down. If the person does not agree to his or her name being written down, he or she shall be written down as an observer.

When participating during an annual meeting your name might be written down in the protocol. The protocols from the annual meeting are public on the website and stored on Google Drive until further notice.

E-mail

When sending an e-mail to many members at the same time this must be done without making it possible for everyone to see others e-mail address. You send the e-mail to your own e-mail address and add the others in the field BCC (hidden copy). This might lead to the e-mail ending up in the receivers spam mail so make sure to inform about the e-mail in other channels.

E-mail history is saved up to two years before it is deleted. The purpose of the storing is to help the new board members. If an e-mail older than two years are being saved, legal grounds and a purpose must be identified. This can be done accordingly:

1. *Identify* the personal details in the e-mail.
2. Determine what *the purpose* of saving the detail.
3. Determine what *legal grounds* the saving of the detail is supported by.
4. Determine *how long* the e-mail shall be saved before being deleted.
5. *Move* the details from the inbox if it shall be saved for a long period of time.

Photographs

When photos are taken on behalf of UPS during UPS events, consent shall be obtained as soon as possible. Consent is mostly obtained verbally by asking the person in question if they would like to be in the photo. When it comes to event photos during a mingle or similar situations where personal consent is more difficult to obtain, participants of the events shall be made aware that photos will be taken. The participants shall also be made aware of whom to contact if they wish to not be in any photos. This information could be presented when a member is signing up for an event.

When photo albums are published in UPS social media, information about how to get a specific photo, on which the person in question appears, removed shall be stated in the description. When the board has been informed about this, the photo will be removed.

Photo albums taken on behalf of UPS during UPS events are being kept on the associations Google Drive in the folder “Arkivet’’ (the archive). This folder is only accessible by the members who hold a position of responsibility.

Forms

On some occasions, forms are being sent out to members about dinner parties, field trips, trips, evaluations etc. When this is done and personal data are included in the answers, information about why it is being collected, if it will be shared and in that case to whom, how long it will be saved and where you can turn if you want the information to be deleted earlier must be included. The personal details are saved until the event is over and/or when they are no longer necessary to keep.

Health details

Health details such as allergies, special diets or something similar are particularly sensitive data. It is therefore extra important that forms and documents were information like this is being deleted after the event has taken place. When a member is being asked about this, the question should be “Is there anything you can not/do not want to eat?” since this does not ask about the reason behind it. It is not desirable to get answers like “lactose intolerant” or “does not eat beef because of my religion”. When a special diet is being reported to nations or others it is written as “no gluten” instead of “gluten intolerant”.