vitamin B
in the service of associations

Data protection: What factors must associations consider?

Authors Dr Roman Baumann Lorant, solicitor,
Fanni Dahinden, Maja Graf and Sibylle Sutter, vitamin B

On 1 September 2023, the new Data Protection Act (DPA) and new Data Protection Ordinance (DPO) will enter into force in Switzerland. These legal bases regulate the legal handling of personal data. They have been adapted to take into account digitalisation and the EU's General Data Protection Regulation (GDPR). Data protection is not merely a bureaucratic end in itself. Instead, it is a matter of protecting people and their personal rights.

1. Swiss Federal Data Protection Act

The new Data Protection Act does not include any provisions designed specifically for associations. It also does not require association members to be proactively notified of the 1 September 2023 implementation date. *However, a privacy policy will be required from that point forward.*

1.1 Who is responsible for ensuring data protection at an association?

An association holds a great deal of personal data, primarily concerning its members (→ refer to Item 1.4). It must handle such data carefully. The association's board of directors is responsible for handling this data in accordance with data protection regulations. Specifically, it is responsible for ensuring that the association has a privacy policy in force.

1.2 What does the privacy policy provide?

The privacy policy is not intended to seek any consent for data processing. An association uses the privacy policy to meet its *obligation to inform* individuals whose personal data it processes (e.g. by storing the data of website visitors or by recording, processing and passing on such data when they join the association). The privacy policy does not have to be accepted. It must, however, be possible for data subjects to view the privacy policy. The easiest way to do this is by posting the privacy policy on an association's website – ideally in the footer of the website.

If the data processing requires consent, this consent must be acquired *separately* from all individuals whose data is being processed. (→Refer to Item 1.6)

1.3 What should the privacy policy contain?

- General declaration and information about the association
- List of which data is collected and processed
- Description of the purposes for which the data is processed
- Statement of cookies, tracking, social media plug-ins and other technologies in connection with the use of the website
- Transfer of data to third parties and, if necessary, data transfer abroad
- Duration of the retention of personal data
- Data security
- Explanation of the rights of data subjects
- Internal contact person
- Change of privacy policy (can occur at any time and unilaterally)

1.4 What is personal data?

Personal data is any information that refers to an identified or identifiable natural person. Personal data therefore includes all member data of an association, such as names, postal and e-mail addresses, as well as telephone numbers, etc. It also includes *IP addresses (*sequence of digits that uniquely identifies each device on the Internet and traces it back to the owner).

In particular, data concerning a person's religious, ideological or political views or activities, health data and data relating to privacy and race/ethnicity, genetic and biometric data, data relating to administrative and criminal proceedings or social assistance measures merit special protection. If an association processes such data, special care must be taken due to the stricter requirements. In this case, we recommend consulting an expert who specialises in data protection.

1.5 What does "data processing" mean?

In principle, this means any action involving data, such as obtaining (e.g. collecting addresses via a newsletter registration form), storing, holding, using, modifying, disclosing, archiving, deleting or passing on data. The following *processing principles* apply:

Transparency: Open and comprehensive information on the purpose and scope of the personal data processed is obligatory.

Expediency: Only the personal data that is actually required to achieve the intended purpose may be collected. Data may not be collected in advance. For example, the e-mail addresses of members are sufficient for sending out the membership fee invoice or the invitation to the General Assembly. Only the amount of personal data that is actually necessary for the association's activities may be collected and processed.

Purpose: Members' data may be processed only for the purpose specified at the time it is collected, as evident by the circumstances or as prescribed by law.

E-mail addresses that have been collected for sending a membership fee invoice may therefore not be used to send advertising or passed on to third parties without prior consent.

Retention: Data must be deleted as soon as it is no longer necessary for processing and there is no legal obligation to retain it. Such an obligation is, for example, the 10-year retention obligation for annual reports, annual accounts and accounting documents.

Security: Data security which is appropriate to the risk must be ensured by the association in the form of technical and organisational measures (e.g. encryption, back-up systems, access restrictions, passwords, staff training.).

1.6 When is consent required?

In Switzerland, data processing is generally allowed without consent. However, consent is required in the following cases,

- if the above-mentioned principles (→ refer to Item 1.5) are not observed,
- if personal data is processed against the express will of a person, or
- if particularly sensitive personal data (→ refer to Item 1.4) is disclosed to third parties.

To avoid uncertainties from the onset, we recommend obtaining consent as a standard procedure, for example, when joining an association.

1.7 When may an association pass on personal data to third parties?

For an association to be allowed to pass on personal data to third parties (e.g. addresses or address lists), it must have the *consent of the data subjects* or it must inform them before passing on the data and offer them the opportunity to object. A statement on when data is passed on to third parties appropriately can be integrated in the association's statutes or in the privacy policy. Members may prohibit the transfer of their personal data (right to block) or revoke their consent at any time.

If personal data is passed on to third parties to fulfil an order (e.g. printer, newsletter service provider and cloud service provider), this action may also be carried out without consent if the following conditions are met (Art. 9 of the Data Protection Act):

- The information on the transfer of data for the fulfilment of the order is indicated in the privacy policy.
- There is a contract with the order processor.
- Data is processed by the processor in accordance with the same principles applicable at the association itself.
- There is no legal or contractual restriction on this.
- The association has ensured that the order processor can ensure the security of the data (integrity check).

Important: If the order processor is based abroad, observe Article 16 of the Data Protection Act on the cross-border transfer of personal data.

If a law requires the member data to be disclosed (e.g. in criminal proceedings), the association is entitled and obliged to disclose the data.

1.8 When may an association pass on personal data within the association?

This also requires the *consent of each member or the provision of prior information* about the purpose of the data transfer with the possibility to object. The purposeful provision of member data to other members can be stipulated in the articles of association. This includes, for example, information on the forwarding of lists with member data to umbrella organisations or a note stating that the member list is made available to all members in the secured member area of the website. In this case, members also have a blocking right or may revoke consent at any time after it has been issued.

The transfer of member data within the association is also permitted if required to exercise membership rights, e.g. to convene an extraordinary General Assembly (Article 64 paragraph 3 of the Swiss Civil Code). In this case, however, only the amount of data actually required to exercise the right should be transferred (e.g. names and addresses).

1.9 What must be observed when publishing member data?

When publishing member data (website, association newsletter, association newspaper and similar), the rules for disclosure to third parties apply. In particular, when publishing personal data on the website, careful consideration of the expediency is important.

If specific personal data is to be accessible only to members, we recommend setting up a restricted members' area on the website. Publishing personal data in a protected area, however, also requires consent or the possibility to object for each member.

Important: The publication of photos containing persons also requires the consent of each person who can be recognised on the photos (→ refer to vitamin B glossary entry "Right to one's own image", https://www.vitaminb-e.ch/keywords/right-to-one-s-own-image/).

The information on collecting and using data within an association of the Federal Data Protection Commissioner serves as the basis for clarifying the requirements to be met by an association in this regard (→ refer to Items 1.7 – 1.9):

https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/freizeit_sport/datenbearbeitung_vereine.html (last visited on 8 June 2023)

2. EU data protection: relevance for Swiss associations

The EU General Data Protection Regulation (GDPR) entered into force on 25 May 2018. The Swiss Data Protection Act has been amended to comply with the GDPR in many respects.

2.1 Which Swiss organisations are subject to the GDPR?

Swiss companies and organisations (including associations) that process the personal data of natural persons residing in the EU must comply with the GDPR if they

- process the data in the connection with an establishment in the EU or an order processor established in the EU;
- offer goods or services to such persons for payment or free of charge or demonstrate a clear *intention* to do so, e.g. if they target potential EU customers on the website or offer their goods in an EU currency;
- analyse the *behaviour* of persons from the EU (Article 3(2)(a) and (b) of the GDPR), e.g. collect the user behaviour of persons from the EU territory on their website using Google Analytics.

2.2 When is the use/processing of personal data allowed under the GDPR?

The processing of personal data, e.g. by collecting it using the contact form on the website, is permitted under Article 6 paragraph 1 of the GDPR if essentially

- The person has provided consent (for children, this must usually be provided by the legal guardian).
- The personal data is required for the performance of a contract.
- There is a legal obligation (e.g. obligation to keep business records).
- There is a legitimate interest (expediency).

Important: The GDPR is a complex set of rules for processing personal data. Since Swiss associations may be affected in particular by their Internet presence (via website, social media, etc.), we recommend consulting a specialist for further detailed advice.

3. What measures are required for associations?

3.1 Preparing a privacy policy on the website

The privacy policy on an association's website must inform users in clear language who processes their data, for what purpose, how and where. The privacy policy must also refer to the use of external services (e.g. newsletter tools, social media or analysis tools) if they collect personal data when users visit the website.

3.2 Reference to cookies

Cookies automatically save text files about the users of a website in order to identify them. If an association uses cookies on its website, this must be indicated (in the privacy policy or via a cookie banner). A number of content management systems used today (software for creating a website) use cookies as a standard feature. We would therefore recommend the general use of a cookie banner for information purposes. This should be clearly visible to users when they first visit the website. However, it must not conceal mandatory information such as the link to the imprint or the privacy policy.

3.3 Anonymisation of recorded IP address for use with analytics tools

The use by web analysis services (e.g. by Google Analytics) must be documented in the privacy policy on the website. This must also include details of the right to withdraw consent. Since IP addresses are regarded as personal data, it must be ensured that the analytics tool records the IP addresses only in truncated form (using the anonymisation function). Contact your website operator in connection with this.

3.4 Be careful when using social media

If your association uses social media, you may not collect any data from website visitors without their consent. Information on the use of social media offers and the type of social plug-ins used (e.g. Like button, Share button) must be included in the privacy policy. Reference must also be made to the option to withdraw consent.

4. What is the best course of action?

1. Designate a person at the association to handle data protection and to ensure appropriate data security.
2. Make the board members and personnel aware of the issue of data protection.
3. Review internal procedures and obtain an overview of the personal data that is processed at your association: what data is collected? Where does it come from? Where is it stored? Who has access?
4. Check whether your association falls under the EU GDPR.
5. If possible, create a list of your processing activities (this is voluntary at smaller associations but required by law at associations with 250 or more staff members). Only such a list will give you the necessary overview of your processing activities. It does not matter whether you use Excel, Mindmap or a professional online tool.
6. Make the following necessary adjustments:
    - Contact your website operator and discuss any necessary adjustments to the website. Draft a *privacy policy* or review an existing one.
    - Optimise your *membership form* (declaration of consent).
    - Consider including an article on data protection in the next *revision of the articles of association*.
    - Define the *procedure in the event of a request for information* on data processing (Article 25 ff. of the Data Protection Act). You should be able to provide the necessary information within 30 days.
    - If necessary, issue *data protection instructions or a data protection guideline.*
    - Check *contracts with order processors***.**
7. In cases of doubt, contact a legal expert or the Federal Data Protection Commissioner: https://www.edoeb.admin.ch/edoeb/en/home/deredoeb/kontakt.html
8. Notify your members about amendments (e.g. in the newsletter or at the next General Assembly). Although there is no obligation to do so under the Data Protection Act, it raises awareness and demonstrates that you take data protection seriously
9. Data protection is part of risk management. Exercise restraint in collecting personal data and regularly check your technical and organisational measures.
10. Regularly update membership data (e.g. at the General Assembly).
11. Delete data that you no longer need and for which there is no retention duty.

5. More information

5.1 On data protection in Switzerland:

https://www.edoeb.admin.ch/edoeb/en/home/datenschutz.html

https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/grundlagen/ndsg.html

https://www.edoeb.admin.ch/edoeb/en/home/deredoeb/kontakt/faq_beratung1.html

https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/freizeit_sport/datenbearbeitung_vereine.html

(last visited on 15 May 2023)

5.2 On data protection in the EU (GDPR):

https://www.kmu.admin.ch/kmu/en/home/facts-and-trends/digitization/data-protection/data-protection.html

https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/grundlagen/rechtsgrundlagen-ds-international.html

(last visited on 15 May 2023)

6. Text examples

Here, you will find samples for notifying the members of your association or the recipients of a newsletter.

1. Mail to members/newsletter recipients

Dear members,

We have amended our Privacy Policy to align it with the requirements of the new Swiss Data Protection Act. Details are available on our website under *Privacy Policy*.

Dear newsletter recipients,

The new Swiss Data Protection Act enters into force on 1 September 2023. We are taking this as an opportunity to update our customer and prospect data. If you no longer wish to be informed about our news and events in the future, you can unsubscribe from the newsletter using this link. Your data will then be deleted from our distribution list. Otherwise, we will assume that you would like to continue receiving our information.

2. Cookie banner

[Short version footer]
We use cookies to provide you with the best possible experience on our website.
In the Settings *[link]*, you can find out which cookies we use or switch them off.

[Linked versions]
This website uses cookies so that we can provide you with the best possible user experience. Cookie information is stored in your browser and performs functions like recognising you when you return to our website. Cookies help our team identify which sections of the website are most interesting and useful to you.
For further information, see the: Privacy Policy *[link]*

3. Privacy policy on the website

First, obtain an overview of how your association processes personal data and develop your privacy policy accordingly. You can find inspiration for formulating your own personalised privacy policy from examples available on the Internet (e.g. for vitamin B): https://www.vitaminb-e.ch/about-us/privacy/?_locale=en

4. Sample wording for articles of association

Art. [number] **Data protection**

The association exclusively gathers the personal data of the members required to fulfil the purpose of the association. The executive committee ensures data security appropriate to that of the risk.

The member data, particularly name, address, phone number and email address [list other data, if necessary], will be disclosed to all association members.

Variants: The member data will not be disclosed to other members, unless a legal provision applies.

> *Comment: The member data may be required of the members to exercise membership rights (e.g. calling of an extraordinary meeting pursuant to Article 64(3) CC).*

The member data, particularly [which data], will be published on the website, in the newsletter as well as in the bulletin of the association [other publications, if applicable]. Otherwise, data will only be disclosed to third parties within the scope of legally permissible order processing, and if this should be required by law or ordered by the authorities.

> *Comment: Should member data be forwarded to third-parties, which data (e.g. name, address and email address), for what purpose (e.g. advertising) and to which parties (e.g. sponsor) must be clear from the provision. The umbrella organisation of a section is also deemed a third party.*

Otherwise, member data is processed in accordance with the provisions of Swiss data protection legislation and the privacy policy on the association's website.

> *Comment: Every association create a privacy policy to fulfil its legal data protection information obligation, which it preferably publishes on its website.*