Protection des données: que doivent savoir les associations?

Auteur et autrices: Roman Baumann Lorant, docteur en droit, avocat
Fanni Dahinden, Maja Graf et Sibylle Sutter, vitamine B

La nouvelle loi sur la protection des données (LPD) et la nouvelle ordonnance sur la protection des données (OPDo) entreront en vigueur en Suisse le 1er septembre 2023. Ces bases juridiques règlent la gestion conforme à la loi des données dites personnelles. La nouvelle loi s'adapte à la numérisation et au Règlement européen sur la protection des données (RGPD). La protection des données n'est pas une chicane administrative: il s'agit de protéger les personnes et leurs droits de la personnalité.

1. Loi fédérale sur la protection des données

La nouvelle loi sur la protection des données ne prévoit pas de directives spécifiques pour les associations. Elle ne prévoit pas non plus une information proactive des membres au 1er septembre 2023. *En revanche, une déclaration de protection des données sera dès lors obligatoire.*

1.1 Qui est responsable de la protection des données au sein d'une association?

Une association dispose de nombreuses données personnelles, notamment celles de ses membres (→ cf. chiffre 1.4), qu'elle doit gérer avec soin. Le comité de l'association est responsable de leur gestion conforme à la loi sur la protection des données. Il est en particulier responsable du fait que l'association dispose d'une déclaration de protection des données.

1.2 À quoi sert une déclaration de protection des données?

La déclaration de protection des données (DPD) ne sert pas à demander d'éventuels consentements relatifs au traitement des données. Par le biais de la DPD, l'association remplit en revanche son *devoir d'information* envers les personnes dont elle traite les données personnelles, p. ex. en sauvegardant les données des personnes visitant le site Internet ou en traitant et transmettant les données saisies dans le cadre d'une adhésion. Il ne faut donc pas accepter la DPD, mais en prendre connaissance. Le plus simple est de placer la DPD sur le site Internet de l'association, idéalement dans le pied de page (footer).

Si le traitement des données nécessite un consentement, ce dernier doit être demandé *séparément* à toutes les personnes dont les données sont traitées (→cf. chiffre 1.6).

1.3 Que doit contenir la déclaration de protection des données?

- Explications générales et renseignements relatifs à l'association

- Énumération des données collectées et traitées
- Description des buts du traitement des données
- Mention des cookies, du tracking, des plugins de médias sociaux et d'autres technologies en lien avec l'utilisation du site Internet
- Transmission de données à des tiers et, le cas échéant, transmission de données à l'étranger
- Durée de conservation des données personnelles
- Sécurité des données
- Explication relative aux droits des personnes concernées
- Personne à contacter au sein de l'association
- Modification de la DPD (possible unilatéralement et à tout moment)

1.4 Qu'entend-on par données personnelles?

Les données personnelles sont toutes les informations qui se rapportent à une personne physique identifiée ou identifiable. Font donc partie des données personnelles toutes les données des membres d'une association telles que: nom, adresse postale et e-mail, numéros de téléphone, etc. mais aussi les *adresses IP (*séquence de chiffres permettant d'identifier explicitement tout appareil connecté à Internet et de remonter ainsi à son détenteur ou sa détentrice).

Sont considérées comme particulièrement sensibles les données relatives aux positions et activités religieuses, politiques ou idéologiques, les données médicales, en lien avec la sphère intime et la race/l'ethnie, les données génétiques et biométriques, les données relatives à des procédures administratives et pénales ainsi qu'à des mesures d'aide sociale. Si une association traite ce type de données, elle doit être particulièrement prudente, car elle doit satisfaire à des exigences plus strictes. Il est alors recommandé de demander conseil à un-e spécialiste de la protection des données.

1.5 Que signifie «traiter des données»?

Cela comprend en principe toute action impliquant des données, notamment la collecte (p. ex. collecte d'adresses via un formulaire pour l'inscription à une newsletter), la sauvegarde, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la transmission de données. Le traitement doit se faire selon *les principes de base* suivants:

Transparence: une information claire et complète au sujet du but et de l'étendue des données personnelles traitées est obligatoire.

Proportionnalité: seule la collecte des données personnelles nécessaires pour atteindre le but recherché est autorisée. La constitution de réserves de données est interdite. Pour envoyer la facture de la cotisation annuelle ou l'invitation à l'assemblée générale, l'adresse e-mail des membres suffit p. ex. D'une manière générale, il est interdit de collecter et de traiter plus de données personnelles que celles qui sont véritablement nécessaires à l'activité de l'association.

Finalité: les données des membres ne peuvent être traitées que dans le but indiqué lors de leur collecte, prévu par la loi ou qui ressort des circonstances.
Les adresses e-mail saisies pour l'envoi de la facture de la cotisation annuelle ne peuvent donc pas

être utilisées pour envoyer de la publicité ni être transmises à des tiers sans le consentement des personnes concernées.

Conservation: les données doivent être effacées dès qu'elles ne sont plus nécessaires au traitement prévu, sauf si elles sont soumises à une obligation de conservation légale. Il s'agit p. ex. de l'obligation de conservation des rapports annuels, comptes annuels et justificatifs comptables pendant 10 ans.

Sécurité: l'association doit garantir une sécurité des données appropriée au risque par le biais de mesures organisationnelles et techniques (p. ex. cryptage, système de sauvegarde, limitation d'accès, mots de passe, instruction au personnel, etc.).

1.6 Quand un consentement est-il nécessaire?

En Suisse, le traitement des données ne requiert en principe pas d'autorisation, sauf dans les cas suivants:

- lorsque les principes susmentionnés ne sont pas respectés (→ cf. chiffre 1.5),
- lorsque les données sont traitées à l'encontre de la manifestation expresse de la volonté de la personne concernée ou
- lorsque des données personnelles sensibles sont communiquées à des tiers (→ cf. chiffre 1.4).

Pour parer à toute éventualité, il peut être judicieux de demander un consentement par défaut, p. ex. dans le cadre du formulaire d'adhésion à l'association.

1.7 Quand est-ce que l'association est autorisée à transmettre des données personnelles à des tiers?

Pour qu'une association soit autorisée à transmettre des données personnelles (p. ex. des adresses ou listes d'adresses) à des tiers, elle doit obtenir *le consentement des personnes concernées* ou les informer avant la transmission des données en leur donnant la possibilité de s'y opposer. Une mention précisant quand les données peuvent être transmises à des tiers de manière appropriée peut être ancrée dans les statuts de l'association ou dans la DPD. Les membres ont le droit d'interdire la communication de leurs données personnelles (droit d'opposition) ou de révoquer en tout temps un consentement accordé au préalable.

La transmission de données personnelles à des tiers dans le cadre de l'exécution d'un mandat (p. ex. imprimerie, service de newsletter, prestataire de services Cloud, etc.) est permise sans autorisation préalable si les conditions suivantes sont remplies (art. 9 LPD):

- L'information relative à la transmission de données dans le cadre de l'exécution d'un mandat est visible dans la DPD.
- Il existe un contrat avec le sous-traitant.
- Ce dernier traite les données comme l'association serait elle-même autorisée à le faire.
- Il n'existe pas d'interdiction légale ou contractuelle.
- L'association s'est assurée que le sous-traitant est en mesure de garantir la sécurité des données (vérification du sérieux).

Important: si le sous-traitant a son siège à l'étranger, référez-vous à l'art. 16 LPD sur la communication transfrontalière de données personnelles.

Si la loi prévoit la transmission de données de membres à des tiers (p. ex. lors d'une procédure pénale), l'association est autorisée et obligée de transmettre lesdites données.

1.8 Quand est-ce qu'une association est autorisée à transmettre des données en interne?

En général, il faut, dans ce cas aussi, *l'autorisation de chaque membre ou une information préalable* sur le but de la transmission des données avec la possibilité de refus. La transmission appropriée de données de membres à d'autres membres peut être réglée dans les statuts. Cela concerne p. ex. l'information sur la transmission de listes contenant des données de membres à des associations faîtières ou la remarque que la liste des membres est mise à disposition de tous les membres dans la partie réservée aux membres du site Internet. Dans ce cas également, les membres ont le droit de s'y opposer ou peuvent révoquer en tout temps un consentement accordé au préalable.

La transmission des données des membres au sein de l'association est en outre autorisée lorsqu'elle est nécessaire pour l'exercice des droits de membre (p. ex. convocation à une assemblée générale extraordinaire, art. 64 al. 3 CC). Mais dans ce cas, seule la quantité de données nécessaire à l'exercice des droits devrait être transmise (p. ex. noms et adresses).

1.9 À quoi faut-il veiller lors de la publication de données de membres?

La publication de données de membres (site Internet, bulletin ou journal associatif et autres) est soumise aux règles régissant la divulgation de données personnelles à des tiers. Lors de la publication de données personnelles sur le site Internet en particulier, il faut vérifier soigneusement l'utilité de la communication.

Si des données personnelles spécifiques doivent être rendues accessibles aux seuls membres, il est recommandé de leur créer un espace fermé et réservé sur le site. Mais même la publication de données personnelles dans un espace protégé requiert le consentement de chaque membre, qui doit avoir la possibilité de le révoquer en tout temps.

Attention: la publication de photos sur lesquelles des personnes sont présentes nécessite l'autorisation de chaque personne reconnaissable (→ cf. entrée «Droit à l'image» dans le glossaire de vitamine B, https://www.vitamineb.ch/400_mots_cles/droit-a-l-image/).

Le site «Collecte et utilisation des données au sein d'une association» du Préposé fédéral à la protection des données constitue la base de clarification des directives auxquelles sont soumises les associations à cet égard (→ cf. chiffres 1.7 à 1.9):

https://www.edoeb.admin.ch/edoeb/fr/home/datenschutz/freizeit_sport/datenbearbeitung_vereine.html (dernière visite du site le 8 juin 2023)

2. Règlement de l'UE sur la protection des données: importance pour les associations suisses

Le Règlement européen sur la protection des données (RGPD) est entré en vigueur le 25 mai 2018. De nombreux points de la loi suisse sur la protection des données ont été adaptés au RGPD.

2.1 Quelles organisations suisses sont soumises au RGPD?

Les entreprises et organisations suisses (aussi les associations) qui traitent les données personnelles de personnes physiques situées sur le territoire de l'UE doivent se conformer au RGPD lorsqu'elles:

- traitent les données dans le cadre d'une succursale dans l'UE ou d'un sous-traitant ayant son siège au sein de l'UE;
- proposent à ces personnes de la marchandise ou des services (payants ou gratuits) ou montrent une *intention* claire de le faire, p. ex. si elles s'adressent à de potentiel-les client-es situé-es dans l'UE sur leur site Internet ou affichent leurs prix dans une devise courante au sein de l'UE;
- analysent le *comportement* de personnes dans l'UE (art. 3 al. 2 lettres a et b RGPD), p. ex. suivi du comportement d'utilisation de personnes de l'UE sur leur site Internet à l'aide de Google Analytics.

2.2 Quand est-ce que le RGPD autorise l'utilisation / le traitement de données personnelles?

Conformément à l'art. 6 al. 1 RGPD, le traitement de données personnelles, p. ex. via formulaire de contact sur le site Internet, est licite si, pour l'essentiel,

- la personne concernée (ou le titulaire de la responsabilité parentale pour les enfants) a donné son consentement,
- le traitement des données personnelles est nécessaire à l'exécution d'un contrat.
- le traitement est nécessaire au respect d'une obligation légale (p. ex. obligation de conservation de documents professionnels),
- s'il y a un intérêt légitime (utilité).

Attention: le RGPD constitue un ensemble de règles complexes relatif au traitement de données personnelles. Comme il peut concerner les associations suisses, notamment en raison de leur présence en ligne (site Internet, médias sociaux, etc.), il est recommandé de consulter un-e spécialiste pour bénéficier d'un conseil plus détaillé.

3. Quelles mesures sont exigées de la part des associations?

3.1 Mise en ligne d'une déclaration de protection des données sur le site Internet

Le site Internet de l'association doit expliquer en langage simple aux utilisateurs et utilisatrices qui traite leurs données, comment, où et dans quel but. La déclaration de protection des données doit également mentionner le recours à des services externes (p. ex. outils de publication de newsletters, médias sociaux ou instruments d'analyse) dans la mesure où ceux-ci collectent des données personnelles lors de la visite sur le site Internet.

3.2 Information concernant les cookies

Les «*cookies*» sauvegardent automatiquement des fichiers texte qui se rapportent aux internautes visitant un site Internet et permettent de les identifier. Si une association utilise des cookies sur son site Internet, elle doit impérativement le mentionner (soit dans la DPD ou via un bandeau cookies). Nombre de systèmes de gestion de contenu (logiciels de création de sites Internet) utilisés aujourd'hui recourent par défaut à des cookies. C'est pourquoi il est, de manière générale, recommandé de placer, pour information, un bandeau cookies. Ce dernier devrait être clairement visible lors de la première visite du site Internet, sans toutefois cacher des indications obligatoires comme le lien vers les mentions légales ou la déclaration de protection des données.

3.3 Anonymisation des adresses IP collectées par les outils d'analyse

L'utilisation de services d'analyse de site Internet (p. ex. Google Analytics) doit être documentée dans la DPD publiée sur le site. La possibilité de se rétracter doit être garantie. Les adresses IP étant considérées comme des données personnelles, il est impératif de garantir que l'outil d'analyse les collecte sous forme abrégée (à l'aide d'une fonction d'anonymisation). Adressez-vous à ce propos à votre opérateur de site Internet.

3.4 Prudence lors de l'utilisation des médias sociaux

Si votre association utilise les médias sociaux, aucune donnée des personnes visitant le site ne peut être collectée sans leur consentement. La DPD doit informer de l'utilisation d'offres des médias sociaux et du type de plugins de médias sociaux utilisés (p. ex. boutons «j'aime», «partager», etc.). En parallèle, il faut attirer l'attention des internautes sur leur droit de révocation.

4. Comment procéder?

1. Au sein de l'association, définissez une personne chargée de la protection des données et de la garantie d'une sécurité adéquate de celles-ci.
2. Sensibilisez les membres du comité et le personnel à la protection des données.
3. Vérifiez les processus internes et obtenez une vue d'ensemble des données personnelles traitées dans votre association: quelles données sont collectées? D'où proviennent-elles? Où sont-elles sauvegardées? Qui peut y accéder?
4. Vérifiez si votre association est concernée par le RGPD de l'UE.
5. Dans la mesure du possible, établissez un répertoire de vos activités de traitement des données (cette mesure n'est obligatoire qu'à partir de 250 employé-es). Seul ce type de répertoire vous permet d'obtenir la vue d'ensemble nécessaire des activités de traitement, peu importe que vous utilisiez Excel, Mindmap ou un outil professionnel en ligne.
6. Effectuez les modifications suivantes nécessaires:
   - Contactez votre opérateur de site Internet et discutez des modifications à effectuer sur le site. Rédigez une *Déclaration de protection des données* ou vérifiez le cas échéant la version que vous utilisez.
   - Adaptez votre *formulaire d'adhésion* (déclaration de consentement).
   - Envisagez d'ajouter un article relatif à la protection des données lors d'une prochaine *révision des statuts*.
   - Définissez le *processus en cas de demande de renseignements* en lien avec le traitement des données (art. 25 ss LPD). Vous devez être en mesure de fournir les informations nécessaires dans un délai de 30 jours.
   - Élaborez éventuellement des *Lignes directrices / Directives en matière de protection des données.*
   - Vérifiez les *contrats conclus avec des sous-traitants***.**
7. En cas de doute, contactez un-e juriste ou le Préposé fédéral à la protection des données: https://www.edoeb.admin.ch/edoeb/fr/home/deredoeb/kontakt.html
8. Informez vos membres des modifications effectuées (p. ex. via newsletter ou lors de la prochaine assemblée générale). Ce n'est pas une obligation selon la LPD, mais cela renforce la sensibilisation et montre que vous prenez la protection des données au sérieux.
9. La protection des données fait partie de la gestion du risque. Soyez prudent-e en matière de collecte de données personnelles et vérifiez régulièrement vos mesures techniques et organisationnelles.
10. Actualisez régulièrement les données de vos membres (p. ex. lors de l'assemblée générale).
11. Effacez les données dont vous n'avez plus besoin et qui ne sont pas soumises à une obligation de conservation.

5. Informations complémentaires

5.1 La protection des données en Suisse (LPD):

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

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

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

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

(dernière visite le 15 mai 2023)

5.2 La protection des données au sein de l'UE (RGPD):

https://www.kmu.admin.ch/kmu/fr/home/faits-et-tendances/digitalisation/protection-des-donnees/reglementation-ue-pour-la-protection-des-donnees.html

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

https://www.profonds.org/fr/aktuell/datenschutz-nutzen-sie-unsere-hilfmittel/

(dernière visite le 15 mai 2023)

6. Exemples de textes

Vous trouverez ci-dessous des modèles pour informer les membres de votre association ou les personnes abonnées à votre newsletter.

1. E-mail aux membres / personnes abonnées à la newsletter

Chers membres,

Nous avons modifié notre déclaration de protection des données, afin de la rendre compatible avec la nouvelle loi fédérale sur la protection des données (LPD). Vous trouverez des informations détaillées sur notre site Internet, sous *Déclaration de protection des données*.

Chères et chers abonné-es à notre newsletter,

La nouvelle loi fédérale sur la protection des données entre en vigueur le 1.9.2023. C'est l'occasion pour nous d'actualiser les données de notre clientèle et des personnes intéressées par nos activités. Si vous ne désirez plus recevoir d'informations relatives à nos nouveautés et manifestations, vous pouvez vous désabonner de la newsletter en cliquant sur le lien ci-dessous. Vos données seront alors supprimées de notre liste de diffusion. Dans le cas contraire, nous partirons du principe que vous souhaitez continuer à recevoir nos informations.

2. Bandeau cookies

[Version courte pour pied de page]
Nous utilisons des cookies pour vous offrir la meilleure expérience possible sur notre site Internet. Sous Paramètres *[lien]*, vous trouverez des informations par rapport au type de cookies utilisés et pourrez les désactiver.

[Explications via lien]
Ce site Internet utilise des cookies pour vous offrir la meilleure expérience possible lors de votre visite. Les informations des cookies sont sauvegardées dans votre navigateur et permettent certaines fonctionnalités, p. ex. de vous reconnaître lorsque vous revenez sur notre site Internet. Grâce aux cookies, notre équipe comprend mieux quelles parties du site sont particulièrement intéressantes et utiles pour vous.
Vous trouverez de plus amples informations sous Déclaration de protection des données *[lien]*

3. Déclaration de protection des données sur le site Internet

Obtenez une vue d'ensemble de la façon dont votre association traite les données personnelles et structurez votre déclaration de protection des données en conséquence. Sur Internet, vous trouverez des exemples qui pourront vous aider à formuler la déclaration de protection des données de votre association (p. ex. sur le site de vitamine B): https://www.vitamineb.ch/a-propos-de-nous/donnees

4. Formulation type pour les statuts

Art. [numéro] **Protection des données**

L'association ne collecte auprès de ses membres que les données personnelles nécessaires à la réalisation de ses objectifs. Le comité veille à ce que la sécurité des données soit adaptée au risque encouru.

Les données des membres, à savoir le nom, l'adresse, le numéro de téléphone ainsi que l'adresse e-mail [mentionner d'éventuelles autres données] sont communiquées à tous les membres de l'association.

Variante: les données des membres ne sont pas communiquées aux autres membres, à moins qu'une disposition légale ne le prévoie.

> *Commentaire: les données des membres pourraient être nécessaires aux membres pour qu'ils puissent exercer leurs droits (p. ex. convocation à une assemblée générale extraordinaire conformément à l'art. 64, al. 3, CC).*

Les données des membres, notamment [préciser quelles données], sont publiées sur le site web, dans la newsletter ainsi que dans le bulletin d'information de l'association [éventuellement d'autres supports de publication] . Par ailleurs, les données ne sont communiquées à des tiers que dans le cadre d'un traitement par délégation autorisé par la loi et si cela est prescrit par la loi ou ordonné par les autorités.

> *Commentaire: si des données de membres doivent être transmises à des tiers, la disposition doit indiquer quelles données (p. ex. nom, adresse et adresse e-mail) sont transmises à quel tiers (p. ex. sponsor) et dans quel but (p. ex. publicité). L'association faîtière d'un secteur est également considérée comme un tiers.*

Par ailleurs, le traitement des données des membres s'effectue conformément aux dispositions de la législation suisse sur la protection des données et à la déclaration de protection des données figurant sur le site web de l'association.

> *Commentaire: pour satisfaire à son obligation d'information en matière de protection des données, chaque association doit rédiger une déclaration de protection des données qu'elle publiera de préférence sur son site web.*