

FICHE D'INFORMATION DROIT D'ACCÈS

1. SUPPRESSION DE DONNÉES

Lors d'une demande de suppression de données, il est important de réagir rapidement et correctement. Le délai de réponse de 30 jours est imposé par la loi et doit être respecté. La demande doit impérativement bénéficier d'une réponse. Lorsque la suppression des données a été réalisée, une confirmation écrite suffit. Si la demande de suppression des données n'est pas satisfaite, elle doit être refusée et l'action doit être justifiée.

Il y a généralement deux raisons pour lesquelles la suppression des données peut être refusée:

1. La personne est un-e membre actif-ive

En principe, nous avons le droit de savoir qui sont nos membres et de traiter leurs données pour les besoins de notre association. Si un-e membre actif-ive souhaite que ses données soient supprimées, il faut vérifier si cette demande entraîne son exclusion des activités scouts. Par exemple, la date de naissance est nécessaire pour participer à un camp ou à un cours. Avant de procéder à la suppression des données, le cas devrait être discuté avec la personne qui en fait la demande et il faudrait lui expliquer les conséquences de cette suppression. Il se peut aussi que la suppression des données ne soit possible qu'en quittant le groupe.

2. La personne a déjà participé à un camp ou à un cours J+S

Nous devons conserver les données des participant-e-s aux cours et aux camps pendant 10 ans. Dans de nombreux cas, il est donc possible de réduire les données, mais pas de les effacer. Les champs suivants doivent être conservés, même si une suppression des données est souhaitée :

- Nom
- Prénom
- Totem
- Sexe
- Date de naissance
- Numéro AVS



Procéder à une suppression de données

MiData

Pour l'instant, le processus actuel de suppression des données dans MiData ne change pas. Une simplification est en cours de planification et sera discutée au sein de la communauté Hito-bitto au cours de l'année 2023.

Procédure pour supprimer des données :

1. Remplacer le nom, le prénom et le totem par "!DELETE!"
2. Supprimer tous les autres champs concernant la personne

Le MSdS supprimera toutes les personnes avec "!DELETE!" comme totem dans les 30 jours à suivre.

Archives et autres systèmes

Tous les dépôts dans des clouds tels que Dropbox, Nextcloud, etc. qui contiennent des données de la personne concernée doivent être examinés et les données concernées doivent être supprimées. Si d'autres bases de données ou d'autres systèmes contenant des données personnelles sont utilisés, une suppression des données doit également y être effectuée.

Listes sur papier

Enfin, les listes sur papier qui contiennent des données personnelles de la personne concernée doivent également être détruites.

Information à des tiers

Si d'autres entreprises ont traité les données de la personne concernée, elles doivent également être informées de la suppression des données. Pour exercer le droit d'accès, le droit à l'arrêt du traitement des données et à leur suppression auprès de la BDNS, il est possible de transmettre le contact des conseillers en protection des données de l'OFSPD (info@baspo.ad-min.ch).

Communication à d'autres niveaux

Par ailleurs, il peut arriver que des personnes soient actives à la fois dans un groupe et dans une association cantonale ou au sein du Mouvement Scout de Suisse. Afin d'éviter que la demande de suppression n'atteigne qu'un seul niveau, la personne qui demande une suppression doit être informée de l'existence des autres niveaux. Pour le MSdS, il est également possible de donner l'adresse e-mail protectiondesdonnees@msds.ch.



2. DROIT D'ACCÈS

"Conformément à la loi fédérale sur la protection des données, toute personne a le droit de savoir quelles données la concernant sont enregistrées, et peut – si nécessaire – les faire effacer ou rectifier. Ce droit d'accès permet à chacun de garder le contrôle des données récoltées à son sujet. Chaque personne doit toutefois agir elle-même pour exercer ce droit."

PPPDT sur le droit d'accès

Lorsque ton groupe reçoit une demande d'accès, il est important d'y répondre dans les 30 jours. Pour ce faire, il faut d'abord s'assurer que la personne qui fait la demande est autorisée à recevoir les données demandées. Une preuve d'identité peut et doit être fournie pour s'assurer que les données peuvent être envoyées à la personne.



Pour les données concernant des adultes, la demande doit en principe provenir de la personne concernée. S'il s'agit de données concernant des enfants, les tuteur·trice·s légaux·ales peuvent également demander un accès aux données.

Qu'est-ce qui fait partie d'une demande d'accès aux données ?

Les renseignements sur les données doivent d'une part montrer toutes les données enregistrées concernant la personne. Le fichier peut contenir des textes, des listes, des profils et des photocopies. De plus, les renseignements sur les données doivent également contenir les éléments suivants :

- Quelle est la finalité du traitement des données ?
- Existe-t-il des données sur la santé ou d'autres données sensibles ?
- Qui a accès aux données ?
- À qui les données ont-elles été transmises ?

En plus des renseignements sur les données, la personne qui fait la demande peut également demander une modification ou une correction des données enregistrées. Dans ce cas, les données concernées doivent être adaptées dans la mesure où elles sont effectivement erronées.

Plus d'informations sur le droit d'accès : **Fedlex, art. 8 Droit d'accès**

