MIGROS

Directive sur la protection des données
R–1 –0006 version 2.1

Cette directive concrétise le principe contenu dans le code de conduite du groupe Migros par rapport aux données personnelles:

> *« Nous respectons la vie privée de nos clients, collaborateurs et partenaires commerciaux. Nous ne travaillons avec des données à caractère personnel que si cela est nécessaire pour les finalités poursuivies. Nous traitons ces données avec soin et les protégeons par des mesures de sécurité appropriées.*
>
> *La confiance de nos clients, collaborateurs et partenaires commerciaux est notre priorité absolue. Nous expliquons aux personnes concernées de manière transparente et compréhensible pourquoi nous traitons leurs données. Nous utilisons les données personnelles uniquement et toujours à des fins légales et de manière transparente.*
>
> *Lors du développement de nouveaux produits et dans le cadre des projets, nous accordons une attention toute particulière à la protection des données. Notre objectif est l'intérêt du client lorsque nous utilisons des technologies nouvelles ou novatrices, en tenant compte des effets sur les individus et la société. »*

Des réponses aux questions concernant cette directive peuvent être obtenues auprès du coordinateur local de la protection des données, auprès d'un éventuel service juridique local et/ou auprès de la Direction Legal & Compliance de la Fédération des coopératives Migros.

Cette directive a été adoptée en allemand. En cas de problèmes d'interprétation et de décalages dus à la langue, la version allemande de la présente directive (y compris les fiches correspondantes) prime sur les versions en d'autres langues.

Édition: Direction Legal & Compliance FCM
Approbation: Direction générale FCM
Domaine d'application: groupe Migros

L’essentiel en bref

Domaine d’application. Cette directive s’applique à toutes les entreprises du groupe Migros et s’applique à tout traitement de données personnelles. Il s’agit de tout processus en lien avec des informations qui se rapportent à une personne identifiée ou identifiable.

Principes applicables au traitement. Nous traitons les données personnelles exclusivement en conformité avec la finalité annoncée et uniquement de la façon que l’on attend légitimement de nous. Nous ne collectons pas davantage de données que ce qui est nécessaire pour la finalité du traitement.

Base pour le traitement. Nous traitons uniquement les données personnelles si cela est nécessaire pour l’exécution d'un contrat ou pour le respect d’une obligation légale, si la personne concerné a accepté activement le traitement ou si nous sommes en mesure de faire valoir un intérêt prépondérant dominant dans le traitement de données.

Transparence. Nous informons la personne concernée du traitement de ses données personnelles d’une manière précise, transparente, compréhensible et aisément accessible. Si possible, l’information est communiquée avant la collecte des données ou en même temps que celle-ci.

Droits des personnes concernées. Nous respectons les droits à l’information, à la rectification, à la suppression, à l’opposition, etc., des personnes concernées. Les demandes en ce sens sont en principe traitées gratuitement, dans les délais impartis et de manière appropriée.

Transmission à des tiers. Nous ne transmettons de données personnelles à un autre destinataire que s’il existe un fondement juridique suffisant pour cela et si cela est compatible avec la finalité du traitement annoncée.

Transmission à l’étranger. Des données personnelles ne peuvent être transmises à l'étranger que s’il existe un niveau de protection des données approprié dans le pays de destination ou si des mesures de protection particulières ont été prises, comme par exemple des garanties contractuelles.

Traitement par délégation. Le traitement de données personnelles ne peut être transmis à une autre entreprise Migros ou à un prestataire de services externe que sur la base d’un accord écrit.

Inventaire des traitements de données. Tous les traitements de données existants et nouveaux sont documentés dans un registre des traitements de données.

Privacy by Design (respect de la vie privée dès la conception). Nous prenons en considération la protection des données dès la phase de conception. Dans le cas de traitements de données particulièrement risqués, il convient d’effectuer à temps une analyse d’impact relative à la protection des données.

Sécurité des données. Nous prenons des mesures appropriées sur le plan technique et organisationnel afin de protéger les données personnelles contre la perte, l’accès non autorisé ou le traitement non autorisé.

Violation des données. En cas d’atteinte à la protection des données, il faut immédiatement impliquer les instances internes compétentes. Le cas échéant, il existe une obligation de déclaration à l’autorité de contrôle compétente et/ou aux personnes concernées.

Organisation de la protection des données. Chaque entreprise Migros désigne une personne en charge des questions de protection des données. Le cas échéant, il faut également désigner officiellement une représentation UE et/ou un délégué à la protection des données.

Sommaire

1. Introduction

Les collaborateurs, les clients et les autres personnes, dont les données personnelles sont traitées par la fédération des coopératives Migros, par ses coopératives affiliées et par les filiales respectives (ci-après: « **Entreprises du Groupe Migros** »; conjointement « **Groupe Migros** »), attendent de nous une gestion responsable et légale de leurs données personnelles. Nous assumons notre responsabilité dans la gestion de données personnelles et nous nous efforçons de protéger, dans tout le Groupe Migros, les données personnelles en conformité avec la législation applicable.

Le pronom « nous » et ses dérivés, dans cette directive sur la protection des données, désignent aussi bien les entreprises du Groupe Migros que les collaborateurs Migros dans leur domaine respectif de responsabilité et d'activité.

Certains des termes utilisés dans la présente directive sont expliqués dans le glossaire ci-joint.

2. Domaine d'application

Cette directive établit des principes généraux concernant la gestion de données personnelles au sein du Groupe Migros, et ce sur la base du Loi fédérale sur la protection des données (« **LPD** ») et du règlement général européen sur la protection des données (« **RGPD** »). Elle est contraignante pour toutes les entreprises du Groupe Migros.

Cette directive est applicable à tout **traitement de données personnelles**. Les termes « données personnelles » et « traitement » doivent être compris au sens très large:

- Les « **données personnelles** » correspondent à toutes les informations qui se rapportent à une personne physique identifiée ou identifiable. Une personne physique est identifiable lorsqu'elle peut être identifiée directement ou indirectement, par exemple du fait de l'attribution d'informations sur une identification, comme un nom, un numéro d'identification, sur des sites, sur une identification en ligne ou sur d'autres caractéristiques relatives aux personnes.
  Exemples: informations personnelles (nom, date de naissance, etc.), coordonnées (adresse, numéro de téléphone, e-mail, etc.), caractéristiques physiques (sexe, couleur des yeux, etc.), numéros d'identification (numéro AVS, etc.), informations financières (numéro de compte, revenus, patrimoine, etc.), données relatives à la position géographique, adresse IP, numéros d'identification d'appareils, données relatives à une utilisation ou un comportement, préférences et habitudes.
- Le « **traitement** » correspond à tout processus lié aux données personnelles, indépendamment du fait que le processus en question soit automatisé ou non.
  ***Exemples*:** collecte, saisie, organisation, classification, sauvegarde, adaptation ou modification, relevé, interrogation, utilisation, divulgation par transmission, traitement ou autre forme de mise à disposition, comparaison ou association, limitation, suppression, anonymisation et destruction.

Cette directive n'est pas applicable aux (1) informations de personnes morales et de sociétés de personnes (mais aux données des personnes physiques agissant pour leur compte, comme les interlocuteurs, les membres d'organes de direction, etc.), ainsi qu'aux (2) recettes, plans marketing, documents stratégiques, calculs de prix, données financières et informations similaires non liées aux personnes (cependant, de telles informations peuvent constituer des secrets commerciaux).

Cette directive est complétée par des fiches, des instructions et des règlements supplémentaires concernant la gestion de données personnelles (par ex. règlements concernant le personnel, règlements concernant l'utilisation de l'informatique, etc.). En outre, si le droit local applicable ou certaines entreprises du Groupe Migros ou leurs services prévoient des règles plus strictes que celles définies dans la présente directive, ces règles plus strictes doivent également être respectées.

3. Principes pour le traitement de données personnelles

Tous les principes ci-après doivent toujours être respectés quand des données personnelles sont traitées.

(a) **Affectation claire de la responsabilité**: pour chaque traitement de données, au moins une entreprise est responsable. Des responsables communs et/ou sous-traitants peuvent par ailleurs être impliqués. Les rôles des entreprises impliquées doivent toujours être définis et représentés dans un contrat (voir à ce sujet le chiffre 8).

(b) **Légitimité du traitement:** les données personnelles ne peuvent être traitées qu'en conformité avec la loi. Surtout, nous ne traitons les données personnelles que si nous pouvons nous appuyer sur un fondement juridique suffisant (voir à ce sujet le chiffre 4).

(c) **Équité**: nous traitons les données personnelles de manière équitable et uniquement de la manière qu'attend de nous la personne concernée, et ce à juste titre. Nous évitons les discriminations, en particulier lorsque nous établissons un profil d'une personne concernée.

(d) **Transparence**: lorsque nous nous procurons des données personnelles auprès de la personne concernée elle-même ou auprès d'autres sources, nous informons les personnes concernées activement, suffisamment tôt, de façon détaillée et compréhensible, du traitement de leurs données personnelles (voir à ce sujet le chiffre 5).

(e) **Finalité**: les données personnelles ne doivent être collectées et traitées qu'à des fins qui ont été indiquées de manière transparente lors de l'acquisition ou qui sont compatibles avec la finalité indiquée. Cependant, si le traitement repose sur un consentement, ce consentement doit alors clairement inclure ces finalités.

(f) **Proportionnalité**: le traitement de données personnelles ne doit pas aller au-delà de ce qui est approprié et nécessaire pour atteindre l'objectif poursuivi par le traitement. L'accès aux données personnelles doit par principe être limité aux collaborateurs de Migros et aux entreprises du Groupe Migros qui en ont besoin pour accomplir leurs tâches.

(g) **Minimisation des données et limitation de la conservation**: il ne faut pas collecter et traiter davantage de données personnelles que nécessaire. Les données qui ne sont plus nécessaires à la finalité prévue doivent être effacées ou anonymisées, dans la mesure où des obligations ou des droits de conservation ne s'y opposent pas. Un concept d'effacement devrait exister pour chaque fichier de données et pour chaque traitement de données.

(h) **Exactitude**: les données personnelles doivent être correctes et, dans la mesure où elles ne doivent pas fournir uniquement des renseignements concernant l'état à un moment précis, toujours être à jour. Les données personnelles inexactes ou incomplètes doivent être corrigées ou complétées. Si cela n'est pas possible, elles doivent par principe être effacées ou anonymisées, dans la mesure où aucune obligation de conservation ne s'applique.

(i) **Sécurité**: La sécurité des données personnelles traitées par nos soins doit être garantie à tout moment de manière appropriée. Les données personnelles doivent en particulier être protégées contre la destruction, la perte, la modification ou la divulgation non autorisée. À cet effet, il convient d'évaluer suffisamment tôt les risques liés au traitement pour les personnes concernées et des mesures de protection appropriées doivent être prévues.

(j) **Documentation**: nous tenons des registres des traitements de données pour lesquels nous sommes compétents en tant que responsables ou chargés du traitement par délégation, et les tenons à jour. Nous documentons de manière appropriée tout traitement de données personnelles et les décisions essentielles prises lors du traitement (voir à ce sujet le chiffre 9).

4. Fondement juridique pour le traitement de données personnelles

Tout traitement de données personnelles doit s'appuyer sur un fondement juridique suffisant. Pour le traitement de données personnelles par des entreprises du Groupe Migros, les fondements juridiques suivants entrent principalement en ligne de compte:

(a) **Exécution d'un contrat**: le traitement est nécessaire pour la conclusion ou l'exécution d'un contrat (par ex. traitement de l'adresse d'une personne dans le cadre d'une commande).

(b) **Obligation légale**: le traitement est nécessaire pour respecter une obligation légale (par ex. dans le cadre d'obligations de conservation).

(c) **Consentement**: le traitement a lieu avec un consentement valable de la part de la personne concernée pour la finalité. ***Remarque:***
- Le consentement est valable uniquement s'il est accordé sans ambigüité, à des fins spécifiques, volontairement et en connaissance de cause.
- Le consentement doit être signifié par une action volontaire, par ex. au moyen d'une signature manuscrite, de l'activation d'une case à cocher ou de l'adaptation de réglages usine. Les cases à cocher préactivées, le fait de garder le silence ou la simple utilisation d'une prestation ne constituent pas un consentement valide.
- Le consentement peut être annulé à tout moment. L'annulation doit être possible de manière simple et sans ambigüité.
- Pour les enfants, les parents doivent signifier leur consentement ou l'approuver.

(d) **Intérêt prépondérant**: le traitement est nécessaire pour préserver un intérêt légitime de notre part ou de la part d'un tiers ***Remarque:***

- L'intérêt légitime doit être mis en balance avec les droits et les libertés de la personne concernée. Cette mise en balance doit être documentée. En cas de litige, il doit être possible de prouver que l'intérêt légitime prédomine.
- En aucun cas, un intérêt légitime n'est suffisant (1) pour le traitement de données relatives à la santé, de données biométriques/génétiques ainsi que d'autres données personnelles particulièrement sensibles ou (2) pour le traitement de données personnelles dans le cadre de décisions appliquées de façon automatisée (y compris le profilage), dans la mesure où celles-ci ont des conséquences considérables pour les personnes concernées.

5. Information sur le traitement de données personnelles

Nous informons les personnes concernées du traitement de leurs données personnelles d'une manière précise, transparente, compréhensible et aisément accessible. ***Remarque:***

- L'information sur le traitement de données doit être clairement séparée des autres faits et ne doit pas, en particulier, être mélangée avec d'autres sujets dans les conditions générales. En règle générale, nous informons les personnes concernées du traitement de leurs données personnelles dans une déclaration de protection des données spécifique.
- L'information concernant le traitement de données doit être réalisée dans un langage clair et simple. Lorsqu'il s'agit d'enfants, de personnes âgées et d'autres personnes vulnérables, nous veillons tout particulièrement à un langage et à une présentation des informations facilement compréhensibles.

L'information est en principe toujours communiquée avant la collecte des données ou en même temps que celle-ci. Ce n'est que lorsque nous ne collectons pas les données personnelles directement auprès de la personne concernée que l'information peut être fournie ultérieurement lors du premier contact direct avec la personne concernée ou lors de la première divulgation à un autre destinataire, et dans tous les cas, au plus tard dans un délai d'un mois après l'obtention des données.

L'information sur le traitement de données personnelles doit répondre au moins aux questions suivantes:

- Quelle(s) société(s) est/sont responsable(s) du traitement des donnéeset à qui les personnes concernées peuvent-elles s'adresser?
- Quelles sont les sources et les données utilisées?
- Pourquoi traite-t-on des données (finalité du traitement) et sur quel fondement juridique?
- De quelle manière peut-on annuler un éventuel consentement de traitement de données?
- À qui les données sont-elles transmises et à quelles fins?
- Des données sont-elles transmises à l'étranger – soit directement par le responsable, soit par un sous-traitant – et, si c'est le cas, quels sont les États ou régions concernés et quels sont les mécanismes de protection mis en œuvre pour garantir un niveau de protection des données approprié?
- Combien de temps les données sont-elles stockées?
- De quels droits de protection des données les personnes concernées disposent-elles (renseignement, correction, suppression, limitation, opposition, portabilité des données, plainte adressée à une autorité de contrôle)?
- Des décisions essentielles sont-elles prises de façon entièrement automatique et, si c'est le cas, selon quelle logique et avec quelles conséquences?
- Un profilage a-t-il lieu?
- Existe-t-il une obligation pour la personne concernée de mise à disposition de données et quelles sont les conséquences si les données ne sont pas mises à disposition?

À chaque communication de marketing direct, nous informons la personne concernée de son droit de s'opposer au traitement de ses données personnelles à des fins de marketing direct.

Dans le cas de services en ligne, nous signalons activement l'utilisation de cookies et d'autres technologies de traçage ainsi que leur finalité, et nous informons les utilisateurs de la possibilité de les désactiver.

6. Droits des personnes concernées

Toute entreprise du Groupe Migros qui traite des données personnelles en tant que responsable est tenue de permettre aux personnes concernées d'exercer leurs droits de manière simple. Les demandes en ce sens doivent par principe faire l'objet d'une réponse ou d'un traitement sous forme appropriée, et ce gratuitement et dans les délais, et la gestion de ces demandes doit être intégralement documentée.

Les personnes concernées ont, selon les conditions indiquées, en particulier les droits suivants:

(a) **Renseignements**: demander des renseignements concernant le traitement de leurs données personnelles et obtenir une copie des données traitées, dans la mesure où cela ne porte pas atteinte aux droits des tiers;

(b) **Correction**: faire corriger ou compléter les données personnelles inexactes ou incomplètes;

(c) **Suppression**: faire supprimer, sous certaines conditions, les données personnelles, par ex. lorsque le traitement est effectué à des fins de marketing ou s'il comporte des risques exceptionnels pour la personne concernée;

(d) **Opposition:** s'opposer à tout moment au traitement de données personnelles, notamment lors d'un traitement à des fins de marketing direct. Cela vaut également pour un profilage éventuel, dans la mesure où il est associé à un tel marketing direct. Une opposition peut entraîner une obligation de suppression;

(e) **Limitation du traitement**: faire limiter le traitement supplémentaire de données personnelles dans certaines conditions;

(f) **Vérification de décisions au cas par cas automatisées**: être informé des décisions qui sont prises automatiquement sans intervention humaine et qui entraînent pour la personne concernée des préjudices légaux ou autres importants, et prendre position par rapport à de telles décisions et les faire vérifier par une personne physique;

(g) **Portabilité des données**: se faire envoyer ou faire transférer à un autre responsable les données mises à disposition par leurs propres soins dans un format structuré, courant et lisible par machine.

Une correction, une suppression ou une limitation du traitement doit être notifiée aux destinataires éventuels des données personnelles concernées, dans la mesure où cette notification est possible et où le travail nécessaire n'est pas disproportionné.

En outre, les personnes concernées ont le droit de se plaindre à une autorité de contrôle par rapport à un traitement de données précis.

7. Communication de données personnelles à d'autres destinataires

Toute transmission, divulgation, mise à disposition, diffusion ou autre forme de notification de données personnelles à un autre responsable ou destinataire est autorisée uniquement lorsque la notification a été communiquée à la personne concernée, lorsque la notification s'appuie sur un fondement juridique suffisant (voir le chiffre 4) et lorsque la notification est compatible avec la finalité du traitement notifiée lors de la collecte des données.

Cela vaut aussi bien pour la notification à des entreprises en-dehors du Groupe Migros que pour la notification à une autre entreprise du Groupe Migros. En revanche, la transmission de données personnelles d'un service vers un autre service d'une même entreprise n'est pas considérée comme une notification (par ex. d'une direction de la FCM vers une autre direction de la FCM).

Pour des transmissions vers des destinataires à l'étranger (cela inclut également des entreprises étrangères du Groupe Migros), on applique en plus la condition préalable qu'un niveau de protection des données approprié existe dans le pays du destinataire. Un niveau de protection des données approprié existe en Suisse, mais également en particulier dans les pays membres de l'UE/EEE. Pour les autres pays destinataires, il convient de vérifier au cas par cas s'il existe un niveau de protection des données approprié. Contactez à cet effet la Direction Legal & Compliance de la FCM ou le service juridique local.

En l'absence d'un niveau de protection des données approprié dans le pays destinataire concerné, la transmission n'est autorisée que dans les cas suivants:

- Un contrat de transmission de données approprié a été conclu avec le destinataire, dans lequel le destinataire s'est engagé à assurer un niveau de protection des données approprié.
- La transmission est nécessaire pour exécuter un contrat avec la personne concernée ou pour traiter une demande de contrat de la personne concernée.
- Toutes les personnes concernées par la transmission ont expressément accepté la transmission à l'étranger après avoir été informées de façon détaillée et après une explication des risques associés.
- La transmission est nécessaire pour faire valoir, exercer ou défendre des droits.

Remarque: une transmission de données personnelles dans un pays ne disposant pas d'un niveau de protection des données approprié n'est autorisée qu'en accord avec la Direction Legal & Compliance FCM ou avec le service juridique local.

8. Traitement de données personnelles par délégation

Le traitement de données personnelles peut être transféré à une autre entreprise du Groupe Migros ou à un prestataire de services externe en tant que sous-traitant. Dans tous les cas, l'entreprise du Groupe Migros qui s'est procurée les données reste toutefois responsable du traitement de données personnelles vis-à-vis de la personne concernée.

Le recours à un sous-traitant est soumis aux conditions préalables suivantes:

- Lors du choix du sous-traitant, il a été veillé à ce qu'il puisse garantir la protection des données et en particulier la sécurité des données.
- La transmission de données personnelles au sous-traitant n'enfreint aucune obligation légale ou contractuelle de confidentialité.
- Avant la transmission de données personnelles au sous-traitant, un accord écrit de traitement de données par délégation est conclu.
  Remarque: si l'on utilise pas de document standard fourni par la Direction Legal & Compliance FCM pour l'accord de traitement de données par délégation, il est nécessaire que la Direction Legal & Compliance FCM ou le service juridique local donne son consentement avant le début du traitement de données par délégation.
- Si l'on mandate un sous-traitant dont le siège se situe à l'étranger, les conditions préalables du chiffre 7 doivent alors également être accomplies.

Les sous-traitants doivent notamment être tenus dans un accord de traitement de données par délégation de ne traiter les données personnelles que conformément à leur mandat et aux instructions du responsable, de ne pas les utiliser à d'autres fins et de garantir la sécurité du traitement de données.

En outre, les sous-traitants doivent être tenus d'aider le responsable à respecter la protection des données conformément aux exigences du droit de la protection des données et de l'accord de traitement de données par délégation, en particulier dans la gestion des atteintes à la protection des données et lors des analyses d'impact relative à la protection des données. Le recours à des sous-traitants par le sous-traitant requiert l'approbation du responsable.

Dans certains cas, il peut être difficile de faire la différence entre un sous-traitant et un responsable commun. Il convient également de conclure un accord entre les responsables communs, qui diffère toutefois d'un accord de traitement de données par délégation. En cas de doute, contactez la Direction Legal & Compliance de la FCM ou le service juridique local.

9. Documentation et planification de traitements de données

Tous les traitements de données existants et nouveaux doivent être documentés dans un registre des traitements de données. Un registre des des traitements de données doit être tenu aussi bien par le responsable que par un éventuel sous-traitant. Le «traitement de données » doit à cet égard être compris au sens large du terme et couvre toute opération planifiée liée aux données personnelles.

Le registre des traitements de données du responsable doit inclure au moins les indications suivantes:

- transcription du traitement de données
- entreprise(s) responsable(s)
- coordonnées de la personne responsable du traitement de données
- finalité(s) du traitement
- base du traitement
- Catégories de personnes concernées
- catégories de données personnelles traitées
- catégories de destinataires des données
- transmissions à l'étranger
- durée de conservation des données et concept de suppression
- description ou mention de mesures de sécurité sur le plan technique et organisationnel

Remarque: la documentation des traitements de données peut être réalisée de manière assistée par logiciel par le biais d'un questionnaire standardisé fourni par la Direction Legal & Compliance FCM.

Remarque: les entreprises du Groupe Migros (1) qui emploient moins de 250 collaborateurs, (2) dont le traitement de données ne comporte qu'un faible risque pour les personnes concernées, et (3) qui n'ont aucune activité importante dans l'UE ou l'EEE peuvent demander à la Direction Legal & Compliance de la FCM d'être dégagées de l'obligation de tenir un registre des traitements de données.

La protection des données doit être prise en considération dès la planification de nouveaux traitements de données, lors de modifications de traitements de données et lors de l'acquisition de produits et de prestations de services pour des traitements de données, de manière à ce que les risques pour les personnes concernées soient repérés suffisamment tôt et puissent être réduits de manière appropriée. Dans le cas de traitements de données particulièrement risqués, il convient d'effectuer en temps utile avant l'introduction du traitement de données en question une analyse d'impact relative à la protection des données. Une analyse d'impact relative à la protection des données est nécessaire en particulier dans les cas suivants:

- utilisation de nouvelles technologies ou de technologies d'un nouveau type ;
- évaluation complète d'aspects personnels essentiels (y compris le profilage) ;
- traitement étendu de données personnelles particulièrement sensibles (par ex. données relatives à la santé);
- surveillance systématique des zones accessibles au public (par ex. une surveillance vidéo).

Remarque: les analyses d'impact relative à la protection des données doivent être effectuées en accord avec la personne chargée localement des questions liées à la protection des données, avec un éventuel service juridique local et/ou avec la Direction Legal & Compliance FCM. Dans la mesure où l'entreprise concernée du Groupe Migros a désigné un délégué à la protection des données, il faut également faire appel à ce dernier.

10. Sécurité des données et déclaration des atteintes à la protection des données

Tous les collaborateurs de Migros qui traitent des données personnelles doivent veiller à la sécurité de ces données. Les données personnelles doivent être protégées, en particulier au moyen de mesures appropriées, contre la destruction, la perte, la modification accidentelles ou illégales ou la divulgation non autorisée. Sur le plan organisationnel, il faut veiller, en particulier au moyen d'un concept d'accès et d'autorisatoin, à ce que seuls les collaborateurs Migros qui en ont besoin pour exécuter leur fonction et leurs tâches aient accès aux données personnelles.

En cas d'atteinte à la protection des données engendrant des risques pour les personnes concernées, il faut informer le cas échéant l'autorité de contrôle compétente dans les plus brefs délais. S'il existe des risques élevés pour les personnes concernées ou si cela est nécessaire à leur protection pour d'autres raisons, une déclaration doit, le cas échéant, être en outre adressée aux personnes concernées.

Remarque : une atteinte à la protection des données doit immédiatement être signalée au supérieur hiérarchique ou aux instances compétentes dans l'entreprise concernée du Groupe Migros et, dans la mesure où

des risques pour les personnes concernées ne peuvent pas être exclus, à la Direction Legal & Compliance FCM.

11. Organisation de la protection des données

Il est de la responsabilité des entreprises du Groupe Migros de garantir une organisation appropriée de la protection des données, de façon à pouvoir respecter les exigences du droit de la protection des données et de la présente directive. L'organisation de la protection des données comprend en particulier la conception et la mise en œuvre de processus locaux de protection des données, la réalisation de formations appropriées et régulières et la tenue des registres et des documentations nécessaires.

Chaque entreprise du Groupe Migros désigne un interlocuteur interne en charge des questions en matière de protection des données (coordinateur de protection des données). Selon le domaine d'activité et le droit de protection des données applicable, les entreprises du Groupe Migros doivent également désigner un représentant dans l'UE et un délégué à la protection des données indépendant :

- **Représentant UE**: il faut désigner une personne physique ou morale en tant que représentant UE lorsque des marchandises ou des prestations de services sont proposées dans l'UE ou l'EEE ou si une observation du comportement est réalisée dans l'UE ou l'EEE (sauf si le traitement n'a lieu qu'occasionnellement et ne comprend pas le traitement étendue de données particulièrement sensibles) et, *en plus*, il n'existe aucun établissement dans un État membre de l'UE/EEE;

Délégué à la protection des données: il faut désigner une personne physique ou morale en tant que délégué à la protection des données lorsque des marchandises ou des prestations de services sont proposées dans l'UE ou si une observation du comportement est réalisée dans l'UE et si, *en plus*, l'activité principale comporte une surveillance étendue, régulière et systématique de personnes concernées ou le traitement de données particulièrement sensibles. Le droit local peut également exiger la désignation d'un délégué à la protection des données pour d'autres cas.
Les entreprises du Groupe Migros peuvent par ailleurs désigner volontairement un conseiller à la protection des données comme point de contact pour les personnes concernées et les autorités. Lorsqu'un conseiller à la protection des données a été désigné, il est possible dans certaines conditions de ne pas consulter l'autorité de contrôle suisse pour les traitements de données présentant des risques élevés pour la personnalité ou les droits fondamentaux des personnes concernées. Dans la mesure où une entreprise du Groupe Migros a désigné un délégué à la protection des données, celui-ci exerce également la fonction de conseiller à la protection des données.

12. Exigences du droit local

Dans la mesure où le droit local applicable à certaines entreprises du Groupe Migros prévoit des règles plus strictes ou différentes par rapport à la présente directive, ces règles doivent être respectées en plus des dispositions de cette directive.

13. Sanctions et obligation de déclaration

Les violations du droit de la protection des données et de la présente directive peuvent avoir des conséquences radicales pour les entreprises du Groupe Migros . Il y a en particulier un risque d'amendes élevées, de demandes d'indemnisation et d'atteinte à la réputation pour tout le Groupe Migros. En ce qui concerne les collaborateurs individuels Migros, les violations du droit de la protection des données et de cette directive peuvent entraîner des conséquences pénales, des mesures disciplinaires relevant du droit du travail (y compris le licenciement) et des prétentions du Groupe Migros à leur encontre.

Les collaborateurs Migros sont tenus de notifier immédiatement à leurs supérieurs hiérarchiques ou aux services indépendants compétents au sein de leur entreprise toute violation du droit de la protection des données et de la présente directive et toutes autres circonstances importantes qui concernent cette directive sur la protection des données. Si cela n'est pas possible pour des motifs déterminés ou si cela n'aboutirai pas à un résultat, ils peuvent s'adresser directement à la Direction Legal & Compliance FCM.

14. Responsabilités

Les responsabilités suivantes existent pour le respect de la présente directive :

Les collaborateurs Migros	• sont responsables, dans leur domaine de responsabilité et d'activité, du respect des principes définis dans la présente directive concernant la gestion des données personnelles
Les propriétaires de données/de processus	• sont des unités opérationnelles qui décident de la finalité et du contenu d'un fichier ou d'un traitement de données • assument la responsabilité principale, par rapport au respect du droit de la protection des données et de cette directive, du fichier concerné ou du traitement de données concerné • se chargent de la documentation du traitement de données concerné et, si nécessaire, de la réalisation d'une analyse d'impact relative à la protection des données • fournissent au service informatique de l'entreprise respective du Groupe Migros les informations nécessaires, de façon à ce que celui-ci puisse prendre les mesures techniques nécessaires au respect de la sécurité des données
Direction Legal & Compliance FCM	• conseille les collaborateurs Migros et les entreprises du Groupe Migros en matière de protection des données • gère le module Protection des données dans le cadre du système central de gestion de la Compliance • adopte pour tout le groupe des prescriptions minimales en matière de protection des données et peut fournir des documents types et d'autres modèles et instructions
Le délégué à la protection	• exerce une fonction indépendante de la ligne et affectée à la Direction Legal & Compliance FCM • exerce pour la FCM la fonction de délégué à la protection des données

des données de la FCM	au sens du RGPD et de conseiller à la protection des données au sens de la LPD • est responsable de la sensibilisation et de la formation des collaborateurs de la FCM • contrôle et surveille au sein de la FCM le respect du droit de la protection des données et de la présente directive • conseille la FCM et ses collaborateurs, ainsi que les coordinateurs de la protection des données des entreprises du Groupe Migros, sur les questions de protection des données • collabore avec les personnes concernées et les autorités compétentes • rend régulièrement compte à la direction générale et au Comité d'audit de la FCM
Coordinateur de la protection des données FCM	• coordonne les processus opérationnels de protection des données à la FCM • assure le suivi fonctionnel des coordinateurs de la protection des données décentralisés au sein des directions de la FCM • conseille les entreprises du Groupe Migros pour la mise en œuvre opérationnelle des exigences en matière de protection des données • assure le suivi de l'outil de gestion de la vie privée utilisé et le gère
Les organes dirigeants des entreprises du Groupe Migros	• garantissent le respect de cette directive et du droit de la protection des données dans leur entreprise • veillent dans leur entreprise à une organisation appropriée de la protection des données et à la mise en œuvre de processus adaptés
Les coordinateurs locaux de protection des données	• sont des interlocuteurs internes désignés par les différentes entreprises du Groupe Migros pour les questions de protection de données • exercent pour l'entreprise concernée la fonction d'interlocuteur central de la Direction Legal & Compliance FCM en matière de protection des données • coordonnent dans l'entreprise concernée la mise en œuvre des mesures nécessaires pour le respect de cette directive et du droit de la protection des données • sont responsables des processus opérationnels de protection des données de l'entreprise concernée
Les délégués locaux à la protection des données	• exercent pour l'entreprise concernée la fonction de délégué à la protection des données au sens du RGPD et de conseiller à la protection des données au sens de la LPD • accomplissent pour l'entreprise concernée les tâches susmentionnées du délégué à la protection des données de la FCM
Conseiller locaux à la protection des données	• exercent pour l'entreprise concernée la fonction de conseiller à la protection des données au sens de la LPD • sont le point de contact pour les personnes concernées et les autorités dans le domaine de la protection des données

- sont responsables de la sensibilisation et de la formation des collaborateurs de l'entreprise concernée
- contribuent à l'exécution de cette directive et des dispositions relatives à la protection des données.

Les services informatiques

- prennent, dans les systèmes informatiques généraux de l'entreprise concernée ainsi que dans les fichiers spécifiques, les mesures techniques et organisationnelles nécessaires pour protéger les données personnelles conformément au chiffre 10 de cette directive

Glossaire

Anonymisation: modification de données personnelles de manière rendant impossible l'attribution d'informations à une personne physique déterminée ou déterminable.

Sous-traitant: personne physique ou morale ou autre organisation traitant des données personnelles sur mandat d'un responsable.

Décision au cas par cas automatisée: décision reposant exclusivement sur un traitement automatisé et produisant un effet juridique par rapport à la personne concernée ou, de manière analogue, l'affectant considérablement.

Personne concernée: personne à laquelle se rapportent les données personnelles traitées.

Données personnelles particulièrement sensibles: dans une énumération exhaustive, il s'agit des données personnelles concernant la race, l'ethnie ou des convictions ou activités religieuses, politiques, syndicales ou philosophiques; données relatives à la santé; données génétiques et biométriques; données concernant la vie intime et sexuelle ou l'orientation sexuelle; données concernant des mesures d'aide sociale; et données concernant des infractions, des procédures pénales, des condamnations et des mesures pénales. Les données sur le patrimoine et le revenu ne sont pas des données personnelles particulièrement sensibles.

Délégué à la protection des données: personne externe ou interne indépendante ou entreprise externe indépendante nommé conformément aux dispositions du RGPD conseillant le responsable sur les questions de protection des données et vérifiant si le responsable respecte le droit de la protection des données.

Conseiller à la protection des données: personne externe ou interne nommé conformément aux dispositions de la LPD conseillant le responsable sur les questions de protection des données et participant à l'exécution du droit de la protection des données.

Coordinateur de la protection des données: personne interne exerçant pour l'entreprise concernée la fonction de premier interlocuteur pour les questions de protection des données, coordonnant les mesures nécessaires à la mise en œuvre des exigences en matière de protection des données et étant responsable des processus opérationnels de protection des données.

Paramètres par défaut facilitant la protection des données: principe selon lequel un responsable s'assure que les paramètres utilisateur sont configurés en usine de manière à ce que seules soient traitées les données personnelles qui sont nécessaires pour la finalité du traitement.

Droit de la protection des données: dispositions légales respectivement applicables qui régissent la protection des données. Selon l'entreprise et la situation, cela couvre le règlement général européen sur la protection des données, la loi fédérale sur la protection des données et les ordonnances correspondantes, tout autre droit national de la protection des données et autres dispositions, par ex. du droit du travail.

Atteinte à la protection des données: atteinte à la sécurité des données entraînant de manière accidentelle ou illégale la destruction, la perte, la modification ou la divulgation de données personnelles ou un accès non autorisé à des données personnelles.

Consentement: toute approbation volontaire accordée sans équivoque par une personne concernée pour une finalité concrète et de manière active après une information suffisante concernant le traitement des données personnelles la concernant, par ex. au moyen d'une déclaration écrite ou électronique. Un consentement peut être annulé à tout moment par la personne concernée.

Destinataire: personne physique ou morale ou autre organisation à laquelle sont divulguées des données personnelles.

Représentant UE: personne physique ou morale dont le siège, le domicile ou tout autre établissement se trouve dans l'UE, et qui a été mandatée par écrit par le responsable ou par le chargé du traitement de données par délégation et qui représente le responsable ou le chargé du traitement de données par délégation en ce qui concerne les obligations de protection de données.

Données relatives à la santé: données personnelles portant sur la santé physique ou mentale d'une personne physique et qui révèlent des informations relatives à leur état de santé.

Enfant: personne physique dont l'âge maximal est de 16 ans révolus. Les pays membres de l'UE peuvent abaisser ce seuil à l'âge de 13 ans révolus.

Établissement: institution permanente qui est effectivement et réellement active, par ex. une succursale ou une filiale, et non simplement un site de serveurs.

Profilage: traitement automatisé de données personnelles visant à évaluer des aspects personnels d'une personne physique, par ex. pour l'analyse ou la prédiction d'aspects concernant le rendement au travail, la situation économique, la santé, les goûts personnels, les centres d'intérêt, la fiabilité, le comportement, la localisation ou le changement de lieu.

Pseudonymisation: traitement de données personnelles de façon à ce que, sans informations supplémentaires, les données personnelles ne puissent plus être attribuées à une personne concernée déterminée ou déterminable. Cela suppose que d'éventuelles informations supplémentaires permettant l'identification soient stockées séparément et que des mesures techniques et organisationnelles garantissent que les données ne peuvent pas être attribuées à une personne physique identifiée ou identifiable.

Responsable: personne physique ou morale ou autre organisation décidant seule ou conjointement avec d'autres (« responsables commun » des finalités et des moyens du traitement de données personnelles.