Directive sur la protection des données de BMS Building Materials Suisse

en conformité avec le règlement général de l'Union Européenne sur la protection des données

Département:	Legal & Compliance
Rédaction:	Christina Hooker, Legal Counsel
Création:	Septembre 2022

Cette directive comprend des dispositions relatives à la protection des données à caractère personnel qui s'appliquent à l'ensemble des entreprises sous la marque faîtière BMS building Materials Suisse (ci-après **entreprises BMS**). Elle définit l'importance et la pertinence de la protection des données dans le respect des droits et des libertés fondamentaux des collaborateurs, des clients et des partenaires commerciaux des entreprises BMS.

Elle se réfère au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, dit règlement général sur la protection des données (**RGPD**), et à la législation fédérale suisse, dont la loi fédérale sur la protection des données (**LPD**).

Le RGPD établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, sur la libre circulation de ces données et sur la protection des droits et des libertés fondamentaux des personnes physiques et en particulier de leur droit à la protection des données à caractère personnel (art. 1 RGPD). Il est applicable directement dans tous les États membres de l'UE depuis le 25 mai 2018.

Selon l'art. 3 par. 1 du RGPD, ce règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union. Les entreprises BMS font partie du groupe BME, dont le siège se trouve sur le territoire de l'UE. En tant que telles, et suivant la décision de BME de faire appliquer le RGPD à l'ensemble du groupe, elles sont tenues de se conformer à ses exigences lors du traitement de données à caractère personnel.

En tant qu'entreprises ayant des établissements en Suisse, les membres de BMS sont naturellement soumis à la législation suisse en matière de protection des données.

À savoir

Le RGPD et la LPD encadrent les modalités de la protection des données personnelles lorsque celles-ci sont traitées par quelqu'un d'autre (personne ou entreprise) que la personne concernée.

Nous appartenons au groupe BME (Building Materials Europe), dont le siège se trouve aux Pays-Bas, un État membre de l'Union européenne. BME souhaite faire appliquer les principes de la protection des données à l'ensemble du groupe, aussi nous nous soumettons également au RGPD. En tant qu'entreprise suisse, nous nous conformons en outre à notre LPD nationale.

Contenu

1. Objet

Cette directive sur la protection des données a pour objet le traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi que le traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier, et ce, indépendamment de la nature de leur traitement ou de leur format (papier, numérique, oral) (cf. art. 2 par. 1 RGPD, art 1 LPD).

2. Champ d'application

Cette directive s'applique à tous les collaborateurs des entreprises BMS qui traitent des données à caractère personnel.

Dans le cadre de leur contrat de travail, les collaborateurs sont tenus de se conformer aux dispositions légales pertinentes en matière de protection des données, ainsi qu'à la présente directive. Les personnes et les entreprises externes mandatées par une entreprise BMS pour traiter des groupes de données sont tenues par contrat de se conformer aux dispositions en matière de protection des données les concernant.

La présente directive s'applique également pour le traitement des données à caractère personnel des collaborateurs des entreprises BMS. Tous les collaborateurs se voient remettre une politique de confidentialité en même temps que leur contrat de travail. Ce document leur indique quelles données sont traitées par les entreprises BMS, à quelle fin, et les droits dont ils disposent à cet égard.

À savoir

Les données à caractère personnel sont: Des informations concernant une personne vivante qui permettent de l'identifier (p. ex. nom et prénom, adresse, date de naissance, numéro de téléphone, numéro de compte, titre professionnel, photo, éventuellement adresses IP, etc).

Le traitement désigne: Toute opération portant sur des données à caractère personnel (p. ex. collecte, enregistrement, organisation, structuration, conservation, adaptation ou modification, extraction, consultation, utilisation, transmission / partage / diffusion ou autre mise à disposition, comparaison ou interconnexion, limitation, effacement ou destruction).

La présente directive permet non seulement de vous protéger en tant que collaborateur de BMS, mais elle vous oblige aussi à protéger les données personnelles d'autrui. Elle comprend des règles que vous devez suivre lors du traitement de données de nos clients, de nos partenaires commerciaux, de nos fournisseurs, de nos prestataires de services, ainsi que des visiteurs de notre site web.

3. Registre des activités de traitement

Les entreprises BMS tiennent un registre des activités de traitement effectuées sous leur responsabilité. Y figurent a minima les informations suivantes:

a. le nom et les coordonnées de l'entreprise ou du département concerné
b. les finalités du traitement
c. une description des catégories de personnes concernées et des catégories de données à caractère personnel
d. les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers
e. le cas échéant, les transferts de données à caractère personnel vers un pays tiers, y compris l'identification de ce pays tiers
f. dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données
g. dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées art. 32 par. 1 RGPD et art. 11 LPD.

À savoir

Nous tenons un registre dans lequel nous listons toutes les opérations de traitement de données à caractère personnel (de nos clients, de nos collaborateurs, de nos partenaires commerciaux, etc). Ce registre est important car il nous indique quelles données nous protégeons dans quelles opérations de traitement. Il donne aussi un aperçu des responsables de la protection au sein de l'entreprise et des données spécifiques faisant l'objet d'un traitement. Cette liste est par ailleurs présentée en cas d'audit préalable par une autorité de surveillance.

4. Principes du traitement de données à caractère personnel

Lors du traitement de données à caractère personnel, les entreprises BMS se conforment aux principes suivants:

- **Licéité, loyauté, transparence**
  Les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (cf. art. 5 par. 1 al. a RGPD, art. 4 par. 1,2,3 LPD).

- **Limitation des finalités**
  Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités (cf. art. 5 par. 1 al. b RGPD, art. 4 par. 3 LPD).

- **Minimisation des données**
  Les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (cf. art. 5 par. 1 al. c RGPD, art. 4, par. 3 LPD).

- **Exactitude**
  Les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour (cf. art. 5 par. 1 al. d RGPD, art. 4 par. 5 LPD).

- **Limitation de la conservation**
  Les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (cf. art. 5 par 1 al. e RGPD, art 4 par. 4 LPD).

- **Intégrité et confidentialité**
  Les données à caractère personnel doivent être traitées de façon à leur garantir une sécurité appropriée, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (cf. art. 5 par. 1 al. f RGPD).

- **Responsabilité**
  Les entreprises BMS veillent au respect des principes susmentionnés pour le traitement de toutes les données à caractère personnel et sont en mesure de prouver qu'ils sont respectés (art. 5 par. 2 RGPD).

4.1 Licéité du traitement

Les entreprises BMS ne traitent des données à caractère personnel que si au moins une des conditions listées par l'art. 6 par. 1 RGPD et l'art. 24 LPD est remplie, notamment:

- La personne concernée a **consenti** au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;

- le traitement est nécessaire à **l'exécution d'un contrat** auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

- le traitement est nécessaire au **respect d'une obligation légale** à laquelle l'entreprise responsable du traitement est soumise;
- le traitement est nécessaire **aux fins des intérêts légitimes poursuivis par l'entreprise BMS responsable du traitement** ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel. Selon l'art. 24, par. 2 LPD, les intérêts prépondérants de l'entreprise BMS responsable sont notamment constitués:
    - si le traitement s'inscrit dans un rapport de concurrence économique actuel ou futur avec une autre personne, à condition toutefois qu'aucune donnée personnelle traitée ne soit communiquée à des tiers;
    - si les données personnelles sont traitées dans le but d'évaluer la solvabilité de la personne concernée (client) (à condition toutefois qu'elles ne soient pas sensibles, qu'elles ne soient communiquées que pour conclure ou exécuter un contrat avec la personne concernée, et que cette personne soit majeure)

4.2 Conditions du consentement

- L'entreprise BMS responsable obtient le consentement de la personne concernée dans un délai raisonnable.
- Le consentement est donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant.
- Une déclaration de consentement est mise à disposition sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Son domaine est clairement circonscrit et elle ne contient aucune clause abusive.
- En outre, la personne concernée se voit présentée une méthode simple lui permettant de retirer son consentement à tout moment.

4.3 Exigences en matière de définition des finalités

- Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.
- Dans certaines circonstances, les données à caractère personnel peuvent être traitées à des fins dépassant celles initialement fixées lors de la collecte des données. Celles-ci doivent figurer dans le registre et, si nécessaire, être communiquées à la personne concernée.

4.4 Traitement des données à caractère personnel d'un enfant

- En principe, les entreprises BMS ne traitent que les données à caractère personnel d'un client âgé de seize ans révolus au minimum.
- Si l'enfant n'a pas encore atteint l'âge de seize ans révolus, les entreprises BMS ne traitent ses données à caractère personnel que si et dans la mesure où il donne son consentement avec l'accord du titulaire de la responsabilité parentale, ou si ce dernier donne son consentement.

4.5 Traitement portant sur des catégories particulières de données à caractère personnel

- Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, ou des données sur des poursuites ou sanctions pénales et administratives sont interdits sans consentement explicite (art. 9 par. 1 RGPD, art. 4 par. 6 LPD).
- Le cas échéant, les entreprises BMS ne traitent que des catégories particulières de données à caractère personnel concernant leurs collaborateurs et ce, dans le cadre exclusif de l'organisation de l'activité et pour respecter et vérifier les obligations en matière de droit du travail et de sécurité sociale. Le consentement explicite des personnes concernées est alors requis, à moins qu'il n'existe un autre motif justificatif.

4.6 Marketing numérique

- Sauf accord des personnes concernées, les entreprises BMS ne communiquent pas avec elles à des fins de publicité ou de marketing via des supports numériques (téléphones mobiles, e-mail, Internet, etc.).
- En cas de consentement à l'utilisation de données à caractère personnel à des fins de marketing numérique, la personne concernée est informée dès la première collecte de données qu'elle est en droit de retirer ce consentement à tout moment.

4.7 Durée de conservation

- Les entreprises BMS conservent les données à caractère personnel pour une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles ont été collectées puis traitées (cf. art. 5 par. 1 al. e RGPD, art. 4 par. 4 LPD).
- Les circonstances de chaque cas particulier déterminent ce qui est considéré comme nécessaire, en tenant compte des motifs pour lesquels les données ont été collectées.

À savoir

Nous nous appuyons sur les principes du RGPD et de la LPD: Nous tenons à traiter les données personnelles **de manière licite**, à des **fins clairement définies** (et pas au-delà), nous ne voulons en stocker que '**la quantité nécessaire**,) n'utiliser que des données **exactes**, ne les sauvegarder que **pour la durée nécessaire**, et les **protéger** du mieux possible contre la perte, la destruction, les dommages et la diffusion.

Le traitement des données personnelles est licite lorsqu'il repose sur une **base juridique valable** (RGPD) ou qu'il a un **motif justificatif** (LPD). Ce cas de figure est notamment illustré lors du traitement de données personnelles dans le cadre d'un **contrat** ou **pour remplir une obligation légale**, **aux fins de nos intérêts économiques légitimes** (dans la mesure où ils prévalent sur les droits et libertés fondamentaux de la personne concernée) ou encore si le **consentement** de la personne concernée a été obtenu, sous réserve qu'elle ait été dûment informée des modalités du traitement de ses données. Le consentement de la personne concernée est notamment nécessaire pour les traitements effectués dans le cadre d'opérations marketing.

Un **consentement valide** doit être:

- obtenu dans un délai raisonnable
- formulé clairement et pour un cas spécifique. Par exemple, pour s'abonner à une newsletter, une possibilité de consentir doit figurer juste en dessous de la zone de saisie de données personnelles, typiquement sous la forme proactive d'une case vide que la personne intéressée doit cocher elle-même (et non pas déjà cochée).
- clair et facile à comprendre, pour que la personne concernée saisisse vraiment les informations avant de donner son consentement
- révocable à tout moment. Par exemple, à la fin d'une newsletter, il doit être possible de se désabonner en 1 ou 2 clics.

Les apprentis de moins de 17 ans doivent obtenir le consentement éclairé de leurs parents pour le traitement de leurs données.

Seul notre département RH est autorisé à traiter les données particulièrement sensibles. BMS met alors un point d'honneur à les protéger; les collaborateurs RH sont d'ailleurs formés à cet effet.

5. Droits des personnes concernées

Les individus dont les données personnelles sont traitées disposent de certains droits, en vertu du RGPD et de la LPD.

5.1 Obligation d'information

Au moment où les données à caractère personnel sont collectées, l'entreprise BMS responsable fournit à la personne concernée toutes les informations suivantes (cf. art. 13 par. 1 RGPD, art. 19 LPD): Son **nom et ses coordonnées**, les **finalités** du traitement auquel sont destinées les données à caractère personnel, ainsi que la **base juridique** du traitement ou, le cas échéant, les **intérêts légitimes** poursuivis par le responsable du traitement ou par un tiers (RGPD uniquement), le cas échéant, les **destinataires** des données à caractère personnel et, le cas échéant, l'**intention** de transmettre les données à caractère personnel à un pays tiers. Lorsque les données personnelles sont communiquées à l'étranger, la LPD suisse prévoit en outre que l'entreprise responsable communique à la personne concernée le **nom de l'État et, le cas échéant, les garanties** de protection des données personnelles à l'étranger.

L'entreprise BMS responsable fournit à la personne concernée, au moment où les données à caractère personnel sont collectées, les informations complémentaires suivantes qui sont nécessaires pour garantir un traitement équitable et transparent: la **durée de conservation** ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée; l'existence du **droit de demander l'accès**, la **rectification** ou l'**effacement** des données personnelles, ou de **limiter ou de s'opposer au traitement**, ou de **retirer son consentement à tout moment** si celui-ci avait été donné au préalable (sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci); et l'existence du **droit d'introduire une réclamation** auprès de l'autorité de contrôle.

5.2 Droit d'accès

Toutes les personnes concernées dont les entreprises BMS traitent les données personnelles peuvent demander à l'entreprise BMS responsable une confirmation que les données en question sont traitées, en soumettant leur requête par écrit via l'adresse **dataprotection@bmsuisse.ch** et après vérification de leur identité. Si la réponse est positive, la personne concernée peut se voir fournir l'intégralité des informations listées art. 15 par. 1 RGPD et art. 25 LPD concernant ses données personnelles, à savoir:

- l'identité et les coordonnées de notre entreprise
- la finalité du traitement
- les catégories de données à caractère personnel concernées
- les destinataires auxquels les données à caractère personnel ont été ou seront communiquées, en particulier les destinataires qui sont établis dans des pays tiers
- les informations sur les données exportées, telles qu'une liste de pays et de principes de base (LPD suisse uniquement)

- lorsque cela est possible, la durée envisagée de conservation des données à caractère personnel ou, sinon, les critères utilisés pour déterminer cette durée
- l'existence du droit de demander à l'entreprise BMS responsable du traitement la rectification ou l'effacement de données à caractère personnel, ou une limitation du traitement des données à caractère personnel relatives à la personne concernée, ou du droit de s'opposer à ce traitement
- le droit d'introduire une réclamation auprès d'une autorité de contrôle
- lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source
- si les données à caractère personnel sont transférées vers un pays tiers et que des garanties sont prévues à cet égard, la personne concernée a le droit d'être informée des garanties appropriées.

Selon les circonstances, certaines des données à caractère personnel demandées sont susceptibles d'être divulguées à une autre personne concernée lors du transfert. En de pareils cas, les informations en question doivent être éditées ou retenues, selon ce qui s'avère nécessaire ou approprié afin de protéger les droits de la personne concernée.

Selon la LPD suisse, les entreprises BMS peuvent refuser, restreindre ou différer la communication des informations lorsque:

- une loi au sens formel le prévoit, notamment pour protéger un secret professionnel;
- les intérêts prépondérants d'un tiers l'exigent;
- la demande d'accès est manifestement infondée notamment parce qu'elle poursuit un but contraire à la protection des données ou est manifestement procédurière.

Les demandes d'accès des personnes concernées sont traitées conformément à la **procédure** et adressées à dataprotection@bmsuisse.ch au moyen du **formulaire** correspondant.

5.3 Profilage/décision individuelle automatisée

Les entreprises BMS n'utilisent le profilage que dans leur outil de SIRH actuel. Le profilage est effectué avec le consentement explicite des personnes concernées ou pour l'exécution des contrats entre celles-ci et les entreprises BMS. Des mesures adéquates sont prises pour protéger les droits, les libertés et les intérêts légitimes des personnes concernées.

5.4 Droit à la rectification

La personne concernée peut demander à l'entreprise BMS responsable de rectifier les données à caractère personnel la concernant. Cela inclut également le droit de demander que des données incomplètes soient complétées (en tenant compte des finalités du traitement). Les demandes sont traitées conformément à la procédure et adressées à dataprotection@bmsuisse.ch au moyen du formulaire correspondant.

5.5 Droit à la suppression

Dans certaines conditions, les personnes concernées ont le droit d'obtenir de l'entreprise BMS responsable du traitement la suppression de données à caractère personnel la concernant (leur anonymisation irrévocable équivaut à un effacement) et l'entreprise a l'obligation d'effacer/d'anonymiser irrévocablement les données, lorsque l'un des motifs suivants s'applique (cf. art. 17 par. 1 RGPD, art. 32 par. 2 al. c LPD):

- Les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées
- la personne concernée retire son consentement et il n'existe pas d'autre fondement juridique au traitement
- la personne concernée s'oppose au traitement et il n'existe pas de motif légitime pour le traitement
- les données à caractère personnel ont fait l'objet d'un traitement illicite
- l'effacement des données à caractère personnel est exigé par la législation suisse

Le droit à la suppression des données à caractère personnel n'est pas constitué si le traitement est nécessaire:

- pour exercer le droit à la liberté d'expression et d'information
- pour respecter une obligation légale ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investie l'entreprise BMS
- pour la constatation, l'exercice ou la défense de droits en justice

Les demandes d'effacement sont traitées conformément à la procédure et adressées à dataprotection@bmsuisse.ch au moyen du formulaire correspondant.

À savoir

Toute personne concernée dont les données sont traitées dispose des **droits** suivants:

- Le droit de recevoir des informations exactes et exhaustives, notamment sur: la procédure de traitement et son responsable, sur l'ensemble des droits dont elle dispose, sur l'élargissement des finalités du traitement et sur la possibilité de retirer à tout moment son consentement
- Le droit de savoir, en tant que personne concernée, si ses données sont traitées ou non, et comment elles le sont
- Le droit de faire rectifier ou compléter des données personnelles fausses ou incomplètes
- Le droit de faire effacer des données personnelles, si
    - elles ne sont plus nécessaires
    - le consentement n'existe plus
    - la personne concernée s'est opposée au traitement
    - le traitement était illicite
    - une loi suisse prévoit l'effacement

Les liens vers les processus et les formulaires se trouvent au chapitre précédent.

Les demandes d'accès, de rectification, de modification ou d'effacement complétées doivent être envoyées par e-mail à dataprotection@bmsuisse.ch.

6. Transfert de données à caractère personnel à des tiers

6.1 Principe

Un transfert de données à caractère personnel vers un pays tiers peut avoir lieu lorsque le pays tiers en question assure un niveau de protection adéquat. Un tel transfert ne nécessite pas d'autorisation spécifique (cf. art. 45 RGPD, art. 16 f LPD).

En l'absence de décision d'adéquation de la Commission, les entreprises BMS ne peuvent transférer des données à caractère personnel vers un pays tiers que si elles ont prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives (cf. art. 46 RGPD, art. 16 par. 2 LPD).

En l'absence de décision d'adéquation ou de garanties appropriées, un transfert de données à caractère personnel vers un pays tiers ne peut être effectué par les entreprises BMS qu'à certaines conditions, dont les plus importantes sont:

- la personne concernée a donné son consentement explicite au transfert après avoir été informée des risques causés par l'absence de décision d'adéquation et de garanties appropriées
- le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et l'entreprise BMS responsable à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée

6.2 Transferts entre BMS et BME ou d'autres entreprises faisant partie de BME

Aux fins de la réalisation efficace des activités des entreprises BMS, il peut être nécessaire de transmettre des données à caractère personnel à BME ou à d'autres entreprises faisant partie de BME, ou d'accorder à BME l'accès à des données à caractère personnel. Des dossiers personnels peuvent notamment être transmis par des collaborateurs de BMS au département RH de BME à Amsterdam, à des fins de rémunération des cadres et de développement/formation des collaborateurs. Toutes les mesures nécessaires à la protection des données à caractère personnel sont alors systématiquement prises.

Si l'entreprise qui reçoit les données se trouve dans un pays tiers, l'entreprise BMS responsable recourt à des mécanismes de transfert qui confèrent aux personnes concernées des droits juridiquement contraignants et opposables relatifs au traitement de leurs données personnelles (clauses types de protection des données), ou obtient le consentement explicite et éclairé des personnes concernées pour le transfert.

Les entreprises BMS et leurs collaborateurs veillent notamment à ce que:

- l'autorisation du département Legal & Compliance soit obtenue avant transfert vers un pays tiers
- seul le minimum nécessaire de données à caractère personnel soit transmis
- des mesures de sécurité adéquates soient prises pour protéger les données à caractère personnel durant la transmission

6.3 Transferts à d'autres tiers

Les entreprises BMS ne transfèrent des données à caractère personnel à des tiers et ne leur y donnent accès que s'il est garanti qu'elles seront traitées licitement et protégées de manière adéquate par le destinataire.

Si des données à caractère personnel sont traitées par un tiers, l'entreprise BMS responsable vérifie d'abord si la législation en vigueur considère le tiers comme responsable ou comme sous-traitant des données à caractère personnel en question.

Si le tiers est considéré comme responsable du traitement, l'entreprise BMS conclut un contrat de co-responsabilité qui définit les responsabilités de chaque partie vis-à-vis des données à caractère personnel transférées.

Si le tiers est considéré comme sous-traitant, l'entreprise BMS conclut un contrat de traitement des données avec lui qui l'oblige à respecter les principes de la législation sur la protection des données. (cf. art 28 RGPD, art. 9 LPD)

Dans certaines circonstances, le transfert des données à caractère personnel à l'insu ou sans le consentement de la personne concernée est possible, notamment si la démarche est nécessaire à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

À savoir

Les données personnelles peuvent aussi être envoyées et traitées dans un autre pays. Sa législation doit toutefois garantir une protection appropriée de ces données. Tous les pays membres de l'Union européenne remplissent cette condition, car ils sont tous soumis au RGPD. La Suisse et le Royaume-Uni ont eux aussi une législation appropriée. Les données peuvent donc être transférées sans autorisation particulière.

Ce principe s'applique aussi à la transmission de données personnelles vers notre société-mère, BME. Bien évidemment, un transfert vers un pays réputé sûr ne dispense pas de signer des contrats de traitement ou de transfert des données qui garantissent que les données personnelles seront protégées lors de ces opérations. Aucune autre démarche n'est en revanche nécessaire.

D'autres pays, comme les États-Unis ne garantissent pas une protection des données personnelles suffisante. Une autorisation séparée est alors requise. Le plus souvent, elle prend la forme d'un consentement éclairé et explicite de la personne concernée, qui aura été préalablement informée que ses données seront transférées et/ou traitées dans un pays à risque. Lorsque plusieurs personnes sont impliquées, on emploie plutôt des clauses types de protection des données, qui garantissent des mesures de protection supplémentaires.

Lorsque nous partageons des données personnelles avec des prestataires de services (logistique, IT, etc.), des fournisseurs, des partenaires commerciaux ou d'autres tiers, les contrats de sous-traitance des données garantissent une protection appropriée de ces données.

7. Mesures techniques et organisationnelles

Les entreprises BMS prennent les mesures techniques et organisationnelles adéquates pour garantir une sécurité des données à caractère personnel conforme aux dispositions légales en matière de protection des données. Les mesures prises sont détaillées dans le registre qui suit le traitement.

8. Protection des données dès la conception et protection des données par défaut

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, les entreprises BMS mettent en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données tels que définis au chapitre 4 de la présente directive et à assortir le traitement des garanties nécessaires afin de protéger les droits des personnes concernées (art. 25 par. 1 RGPD, art. 7 LPD).

Les entreprises BMS mettent en œuvre les mesures techniques et organisationnelles appropriées pour que, par défaut, seules les données à caractère personnel nécessaires au regard de chaque finalité spécifique du traitement soient traitées. Ces mesures s'appliquent à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. Elles garantissent notamment que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques (art. 25 par. 2 RGPD, art. 7 par. 3 LPD).

Afin de garantir que tous les principes relatifs à la protection des données sont pris en compte lors du développement, de la modification ou de l'extension de systèmes ou de processus, ces derniers doivent être soumis à une procédure d'approbation avant d'être (ré)utilisés. Conformément au chapitre 10 de la présente directive, tout système ou processus nouveau ou modifié fait l'objet d'une analyse d'impact relative à la protection des données.

9. Sensibilisation et formation des collaborateurs

Les entreprises BMS introduisent les processus et les mécanismes internes adéquats pour impliquer et sensibiliser les collaborateurs.

En vertu de la présente directive, la responsabilité de tous les collaborateurs des entreprises BMS qui ont accès à des données à caractère personnel est engagée. Dans le cadre de leur intégration, ils sont informés de la directive sur la protection des données et acceptent la politique de confidentialité. Les entreprises BMS soutiennent leurs collaborateurs tout au long de ces processus et organisent des formations à la protection des données qui abordent au moins les thématiques suivantes:

a) Les principes du traitement des données à caractère personnel, tels que définis au chapitre 4 de la présente directive:

b) La responsabilité incombant à tout collaborateur de s'assurer que les données à caractère personnel ne sont traitées que par les personnes autorisées et aux fins autorisées;

c) La nécessité et l'utilisation correcte des formulaires et des processus approuvés pour la mise en œuvre de la présente directive;

d) L'utilisation appropriée des mots de passe, des tokens de sécurité et d'autres mécanismes d'accès;

e) L'importance de restreindre l'accès aux données à caractère personnel, p. ex. via des écrans de veille protégés par des mots de passe et la déconnexion;

f) Le stockage sécurisé de dossiers physiques et de supports électroniques;

g) La nécessité d'une autorisation appropriée et de mesures de sécurité adéquates pour tous les transferts de données à caractère personnel en dehors du réseau interne et des locaux de l'entreprise;

h) La suppression appropriée des données à caractère personnel;

i) Les risques spécifiques liés aux données à caractère personnel dans le cadre des activités ou des tâches d'un département donné.

Si des points d'ombre subsistent concernant le traitement ou le transfert de données à caractère personnel, les collaborateurs pourront se tourner vers le département Legal & Compliance via l'adresse dataprotection@bmsuisse.ch.

À savoir

Nous protégeons les données personnelles de nos collaborateurs, de nos clients et de nos partenaires commerciaux au moyen de mesures techniques et organisationnelles.

Les **mesures techniques** sont avant tout du ressort de notre département IT. Elles garantissent l'excellence de nos entreprises sur le plan technique, nous préservent des attaques internes et externes, assurent que seules les données personnelles strictement nécessaires puissent être vues et partagées, et que les données devenues inutiles soient supprimées.

Pour que notre protection reste optimale, nos nouveaux traitements sont contrôlés au moyen d'une analyse d'impact relative à la protection des données qui nous permet d'identifier les mesures de protection à mettre en œuvre.

Les **mesures organisationnelles** relèvent de la responsabilité de tous les collaborateurs, qui doivent en outre suivre notre directive informatique: Elle détaille des mesures telles que le verrouillage de l'écran de l'ordinateur, la fermeture à clef des lieux de stockage de documents physiques et le choix de mots de passe complexes, mais aussi la sensibilisation et la formation des collaborateurs amenés à traiter des données personnelles.

Pour en savoir plus sur les mesures techniques et organisationnelles, ou sur les formations proposées,

10. Analyse d'impact relative à la protection des données

L'entreprise BMS responsable effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées, si le type de traitement considéré, compte tenu de sa nature, de sa portée, du contexte et des finalités, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées (art. 35 par. 1 RGPD, art. 22 LPD).

L'analyse d'impact relative à la protection des données doit contenir au moins les éléments suivants (cf. art. 35 par. 7 RGPD, art. 22 par. 3 LPD):

a) une description systématique des opérations de traitement envisagées et des finalités du traitement;

b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;

c) une évaluation des risques pour les droits et libertés des personnes concernées et

d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du RGPD et de la LPD compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

Le collaborateur responsable de l'introduction d'un nouveau traitement (p. ex. nouvelle application, nouvelle plateforme, nouvelles caméras, nouvelle boutique en ligne, etc.) sollicite le département Legal & Compliance pour décider si une analyse d'impact relative à la protection des données est nécessaire. Il convient de suivre les étapes détaillées dans le **concept sur l'analyse d'impact relative à la protection des données**.

11. Notification d'une violation de données à caractère personnel

En cas de violation des données à caractère personnel de personnes se trouvant dans l'Union européenne, le collaborateur responsable du traitement, qui l'a découverte/à qui elle a été rapportée, la notifie sans délai, dans un premier temps en interne, via l'adresse dataprotection@bmsuisse.ch. Legal & Compliance décide alors si la violation en question présente un risque pour les droits et les libertés des personnes physiques. Si tel est le cas, Legal & Compliance la notifie en externe, à l'autorité de contrôle compétente (art. 33 par. 1 RGPD, art. 24 LPD).

La notification doit à tout le moins (art. 33 par. 3 RGPD, art. 24 par. 2 LPD):

- décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;
- communiquer le nom et les coordonnées d'un interlocuteur auprès duquel des informations supplémentaires peuvent être obtenues;
- décrire les conséquences probables de la violation
- décrire les mesures prises ou proposées pour remédier à la violation, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives

Pour savoir comment reconnaître et signaler une violation des données personnelles, voir notre **procédure et schéma pour la notification d'une violation de données à caractère personnel**.

À savoir

Qu'est-ce qu'une **analyse d'impact relative à la protection des données (AIPD)**?

Lorsqu'une nouvelle opération de traitement est utilisée dans l'entreprise (p. ex. une nouvelle boutique en ligne avec possibilité de paiement, qui nous conduit à traiter les données personnelles des clients qui y font leurs achats), cette opération doit être dans un premier temps vérifiée. Il s'agit, en l'occurrence de déterminer si elle permet de réaliser l'objectif qui a justifié sa création (p. ex. traitement d'adresses, de noms et d'informations bancaires pour le paiement en ligne par carte de crédit), si elle est vraiment nécessaire et adaptée pour y parvenir (p. ex. se demander si toutes ces informations sont vraiment essentielles pour que la carte de crédit soit débitée, si certaines ne sont pas superflues), si elle ne fait pas courir de nouveaux risques aux données personnelles (p. ex. les informations bancaires ne pourraient-elles pas être volées lors d'une attaque virale externe?) et par quelles mesures les risques éventuels peuvent être atténués (p. ex. faut-il installer un pare-feu plus puissant ou un autre antivirus pour garantir la sécurité des informations bancaires?).

En quoi consiste une **notification d'une violation de données personnelles**?

Si une violation des données personnelles est constatée (p. ex. une liste de clients contenant des données personnelles est envoyée par inadvertance à un grand groupe de destinataires externes au lieu d'une personne spécifique et autorisée), elle doit être immédiatement notifiée à Legal & Compliance via l'adresse dataprotection@bmsuisse.ch. Reste ensuite à déterminer si la personne concernée se voit exposée à un grand risque ou pas (p. ex. y avait-il beaucoup de clients sur cette liste? Les données étaient-elles de nature particulièrement sensible? Les données contenues dans la liste de clients risquent-elles d'être utilisées par les destinataires non autorisés pour du publipostage, ou revendues à d'autres entreprises?)

Une notification à l'adresse dataprotection@bmsuisse.ch doit comprendre au moins les informations suivantes:

- une description de la nature de la violation (p. ex. une liste de clients envoyée à x personnes, elle contient les données de x clients comme leur nom, adresse, etc.)
- une description des conséquences probables de la violation (p. ex. les données risquent d'être utilisées pour des traitements auxquels elles n'étaient à l'origine pas destinées et pour lesquels nous n'avons pas obtenu de consentement)
- les mesures proposées (p. ex. envoyer un mail à tous les destinataires les enjoignant à effacer ces données clients ou à ne pas les utiliser)

12. Compliance/Reporting

Si un défaut de conformité est constaté, Legal & Compliance, en concertation avec l'entreprise BMS concernée, définit une procédure et un calendrier appropriés pour se conformer aux exigences dans un délai raisonnable et défini. Les cas graves sont signalés à la direction, qui les prend en charge.

13. Organisation

13.1 Direction

La direction définit les principes généraux de la garantie de protection des données dans les entreprises BMS. Elle désigne un intermédiaire chargé de faire appliquer les dispositions en matière de protection des données.

13.2 Supérieurs hiérarchiques

Les supérieurs hiérarchiques de tous les niveaux sont chargés de faire appliquer et respecter, dans leur domaine de responsabilité, les dispositions en matière de protection des données énoncées dans la présente directive. Ils coopèrent avec l'autorité compétente pour former et sensibiliser leurs collaborateurs. Ils assument un rôle de modèle et motivent les collaborateurs à respecter les mesures de protection des données.

13.3 Autorité compétente

La direction désigne Legal & Compliance comme intermédiaire.

Legal & Compliance assume la responsabilité documentaire de la présente directive.

Le groupe de travail Protection des données, constitué de collaborateurs des départements Legal & Compliance, IT et RH, assiste les entreprises BMS dans l'application et la mise en œuvre de la protection des données.

Legal & Compliance surveille et tient compte de l'évolution des exigences légales dans le domaine de la protection des données.

13.4 Tous les autres collaborateurs

Tous les collaborateurs des entreprises BMS sont tenus de lire et de respecter cette directive sur la protection des données dans sa dernière version (disponible sur BMSmobile en suivant le lien interne ASTRA).

Si une infraction délibérée à la présente directive est constatée de la part de collaborateurs, des mesures disciplinaires pouvant aller jusqu'au licenciement peuvent être prises à leur encontre.

13.5 Responsables

13.5.1 Relations extérieures

Dans le cadre des relations extérieures, l'entreprise BMS impliquée est considérée comme responsable.

Compte tenu, notamment, de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées, pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD et à la LPD.

13.5.2 Relations internes

Dans le cadre des relations internes, le directeur RH et les collaborateurs RH sont responsables du traitement consciencieux et conforme à la législation des données à caractère personnel dans leur domaine de compétence.

Le directeur IT est responsable de la mise en place en interne sur le plan technique des mesures de protection des données et de leur sécurité. Les responsables systèmes et applications l'assistent tout particulièrement dans cette tâche. Il coopère étroitement avec Legal & Compliance pour s'assurer de la conformité des mesures. Il évalue ainsi les risques, les incidents et les quasi-incidents susceptibles de mettre en danger la protection des données.

À savoir

La direction définit les **principes** de la protection des données. Les cas graves de violation des données doivent être notifiés à la direction.

Tous les **supérieurs hiérarchiques** doivent se conformer de façon exemplaire aux principes de la protection des données. Ils veillent à ce que les collaborateurs connaissent cette directive et les principes de la protection des données, et soient formés si besoin est.

Legal & Compliance est l'autorité compétente pour les questions, l'enregistrement de nouvelles opérations de traitement dans le registre et sa tenue, l'établissement de documents relatifs à la protection des données, pour les demandes d'informations, d'accès, de rectification, de modification et d'effacement, pour les notifications de violations de données et pour toutes les autres affaires ayant trait à des thèmes liés à la protection des données.

Tous les collaborateurs s'engagent à respecter la présente directive des entreprises BMS dès le début de leur relation de travail avec une entreprise BMS.

Dans les **relations extérieures**, les entreprises BMS se présentent comme responsables des données.

En interne, la responsabilité des données incombe avant tout aux départements Legal & Compliance, IT (pour les mesures techniques, les analyses d'impact relative à la protection des données et l'examen des notifications de violation) et RH (pour les données personnelles particulièrement sensibles et les données des collaborateurs en général). Tous les collaborateurs sont néanmoins tenus d'assurer la protection des données.

14. Dispositions finales

14. Dispositions finales

14.1 Amendements et ajouts

Legal & Compliance peut amender, compléter ou annuler la présente directive. Est entendu par amendement ou ajout toute adjonction, suppression ou modification de certaines dispositions. Les rectifications de forme ou d'erreurs d'inattention en sont exclues.

14.2 Documents complémentaires

La présente directive expose les principes des entreprises BMS concernant les dispositions adoptées en matière de protection des données. Des règlements et d'autres documents nécessaires au traitement de données à caractère personnel peuvent être élaborés à partir de la directive.

14.3 Parties intégrantes

Les annexes suivantes font partie intégrante de la présente directive.

1: Procédure pour les demandes d'accès, de rectification et d'effacement

2: Demande d'accès interne

3: Demande d'accès externe

4: Demande de rectification interne

5: Demande de rectification externe

6: Demande d'effacement interne

7: Demande d'effacement externe

8: Guide et description analyse d'impact relative à la protection des données

9: Procédure et schéma notification violation de données

14.4 Divers

La présente directive est disponible pour tous les collaborateurs sur BMSmobile.

Legal & Compliance assume la responsabilité documentaire de la présente directive. Toute question à ce sujet est à envoyer par e-mail à l'adresse dataprotection@bmsuisse.ch.

Les amendements et ajouts pertinents apportés à la présente directive seront notifiés aux collaborateurs des entreprises BMS par le département RH. Elle entre en vigueur dès sa publication sur BMSmobile.

14.5 Entrée en vigueur

La présente directive entre en vigueur le septembre 2022.