ARBONIA

Directive concernant le traitement des données (Directive sur la protection des données)

16 juin 2020

ARBONIA

TABLE DES MATIÈRES

ARBONIA

1 OBJECTIFS

Il est impératif de collecter et de traiter des données à caractère personnel pour satisfaire aux obligations légales et contractuelles. Les dispositions en matière de protection des données applicables dans les différents pays doivent être respectées. La présente directive décrit le mode de traitement des données à caractère personnel appliqué par Arbonia AG et les sociétés de son groupe (ci-après dénommées conjointement «Arbonia», ou une société individuelle du groupe, ci-après dénommée «société du groupe»). Les dispositions formulées s'appliquent en tant que normes minimales. Si le règlement local sur la protection des données prévoit des dispositions plus strictes, celles-ci doivent être respectées. Toute réglementation locale pour la mise en œuvre de la présente directive doit également être respectée.

L'objectif de la présente directive sur la protection des données («Directive sur la protection des données») est de déterminer, mettre en œuvre, maintenir et améliorer en permanence le respect de la protection des données, conformément aux exigences du règlement de base de l'Union européenne sur la protection des données 2016/679 (le **RGPD**) et de toutes les autres lois locales applicables sur la protection des données (dans leur ensemble, les **lois applicables sur la protection des données**) par Arbonia.

Le non-respect des lois applicables en matière de protection des données expose Arbonia à des risques d'atteinte à sa réputation et à des amendes sévères (par exemple, jusqu'à 4 % des ventes mondiales dans le cadre du RGPD). Elle peut également exposer nos clients et nos salariés à certains risques en matière de protection de protection des données, tels que l'usurpation d'identité ou des pertes financières. Le respect des lois applicables en matière de protection des données nous aide à maintenir la confiance dans l'organisation Arbonia et à assurer le succès du fonctionnement de l'entreprise.

L'objectif de cette directive sur la protection des données est de créer le cadre nécessaire au respect de la protection des données au sein d'Arbonia. Elle vise notamment à mettre en œuvre les principes de base pour le traitement des données à caractère personnel (les **principes de protection des données**) prévus à l'article 6 et dont les entreprises d'Arbonia sont responsables lorsqu'elles agissent en qualité de partie responsable en vertu du RGPD, elle réglemente la mise en œuvre nécessaire de mesures techniques et organisationnelles appropriées et le signalement des incidents de protection des données en tant que norme minimale pour toutes les entreprises d'Arbonia, elle vaut pour tous les salariés d'Arbonia ainsi que les membres du conseil d'administration d'Arbonia AG.

Elle crée également un cadre pour d'autres exigences qui s'appliquent aux responsables du traitement et sous-traitants en vertu du RGPD (ou de lois similaires applicables en matière de protection des données) comme décrit dans la section 7.

ARBONIA

2 TERMES ET DÉFINITIONS

Aux fins de la présente directive sur la protection de la vie privée, les termes et définitions suivants s'appliquent:

L'**anonymisation des données** signifie que l'identité personnelle ne peut jamais être retracée par quiconque ou que l'identité personnelle ne peut être retracée qu'à l'appui d'un temps, d'un coût et d'un effort déraisonnables.

Les **lois applicables en matière de protection des données** sont le Règlement de base sur la protection des données de l'Union européenne 2016/679 (le **RGPD**) ou toute autre loi nationale applicable en matière de protection des données qui contient des dispositions similaires.

Le **responsable du processus de gestion** est une personne physique responsable au titre de la présente directive sur la protection des données et chargée du traitement des données à caractère personnel ainsi que de l'application informatique correspondante.

Le **consentement** désigne le consentement de la personne concernée, c'est-à-dire toute expression libre, éclairée et non équivoque de sa volonté dans un cas précis, sous la forme d'une déclaration ou d'un acte confirmatif non équivoque par lequel la personne concernée donne son accord pour le traitement de ses données à caractère personnel.

Le **responsable du traitement** est la personne physique ou morale, l'autorité publique, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel.

Incident lié à la sécurité des données désigne un événement qui donne lieu à une suspicion raisonnable que des données à caractère personnel sont illégalement saisies, collectées, modifiées, copiées, transmises ou utilisées. Il peut s'agir d'actions de tiers ou de salariés.

Personne concernée désigne une personne physique identifiée ou identifiable. Une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou un ou plusieurs éléments spécifiques à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique.

Le **sous-traitant** est une personne physique ou morale, une autorité publique, une agence ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Registre des opérations de traitement désigne un enregistrement du traitement des données sous la responsabilité du responsable du traitement. Ce registre contient l'ensemble des informations suivantes: (i) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du coordinateur local de la protection des données; (ii) les finalités du traitement; (iii) une description des catégories de personnes concernées et de la catégorie de données à caractère personnel; (iv) les catégories de destinataires auxquels des données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers; (v) le cas échéant, le transfert de données à caractère personnel vers un pays tiers, y compris l'identification du pays tiers et la documentation relative aux garanties appropriées; (vi) les délais prévus pour l'effacement des différentes catégories de données à caractère personnel; (vii) une description générale des mesures de sécurité techniques et organisationnelles.

Délégué à la protection des données ou coordinateur de la protection des données ou **DPD** désigne la personne décrite dans la section 5.

Le terme **données à caractère personnel** désigne toutes les informations (y compris les données à caractère personnel de catégories particulières) relatives à la personne concernée, à savoir se rapportant à une personne physique identifiée ou identifiable, telles que le nom, la date de naissance, l'adresse électronique, la religion, les données de localisation, les données en ligne (adresse IP, données de localisation, etc.), les numéros d'identification (numéro de sécurité sociale, numéro de carte d'identité, etc.), les caractéristiques physiques (sexe, peau, cheveux, couleur des yeux, etc.), les données relatives aux clients, etc., qui sont soumises à un règlement applicable en matière de protection des données.

Traitement désigne toute opération ou séquence d'opérations effectuée, de manière automatisée ou non, en lien avec des données à caractère personnel telle que la collecte, l'enregistrement, l'organisation, le classement, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Pseudonymisation désigne le traitement de données à caractère personnel de sorte à rendre impossible leur attribution à une personne spécifique sans l'utilisation d'informations supplémentaires, à condition que ces informations supplémentaires soient conservées séparément et fassent l'objet de mesures techniques et organisationnelles garantissant que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

Les termes **données à caractère personnel de catégories particulières** désignent les données révélant l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques, les condamnations pénales, l'appartenance syndicale, la santé

ou l'orientation sexuelle de la personne concernée ou les données génétiques, les données biométriques permettant d'identifier sans ambiguïté une personne physique.

Le terme **Pays tiers** désigne toutes les nations qui ne sont pas un pays de l'Union européenne ou de l'Espace économique européen ou un pays ayant un niveau de protection des données jugé adéquat par la Commission européenne (voir la liste des pays ayant un niveau de protection des données adéquat:
< https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >.

Le terme **Tiers** désigne toute personne autre que la personne concernée, le responsable du traitement ou le sous-traitant (y compris, notamment, les partenaires commerciaux, les sous-traitants, les organismes de crédit et autres) ainsi que les personnes autorisées à traiter des données à caractère personnel sous l'autorité directe du responsable du traitement ou du sous-traitant. Lorsqu'ils traitent des données à caractère personnel dans le cadre d'une licence, les sous-traitants ne sont pas des tiers au sens de la loi sur la protection des données, car elles sont légalement attribuées au responsable du traitement.

3 PORTÉE

3.1 Portée organisationnelle

La présente directive sur la protection des données vaut pour toutes les sociétés du groupe Arbonia, tous les salariés d'Arbonia et les membres du conseil d'administration d'Arbonia AG. Elle est à appliquer de manière juridiquement contraignante dans chaque société du groupe.

3.2 Lois, règlements, normes et directives

La présente directive sur la protection des données couvre les exigences du RGPD et les principes de protection des données internationalement reconnus, sans remplacer le droit national existant. Elle complète les lois sur la protection des données applicables à l'échelle nationale. Le droit national applicable prévaut en cas de conflit avec la présente directive sur la protection des données ou si les exigences sont plus strictes que la présente directive sur la protection des données. Le contenu de la présente directive sur la protection des données doit être respecté même s'il n'existe pas de législation nationale correspondante.

Si la présente directive sur la protection des données est en conflit avec les réglementations d'un pays particulier, les dispositions spécifiques de cette directive sur la protection des données peuvent être adoptées dans une directive locale en consultation avec le chef du service juridique et de la conformité. Néanmoins, le contenu et l'objet fondamentaux des dispositions concernées ne peuvent être modifiés.

4 FONDEMENT RÉGLEMENTAIRE

La présente directive sur la protection des données se fonde sur le RGPD et les principes de base de la protection des données acceptées dans le monde entier.

5 RÔLES ET RESPONSABILITÉS

- La responsabilité du directeur d'une société du groupe[1] consiste à:
  1. Veiller in fine au respect des obligations légales en matière de traitement des données à caractère personnel.
  2. Veiller au respect des exigences stipulées dans la présente directive sur la protection des données (y compris la notification en cas d'incidents liés à la sécurité des données).
  3. Veiller à la tenue et à la mise à jour du «Registre des opérations de traitement» au niveau de la société du groupe par le responsable du processus de gestion.
  4. Nommer officiellement un délégué local à la protection des données (interne ou externe) (ci-après dénommé «délégué à la protection des données») si le règlement local applicable en matière de protection des données l'exige et informer le chef du service juridique, de la conformité et de l'audit interne de la nomination de cette personne tous les douze mois, en milieu d'année.
  5. Désigner un responsable local de la protection des données (ci-après dénommé «coordinateur de la protection des données»), si le règlement local applicable en matière de protection des données n'exige pas la désignation officielle d'un délégué local à la protection des données. Informer le chef du service juridique, de la conformité et de l'audit interne de la nomination de cette personne tous les douze mois, en milieu d'année.

- Le coordinateur local de la protection des données ou le délégué à la protection des données désigné[2] par le directeur d'une société du groupe doit:
  1. Contrôler le respect de la présente directive sur la protection des données et des instructions du responsable du traitement ou du sous-traitant concernant la protection des données à caractère personnel, déléguer les responsabilités et effectuer les vérifications correspondantes.
  2. Informer, conseiller et superviser le responsable du traitement ou le sous-traitant et les salariés qui exécutent des obligations de traitement en vertu de la présente directive sur la protection des données.
  3. Sur demande, conseiller sur une analyse d'impact relative à la protection des données à caractère personnel, en contrôler les résultats et répondre à d'autres questions concernant les données à caractère personnel qui lui sont adressées en vertu de la présente directive sur la protection des données.

[1] Pour les sociétés du groupe sans activité opérationnelle, cette responsabilité est déterminée séparément en consultation avec le chef du service juridique et de la conformité.
[2] Pour les sociétés du groupe sans activité opérationnelle, cette responsabilité est déterminée séparément en consultation avec le chef du service juridique et de la conformité.

4. Contrôler et mettre à jour le «Registres opérations de traitement», tenue par la société respective du groupe et remplie par les responsables des processus de gestion, puis confirmer le caractère complet et actuel du registre au directeur et au chef du service juridique et de la conformité tous les douze mois en milieu d'année.
5. Servir de point de contact pour le chef du service juridique et de la conformité et le tenir informé des responsabilités, des risques et des difficultés concernant la protection des données à caractère personnel.
6. Aider le service informatique responsable de l'application informatique à examiner et approuver les nouvelles applications informatiques au niveau des sociétés du groupe pour le traitement des données à caractère personnel ainsi que toute application informatique pour le traitement de catégories particulières de données à caractère personnel eu égard à la protection des données.
7. Autoriser le transfert de données à caractère personnel vers un pays tiers eu égard à la protection des données (voir également ci-dessous, point 14).
8. Servir de point de contact local pour l'autorité de contrôle pour toute question relative au traitement des données et coopérer avec l'autorité de contrôle,
9. Traiter les demandes des salariés impliqués dans le traitement des données à caractère personnel.
10. Répondre aux demandes d'information des personnes concernées sur les données à caractère personnel détenues par Arbonia ou, dans le cas d'une demande concernant plusieurs sociétés du groupe Arbonia, la traiter en coordination avec Corporate IT (voir aussi ci-dessous, point 7.4)
11. Examiner et approuver les contrats ou conventions préparés ou révisés en amont par le responsable du processus de gestion et conclus avec le sous-traitant habilité à traiter des données à caractère personnel pour le compte d'Arbonia, comme décrit dans la section 7.2.
12. Contrôler le délégué local externe à la protection des données s'il a été désigné.
13. Signaler les incidents dans le domaine de la sécurité des données conformément à la directive sur la notification des violations de données (voir point 9 ci-dessous et «Politique d'Arbonia en matière de violations de données»).

- Responsabilités conjointes de l'IT-Board et de Corporate IT:
  1. Définir les normes applicables dans l'ensemble du groupe et les contrôles informatiques généraux (GITC) à respecter lors de la conservation de données.

- Responsabilités du service informatique assurant le suivi d'une société du groupe:
  1. Veiller, au moyen des normes, des politiques et de la mise en œuvre des contrôles informatiques généraux (GITC), à la conformité des systèmes, services et équipements utilisés pour conserver les données aux normes de sécurité acceptables (contrôle d'accès/effacement des données), en tenant compte des avancées techniques, des coûts de mise en œuvre, de la nature, de la portée, du contexte et de la finalité du traitement ainsi que de différents degrés de probabilité et de gravité de l'impact sur les droits et libertés des personnes physiques.

2. Préparer la voie au responsable du traitement et au sous-traitant pour qu'ils mettent en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de protection proportionné au risque, comme prévu dans la section 8.
3. Après consultation auprès du coordinateur de la protection des données ou du délégué à la protection des données, examiner et approuver les nouvelles applications informatiques de traitement des données à caractère personnel sous l'angle de la protection des données.
4. Effectuer des analyses et des contrôles réguliers pour s'assurer que le matériel et les logiciels de sécurité fonctionnent correctement. Les résultats des contrôles de protection des données doivent être communiqués au délégué à la protection des données compétent.
5. Évaluer la sécurité des données de tout service tiers (notamment les sous-traitants) que l'entreprise envisage d'utiliser pour traiter des données à caractère personnel [entre autres les services d'informatique en nuage (Cloud Computing), etc.]
6. Tenir à jour une liste des incidents de sécurité des données et signaler les incidents de sécurité des données au Corporate IT.
7. Coordonner et répondre aux demandes d'information des personnes concernées sur les données à caractère personnel détenues par la société du groupe Arbonia à l'appui du service informatique concerné (voir également le point 7.4 ci-dessous)
8. Signaler les incidents ou risques décelés dans le domaine de la sécurité des données analogues à ceux évoqués dans la directive sur la notification des violations de données (voir point 9 ci-dessous et «Politique d'Arbonia en matière de violations de données»)

- Responsabilités de Corporate IT en collaboration avec le service informatique assurant le suivi d'une société du groupe:
  1. Effectuer des analyses et des contrôles réguliers pour s'assurer que le matériel et les logiciels de sécurité fonctionnent correctement. Les résultats des contrôles de protection des données doivent être communiqués au délégué à la protection des données compétent.
  2. Tenir à jour une liste des incidents de sécurité des données.
  3. Signaler les incidents ou risques décelés dans le domaine de la sécurité des données analogues à ceux évoqués dans la directive sur la notification des violations de données (voir point 9 ci-dessous et «Politique d'Arbonia en matière de violations de données»).

- Responsabilités de l'audit interne:
  1. Vérifier, au cours des audits réalisés conformément à la planification régulière des audits, dans le cadre d'un audit fondé sur les risques, si les procédures organisationnelles sont conformes aux exigences essentielles de la présente directive sur la protection des données.

- Compétences du responsable du processus de gestion:

1. Assurer l'intervention appropriée et en temps utile du délégué local à la protection des données pour tout ce qui a trait à l'évaluation du traitement des données à caractère personnel.
2. Préparer ou réviser en amont les contrats ou conventions à conclure avec le sous-traitant habilité à traiter des données à caractère personnel pour le compte d'Arbonia, comme décrit dans la section 7.2.
3. Remplir et mettre à jour le «Registre des opérations de traitement», tenu par la société respective du groupe, puis confirmer le caractère complet et actuel des entrées au coordinateur de la protection des données ou au délégué à la protection des données chaque année avant la fin du mois d'avril.
4. Avant de mettre en œuvre de nouvelles opérations de traitement de données à caractère personnel, évaluer les risques qui en résultent pour la personnalité et les droits fondamentaux de la personne concernée et, en cas de risque élevé lié au traitement, effectuer en amont une analyse d'impact relative à la protection des données.

6 PRINCIPES DE PROTECTION DES DONNÉES DANS LE CADRE DU TRAITEMENT DES données à caractère personnel

Chaque société du groupe agissant en tant que responsable du traitement des données à caractère personnel doit s'assurer qu'elle peut démontrer le respect des **6 (six) principes clés suivants en matière de protection des données:**

1. Traiter des données à caractère personnel uniquement si une base juridique valable au regard des lois applicables en matière de protection des données peut être prouvée et si la personne concernée est informée de l'identité et des coordonnées du responsable du traitement, de la nature et de la base juridique des données à caractère personnel collectées, des périodes de conservation respectives et de la finalité de la collecte des données à caractère personnel

2. Toujours respecter la finalité à l'origine de la collecte des données à caractère personnel

3. Exclusivement collecter/traiter les données à caractère personnel réellement nécessaires

4. Conserver les données à caractère personnel correctes et supprimer les données à caractère personnel incorrectes

5. Conserver les données à caractère personnel exclusivement pendant les périodes de conservation légales réellement nécessaires

ARBONIA

6. Préserver la confidentialité des données à caractère personnel et partager exclusivement les éléments nécessaires

6.1 Équité, légalité et transparence

Seules peuvent être traitées les données collectées aux fins spécifiquement autorisées décrites ci-après et en totale transparence. Les données à caractère personnel doivent être traitées légalement et équitablement dans le respect des droits individuels des personnes concernées. Il peut s'agir de données à caractère personnel qu'Arbonia reçoit directement d'une personne concernée (par exemple par renseignement d'un formulaire ou correspondance avec nos services via courrier, téléphone, e-mail ou autre) ainsi que de données à caractère personnel reçues par Arbonia de tiers.

En vertu des lois applicables en matière de protection des données, les données à caractère personnel peuvent être traitées légalement sur la base de l'un des **cinq motifs légitimes** (les **motifs légitimes**) conformément au RGPD. Ces motifs sont les suivants:

1. **Contrat:** le traitement de données à caractère personnel est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée, ou

2. **Consentement:** le traitement des données à caractère personnel est fondé sur le consentement (modèle d'adhésion) de la personne concernée à plusieurs fins spécifiques ou à une seule. Le consentement doit être documenté, ou

3. **Obligation légale:** le traitement des données à caractère personnel se fonde sur une obligation légale d'Arbonia. La nature et la portée du traitement des données doivent être nécessaires au traitement légalement autorisé et respecter les conditions légales applicables, ou

4. **Intérêt public:** le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public ou

5. **Intérêts commerciaux légitimes :** le traitement des données à caractère personnel est considéré comme étant proportionnel aux intérêts commerciaux légitimes d'Arbonia ou du tiers auquel les données à caractère personnel sont communiquées, à moins que les intérêts ou les droits et libertés fondamentaux de la personne concernée ne prévalent sur ces intérêts. Les intérêts légitimes sont de nature juridique générale (entre autres recouvrement de créances impayées/en lien avec une convention collective avec le comité d'entreprise/la constatation/l'exercice ou la défense de droits en justice impliquant la personne concernée) ou commerciale (notamment prévention de manquements au contrat).

La transparence exige que la personne concernée soit informée du mode de traitement de ses données. Pour cette raison, il est généralement recommandé de recueillir les données à caractère personnel directement auprès de la personne concernée (et non par l'intermédiaire d'un tiers). Lorsque des données à caractère personnel sont traitées, la personne concernée doit être informée des éléments suivants:

- le nom et les coordonnées du responsable du traitement et, le cas échéant, de son représentant dans l'UE
- le cas échéant, les coordonnées du coordinateur de la protection des données ou du délégué à la protection des données
- la finalité du traitement des données à caractère personnel et le fondement juridique du traitement,
- les destinataires tiers ou catégories de destinataires tiers auxquels les données peuvent être transmises
- le cas échéant, informations sur le traitement dans un pays tiers et référence à des garanties appropriées

6.2 Affectation aux seules utilisations prévues

Les données à caractère personnel ne peuvent être traitées que pour la finalité communiquée à la personne concernée avant la collecte des données à caractère personnel. La portée de toute modification ultérieure de la finalité ne peut être que limitée et requiert une justification. Le responsable du traitement est tenu d'informer la personne concernée de la finalité du traitement de ses données à caractère personnel par Arbonia lors de la première collecte ou dès que possible après celle-ci. Tout traitement à des fins publicitaires ou de programmes de marketing doit octroyer à la personne concernée le droit de s'opposer au traitement de ses données à caractère personnel et garantir qu'elle soit expressément informée de ce droit. À cet égard, chaque responsable doit mettre en place un système de traitement des plaintes qui garantit le respect des clauses de non-adhésion.

6.3 Minimisation des données

Traiter exclusivement les données à caractère personnel réellement nécessaires. Avant de traiter des données à caractère personnel, déterminer si et dans quelle mesure le traitement des données à caractère personnel est nécessaire pour atteindre sa finalité première. Les données à caractère personnel de doivent pas être collectées ni conservées à l'avance pour de potentielles futures finalités, à moins que cela ne soit requis ou autorisé par le droit national.

6.4 Exactes et à jour

Les données à caractère personnel doivent être correctes, complètes et, si modifiées, mises à jour. Prendre des mesures appropriées pour garantir l'effacement, la correction, la modification ou l'actualisation de données à caractère personnel inexactes ou incomplètes.

Toute personne traitant des données à caractère personnel est tenue de prendre des mesures appropriées à cet égard (notamment en confirmant les données d'une personne concernée lorsqu'elle appelle ou en supprimant un numéro de téléphone enregistré dans la base de données lorsque la personne concernée ne l'utilise plus).

6.5 Durée de conservation limitée

Conserver exclusivement les données à caractère personnel pendant la durée réellement nécessaire. Supprimer les données à caractère personnel dès qu'elles ne sont plus nécessaires aux fins prévues, si le consentement est retiré ou si l'utilisation est contestée sur la base d'un intérêt légitime et qu'Arbonia n'est pas en mesure d'invoquer des motifs légitimes et impérieux. Dans certains cas, des périodes de conservation plus longues peuvent nous permettre de conserver des données à caractère personnel plus longtemps si la loi l'exige (notamment en vertu des lois fiscales ou commerciales) ou si les données à caractère personnel sont nécessaires pour faire valoir, exercer ou défendre des droits en justice.

6.6 Confidentialité et sécurité des données

Préserver à tout moment la confidentialité des données à caractère personnel et partager exclusivement les éléments nécessaires. Le principe des «informations nécessaires» s'applique de sorte que les salariés et les tiers n'ont accès aux données à caractère personnel que si et dans la mesure où cela est nécessaire pour atteindre l'objectif. Cela requiert un concept minutieusement élaboré qui définit les droits d'accès spécifiques pour chaque processus opérationnel, y compris la mise en œuvre et l'approbation des rôles et responsabilités (concept de droits d'accès). Les destinataires des données à caractère personnel doivent être informés de la confidentialité des données à caractère personnel et **soumis à un accord de secret professionnel/confidentialité** (comme partie intégrante du contrat de travail ou similaire). Exception: le destinataire est soumis à une obligation de secret professionnel ou légal.

Les données à caractère personnel doivent être sécurisées par des mesures organisationnelles et techniques appropriées pour prévenir tout accès illégal, tout traitement ou divulgation illégal et toute perte, altération ou destruction involontaire (voir section 8).

7 AUTRES OBLIGATIONS EN VERTU DU RGPD OU D'AUTRES RÉGLEMENTATIONS SIMILAIRES APPLICABLES EN MATIÈRE DE PROTECTION DES DONNÉES

7.1 Principe de l'obligation de rendre compte

Une société du groupe Arbonia soumise au RGPD (ou à une réglementation similaire applicable en matière de protection des données) doit s'assurer de pouvoir démontrer qu'elle respecte les lois applicables en matière de protection des données (principe de l'«Obligation de rendre compte»). Pour cette raison, outre les exigences générales de la présente directive sur la protection des données, ces sociétés du groupe doivent mettre en œuvre et maintenir

les points suivants, le directeur de la société du groupe concernée étant responsable en dernier ressort de la mise en œuvre et de la maintenance:

1. Coordinateur local de la protection des données ou délégué à la protection des données: désignation d'un coordinateur local de la protection des données ou d'un délégué à la protection des données spécifique

2. Tenue du «Registre des traitements»: tenue et mise à jour d'un inventaire des activités de traitement des données à caractère personnel

3. Vérification de la légitimité: le traitement légal des données à caractère personnel conformément aux motifs légitimes valables doit être vérifié, notamment lors du traitement de catégories particulières de données à caractère personnel

4. Contrôle du sous-traitant: conclusion d'un contrat de sous-traitance avec le sous-traitant ou en qualité de sous-traitant pour la fourniture ou la réception de données à caractère personnel dans le cadre d'une licence conformément à l'article 28 du RGPD.

5. Dans le cas de responsables conjoints du traitement, prévoir une convention entre les responsables conjoints du traitement en vertu de l'article 26 du RGPD.

6. Les salariés d'Arbonia doivent être informés des activités de traitement des données à caractère personnel.

7.2 Règles pour le sous-traitant (principalement les partenaires de service)

Le responsable du traitement fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du de l'article 28 du RGPD et garantisse la protection des droits de la personne concernée.

Pour les prestations partagées au sein d'Arbonia, il existe une convention permettant de transférer des données à caractère personnel, à condition que le transfert de ces données à caractère personnel repose sur des motifs juridiques légitimes conformément aux lois applicables en matière de protection des données.

7.2.1 Fourniture de données à caractère personnel au sous-traitant (sortantes)

Le traitement de données à caractère personnel dans le cadre d'une licence signifie qu'un prestataire de services est engagé par contrat pour traiter des données à caractère personnel sans transfert de la responsabilité du processus de gestion correspondant (c'est-à-dire les

prestataires de services, les services externalisés). Dans ce cas, un contrat de sous-traitance pour le traitement des données à caractère personnel doit être conclu avec des fournisseurs externes dans le cadre d'une licence. La société respective du groupe Arbonia est responsable du traitement et assume l'entière responsabilité du traitement correct des données à caractère personnel par le sous-traitant.

Le responsable du processus de gestion respectif doit s'assurer que le modèle actuel d'accord de sous-traitance, ou un contrat similaire fourni par le prestataire de services pour répondre aux exigences de l'article 28 RGPD, est utilisé pour mandater les prestataires de services. Un prestataire de services peut également prouver qu'il respecte les exigences en matière de sécurité des données en présentant une certification européenne appropriée et approuvée. Tout écart par rapport à cette norme de sécurité doit être approuvé par le délégué à la protection des données ou le coordinateur de la protection des données en collaboration avec Corporate IT. Les contrats existants doivent être révisés dans un délai d'un an à compter de l'entrée en vigueur de la présente directive sur la protection des données et doivent comprendre un accord écrit de sous-traitance.

7.2.2 Réception de données à caractère personnel en qualité de sous-traitant (entrantes)

Si des données à caractère personnel sont transférées à une société du Groupe Arbonia par un tiers, s'assurer que les données à caractère personnel (i) peuvent être utilisées pour la finalité prévue, (ii) sont collectées pour des motifs légitimes (il est recommandé d'obtenir une confirmation écrite) et (iii) qu'il existe un contrat de sous-traitance conforme à l'article 28 du RGPD.

7.3 Transfert transfrontalier de données à caractère personnel

Dans le cas d'un transfert transfrontalier de données à caractère personnel, les exigences nationales respectives applicables à la divulgation de données à caractère personnel à l'étranger doivent être respectées. En vertu du RGPD, un transfert de données à caractère personnel peut avoir lieu au sein de l'UE, de l'EEE ou vers un pays dont la Commission européenne a déterminé qu'il offre des garanties suffisantes pour assurer un niveau adéquat de protection des données. Aucune autorisation spéciale n'est requise pour ce type de transfert de données. La Commission européenne a classé la Suisse comme offrant une protection appropriée (voir la liste actuelle de ces pays:
< https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >.

Un transfert de données à caractère personnel vers un pays tiers n'est autorisé que si des garanties supplémentaires adéquates sont mises en place. Autrement dit, si le destinataire peut prouver qu'il respecte une norme de protection des données conforme à la présente directive sur la protection des données (par exemple i) existence de règles d'entreprise contraignantes, ii) conclusion de clauses contractuelles types de l'UE pour la sous-traitance

dans des pays tiers avec le prestataire de services et d'autres sous-traitants[3], iii) existence de règles de conduite approuvées par l'autorité de contrôle, iv) intégration du prestataire de services dans un système de certification accrédité par l'UE pour atteindre un niveau adéquat de protection des données, ou v) existence d'accords individuels entre le responsable du traitement et le sous-traitant soumis à autorisation de l'autorité de contrôle compétente) et à l'obligation d'informer la personne concernée. Cette obligation ne s'applique pas si la transmission se fonde sur une obligation légale. Un tel transfert requiert l'approbation du coordinateur de la protection des données ou du délégué à la protection des données.

Si des données à caractère personnel sont transférées au sein d'Arbonia, la société du groupe qui importe les données à caractère personnel est tenue de coopérer à la résolution de toutes les demandes faites par l'autorité de contrôle compétente du pays dans lequel la société du groupe exportatrice a son siège social, et de se conformer à toutes les observations faites par l'autorité de contrôle respective concernant le traitement des données à caractère personnel transférées.

7.4 Traitement d'une demande d'information par une personne concernée

Les personnes concernées ont le droit de faire une demande formelle d'information sur les détails des données à caractère personnel détenues par Arbonia et peuvent demander les éléments suivants:

Droit d'accès à l'information concernant:

- la finalité du traitement;
- les catégories de données à caractère personnel traitées;
- les destinataires ou les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, notamment les destinataires dans les pays tiers ou les organisations internationales;
- lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;
- l'existence du droit de demander au 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;
- toutes les informations disponibles sur l'origine des données à caractère personnel si elles ne sont pas collectées auprès de la personne concernée;
- l'existence d'une prise de décision automatisée, y compris le profilage;

[3] Voir la décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil, < https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087 >

- Lorsque les données à caractère personnel sont transférées vers un pays tiers ou à une organisation internationale, la personne concernée a le droit d'être informée des garanties appropriées.

Droit de rectification

- La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient mises à jour, y compris en fournissant une déclaration complémentaire.

Droit à l'effacement («Droit à l'oubli»):

- La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique:
  1. Les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière;
  2. La personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a du RGPD, ou à l'article 9, paragraphe 2, point a du RGPD, et il n'existe pas d'autre fondement juridique au traitement;
  3. La personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1 du RGPD, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2 du RGPD;
  4. Les données à caractère personnel ont fait l'objet d'un traitement illicite;
  5. Les données à caractère personnel doivent être supprimées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis;
  6. Les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1 du RGPD.

Droit à la limitation du traitement

- La personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement lorsque l'un des éléments suivants s'applique:
- l'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel;
- le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation;

- le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement, mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice;
- la personne concernée s'est opposée au traitement en vertu de l'article 21, paragraphe 1, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée.

La personne concernée doit être invitée à soumettre sa demande par écrit, soit par courrier électronique, soit par courrier postal, adressée au délégué local à la protection des données compétent. Les informations sont fournies à la personne concernée par le délégué local à la protection des données sans délai, mais, en tout état de cause, dans le mois suivant la réception de la demande. Cette période peut être prolongée de deux mois compte tenu de la complexité et du nombre de demandes. Dans le mois suivant la réception de la demande, le délégué local à la protection des données ou le coordinateur de la protection des données du responsable du traitement informe la personne concernée de la prolongation du délai ainsi que des motifs du retard. La personne concernée ne peut encourir aucun frais pour s'enquérir des informations qu'une société du Groupe Arbonia détient à son sujet, sauf si les demandes de la personne concernée sont manifestement infondées ou excessives, notamment en raison d'une position répétée. Les demandes d'une personne concernée ayant trait à plusieurs sociétés du groupe Arbonia doivent être transmises à Corporate IT pour coordination et réponse.

7.5 Réalisation d'une analyse d'impact relative à la protection des données

Lorsqu'un nouveau type de traitement des données à caractère personnel prévu, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne concernée, avant le traitement, réaliser une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

Avant de mettre en œuvre de nouvelles opérations de traitement de données à caractère personnel, évaluer les risques qui en résultent pour la personnalité et les droits fondamentaux de la personne concernée. Dans le cas de nouvelles applications informatiques, prendre en compte et aspect dans le processus d'approbation. Si une première évaluation indique qu'une nouvelle forme de traitement de données à caractère personnel envisagée est susceptible de présenter un risque élevé pour la personne concernée, effectuer une analyse d'impact relative à la protection des données.

Les demandes d'information concernant la nécessité ou le déroulement d'une analyse d'impact relative à la protection des données doivent être adressées au coordinateur local de la protection des données ou au délégué local à la protection des données. Après avoir procédé à l'analyse d'impact relative à la protection des données. informer le coordinateur

local de la protection des données ou le délégué local à la protection des données et solliciter son avis.

Lorsqu'il ressort de l'analyse d'impact relative à la protection des données que le traitement comporte un risque élevé pour la personne concernée et qu'aucune mesure appropriée visant à atténuer le risque n'est prise, il convient de consulter l'autorité de contrôle avant la mise en œuvre de nouvelles procédures de traitement.

8 SÉCURITÉ DES DONNÉES À CARACTÈRE PERSONNEL

Les données à caractère personnel doivent être protégées contre tout accès illégal, toute divulgation ou tout traitement illégal ainsi que toute perte, altération ou destruction involontaire. Cela s'applique que le traitement des données à caractère personnel soit électronique ou sur papier.

Le responsable du traitement et le sous-traitant doivent mettre en œuvre des mesures techniques et organisationnelles appropriées pour protéger les données contre tout traitement illégal. Ces mesures doivent s'inspirer (i) des meilleures pratiques, (ii) des risques du traitement, et (iii) de la nécessité de protéger les données à caractère personnel (telle que déterminée par le processus de classification des informations); elles comprennent, entre autres, en fonction des besoins:

(a) la pseudonymisation et le chiffrement des données à caractère personnel;

(b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

(c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;

(d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Les mesures techniques et organisationnelles de protection des données à caractère personnel font partie de la gestion interne de la sécurité de l'information et doivent être constamment adaptées aux avancées techniques et aux changements organisationnels.

Les procédures de sécurité peuvent comprendre au moins:

- Contrôles d'accès: toute personne externe au service localisée dans les zones d'accès contrôlées doit être signalée.

- Tiroirs ou armoires de classement verrouillables et sécurisés: les bureaux et les armoires doivent être maintenus verrouillés s'ils contiennent des informations confidentielles de quelque nature que ce soit. Les données à caractère personnel sont toujours des informations confidentielles. Les salariés doivent veiller à ne pas laisser du papier et des imprimés contenant des données à caractère personnel à la vue de tous, par exemple dans une imprimante. Lorsque des données à caractère personnel autorisées sont enregistrées sur un support amovible (tel qu'un CD, une clé USB ou un DVD), les conserver sous clé en toute sécurité lorsqu'elles ne sont pas utilisées.
- Méthodes d'élimination: les documents sur papier doivent être broyés et éliminés de manière sûre lorsqu'ils ne sont plus nécessaires. Cela vaut également pour les données à caractère personnel généralement conservées sur support électronique, mais qui ont été imprimées.

- Données conservées sous forme électronique: les données à caractère personnel doivent être protégées par des mots de passe conformément à la directive actuelle en matière de mots de passe qui ne doivent jamais être partagés entre les salariés. Si la forme électronique est applicable, les données à caractère personnel doivent être conservées et récupérées sur des systèmes de serveurs informatiques et dans des applications informatiques structurées plutôt que sur des ordinateurs locaux sous forme non cryptée.

- Données à caractère personnel collectées sous forme électronique et fournies par la personne concernée: l'identité de la personne concernée doit être vérifiée, de préférence par un procédé de double adhésion (c'est-à-dire un deuxième e-mail pour valider l'adresse e-mail fournie). Si l'accès à un site web ou à une application est limité aux utilisateurs enregistrés (c'est-à-dire au compte d'utilisateur), l'identification et l'authentification de la personne concernée doivent fournir une protection de sécurité proportionnelle au contenu lors de l'accès.

- Faire preuve de prudence lors du partage de données à caractère personnel: ne jamais partager des données à caractère personnel manière informelle. Règle de principe des «informations nécessaires». Un concept de ventilation et de séparation par processus opérationnel et la mise en œuvre des rôles et responsabilités sont obligatoires. Les données à caractère personnel doivent être cryptées sous forme électronique avant leur transmission. Le responsable des technologies de l'information peut expliquer comment les données à caractère personnel sont envoyées aux contacts externes autorisés.

- Demande d'instructions: en cas de questions ou de doutes concernant un aspect quelconque de la protection des données ou les obligations découlant de la présente

directive relative à la protection des données, s'adresser au supérieur hiérarchique direct, au délégué local à la protection des données ou au service juridique et de la conformité.

Le RGPD exige que la vie privée soit prise en considération le plus tôt possible. Le respect de la vie privée lors de la configuration technologique exige que les organisations s'attellent à ce sujet dès les premières étapes de cette configuration et lors du développement de nouveaux produits, processus ou prestations qui impliquent le traitement de données à caractère personnel. La protection de la vie privée par défaut signifie que lorsqu'un système ou un service implique qu'une personne décide de la quantité de données à caractère personnel à partager avec d'autres, les paramètres par défaut doivent être ceux qui assurent la plus grande protection de la vie privée. Pour cette raison, chaque nouvelle application informatique est soumise à un processus d'approbation interne qui évalue cette nouvelle application informatique sous l'angle de la protection des données.

9 NOTIFICATION DES INCIDENTS DANS LE DOMAINE DE LA SÉCURITÉ DES DONNÉES

De nombreuses réglementations applicables en matière de protection des données exigent que les incidents liés à la protection des données soient signalés directement au législateur. Pour cette raison, il est nécessaire que tous les incidents liés à la sécurité des données soient immédiatement signalés au coordinateur de la protection des données ou au délégué à la protection des données, qu'il s'agisse d'un système local ou d'un système de groupe, conformément à la procédure décrite dans la directive d'Arbonia en matière de sécurité des données («Politique d'Arbonia en matière de violations de données»). Si le service informatique détecte des incidents ou des risques dans le domaine de la sécurité des données, ceux-ci doivent être signalés conformément à la directive sur la notification des violations de données.

L'objectif est de respecter les obligations relatives à la notification d'une violation des obligations en matière de protection des données en vertu des lois applicables en la matière (notamment en vertu du RGPD, au plus tard dans les 72 heures après en avoir eu connaissance).

Dans un tel cas, l'accent doit être mis sur le respect des délais respectifs de notification des violations de données et sur la prise de mesures immédiates pour enquêter sur les incidents et déterminer si des données à caractère personnel ont effectivement été violées. Corporate IT doit tenir un registre interne des violations de la sécurité au sein d'Arbonia devant permettre de respecter les obligations de signalement prévues par le droit national et de veiller à l'application des règles de suppléance respectives pour pouvoir signaler à tout moment les violations. Avant tout signalement auprès d'une autorité nationale, informer Corporate IT ou le service juridique et de la conformité.

Respecter scrupuleusement toutes les autres instructions de Corporate IT et des services informatiques locaux.

10 CONSÉQUENCES D'UN MANQUEMENT

Le respect de la présente directive sur la protection des données revêt la plus haute importance pour Arbonia et la manière dont le public perçoit Arbonia. Le traitement inapproprié des données à caractère personnel ou d'autres violations des lois sur la protection des données peuvent également faire l'objet d'une injonction pénale dans de nombreux pays et donner lieu à des demandes de dommages et intérêts. Au sein d'Arbonia, une violation des règles de la présente directive sur la protection des données peut entraîner des sanctions en vertu de la loi et/ou du contrat (de travail) concerné.

11 DÉROGATIONS

Les dérogations aux dispositions de la présente directive et de ses addenda ne sont autorisées qu'après consultation du chef du service juridique et de la conformité.

12 RENSEIGNEMENTS

La transmission de renseignements concernant la directive sur la protection des données relève du chef du service juridique et de la conformité.

13 ENTRÉE EN VIGUEUR

La présente directive entre en vigueur le 17 juin 2020 et remplace la directive sur le traitement des données (directive sur la protection des données) du 5 décembre 2013.

Arbon, le 16 juin 2020

Arbonia AG

Alexander von Witzleben
Président du conseil d'administration et CEO

Andrea Wickart
Head of Legal & Compliance / Secrétaire générale

ARBONIA

Addenda à la présente directive sur la protection des données

Les addenda suivants dans leur version actuelle précisent la présente directive sur la protection des données:

- Directive sur les demandes des personnes concernées et l'effacement des données
- Directive sur les violations de la protection des données
- Déclaration de confidentialité envers les salariés

Le présent document est valable sans signature.