MIC Datenverarbeitung GmbH
Hafenstraße 24
A-4020 Linz
Téléphone +43(70)77 84 96-0
Télécopieur +43(70)77 84 96-600
e-mail office@mic-cust.com

Politique de confidentialité de MIC

Date : 10/02/2020

Version : 2.0

Informations sur le document

Historique des modifications

Version	Date	Description	Auteur	Statut
1.0	17/04/2018	Politique de confidentialité de MIC	SU	final
2.0	10/02/2020	Ajouts à l'organisation de la protection des données et à l'évaluation de l'impact sur la protection des données	SU	final

Table des matières

1 Objectif 5

2 Champ d'application 5

3 Principes de la confidentialité 5

3.1 Légalité, équité et transparence 5

3.2 Principes du traitement 5

3.2.1 Limites du but 6

3.2.2 Minimisation des données 6

3.2.3 Effacement des données 6

3.2.4 Exactitude et actualité 6

3.2.5 Sécurité des données, intégrité et confidentialité 6

3.2.6 Responsabilité 6

3.3 Traitement illicite 6

4 Confidentialité par conception/confidentialité par défaut 7

5 Organisation de la confidentialité 8

5.1 Rôles et responsabilités 8

5.1.1 Management 8

5.1.2 Coordinateur de la protection des données (CPD) 9

5.1.3 Responsable de la protection des données (RPD) 9

5.2 Exigences 9

5.3 Reporting 9

5.4 Réunions portant sur le RGPD 10

6 Droits de la personne concernée 11

6.1 Principes généraux 11

6.2 Informations à fournir sur les données à caractère personnel, art. 13 f) du RGPD 12

6.3 Droit d'accès par la personne concernée, art. 15 du RGPD 14

6.3.1 Comment traiter les demandes relatives au droit au renseignement 15

6.4 Rectification, art. 16 du RGPD 17
6.4.1 Comment traiter les demandes de rectification 17
6.5 Effacement, art. 17 du RGPD 18
6.5.1 Comment traiter les demandes d'effacement 18
6.6 Droit à la limitation du traitement, art. 18 du RGPD 20
6.7 Droit à la portabilité des données, art. 20 du RGPD 21
6.8 Droit d'opposition/prise de décision individuelle automatisée, art. 21 f) du RGPD 22
6.9 Obligation de notification aux destinataires, art. 19 du RGPD 23
6.10 Notification d'une violation des données à caractère personnel, art. 33 du RGPD 24
6.10.1 Procédure de notification d'une violation des données 25
7 Évaluation de l'impact 27

1 Objectif

MIC respecte la vie privée de chaque individu et considère la protection des données à caractère personnel comme une question fondamentale.

La conformité avec exigences statutaires concernant la collecte et le traitement des données à caractère personnel, qui peut varier grandement d'un pays à l'autre, est très importante pour MIC, une entreprise qui opère à l'international.

Le présent document spécifie la politique applicable chez MIC sur la base du règlement général sur la protection des données (règlement (UE) 2016/679) pour garantir la conformité avec la législation actuelle.

2 Champ d'application

La présente politique de confidentialité s'applique à toutes les entreprises du groupe MIC et à leurs employés.

La politique de confidentialité de MIC couvre toutes les données à caractère personnel traitées dans le groupe MIC.

Toutes les questions concernant la protection des données, les problèmes/supposés incidents liés à la protection des données peuvent être rapportés à l'adresse e-mail suivante : f739c41d.mic.co.at@emea.teams.ms

3 Principes de la confidentialité

3.1 Légalité, équité et transparence

Les données à caractère personnel seront traitées légalement, selon les principes de la bonne foi et sous une forme compréhensible pour la personne concernée.

MIC informera la personne concernée sur les opérations du traitement des données dans le champ d'application des droits de la personne concernée (voir article 6 ci-dessous et la politique de protection des données sur notre site web www.mic-cust.com).

3.2 Principes du traitement

3.2.1 Limites du but

MIC traite les données à caractère personnel exclusivement à des fins définies, claires et légales ; les données collectées sont traitées exclusivement d'une manière compatible au but respectif.

3.2.2 Minimisation des données

MIC se limite au minimum des données à caractère personnel nécessaires dans le champ d'application du traitement et de son but. Lorsqu'il est sensé de le faire, des données à caractère personnel rendues anonymes et/ou des pseudonymes seront utilisés dans une mesure raisonnable.

3.2.3 Effacement des données

MIC conserve des données à caractère personnel uniquement tant que cela est nécessaire pour atteindre le but et/ou comme les exigences statutaires le requièrent.

3.2.4 Exactitude et actualité

Les données à caractère personnel doivent être exactes et mises à jour, si nécessaire. MIC prend des mesures pertinentes pour effacer et/ou rectifier les données à caractère personnel incomplètes ou inexactes.

3.2.5 Sécurité des données, intégrité et confidentialité

MIC procure une sécurité raisonnable pour toutes les données à caractère personnel traitées par MIC. Des mesures techniques et organisationnelles appropriées garantissent que les données à caractère personnel sont protégées contre tout traitement non autorisé ou illicite, tout(e) perte accidentelle ou destruction accidentelle ou dommage accidentel. Pour de plus amples informations, veuillez vous référer à la politique de sécurité de MIC.

3.2.6 Responsabilité

MIC est responsable de la conformité avec les principes énumérés ci-dessus et doit être capable de démontrer cette conformité.

3.3 Traitement illicite

MIC traite les données à caractère personnel uniquement sur la base d'un fondement légal (par exemple un contrat, un consentement, une obligation légale ou un intérêt légitime) et uniquement dans le cadre du but couvert par ces dispositions.

Dans le cas de catégories spéciales de données, MIC se conformera aux exigences strictes des articles 9 et 10 du RGPD.

4 Confidentialité par conception/confidentialité par défaut

Pour pouvoir garantir la confidentialité des données à caractère personnel, il est nécessaire de considérer ce sujet dès le début du processus de développement. Cela signifie qu'il ne suffit pas d'implémenter des mesures techniques et organisationnelles appropriées pour protéger les données, mais de considérer la confidentialité au stade le plus précoce du développement.

La confidentialité par conception signifie que les organisations considèrent la confidentialité aux stades initiaux de la conception et tout au long de l'ensemble du processus de développement de nouveaux produits ou services.

La confidentialité par défaut signifie que, si un système ou service inclut différents choix sur le volume de données à caractère personnel qui devrait être partagé, les paramétrages par défaut devraient être les plus respectueux de la confidentialité.

MIC a incorporé ces deux concepts dans son processus de développement qui garantit la prise de mesures appropriées dans les phases de développement pertinentes par l'équipe chargée du développement.

Les points principaux de la mise en œuvre de ces concepts sont les suivants :

- Politiques strictes du contrôle d'accès selon le principe de la nécessité de savoir
- Suppression des concepts couvrant la suppression logique et physique (y compris la fourniture de services de suppression de données spécifiques à la demande du client)
- Travail avec des pseudonymes dans la mesure du possible et si approprié.

5 Organisation de la confidentialité

Il faut mettre en place une organisation de la confidentialité appropriée pour garantir le niveau de protection visé chez MIC et la conformité avec les principes énumérés ci-dessus.

La structure présentée sous la figure 1 comportant les rôles décrits a été définie pour implémenter l'organisation de la confidentialité.

Les dispositions statutaires ne nécessitent pas la nomination d'un délégué à la protection des données et, par conséquent, une telle nomination n'a pas eu lieu.

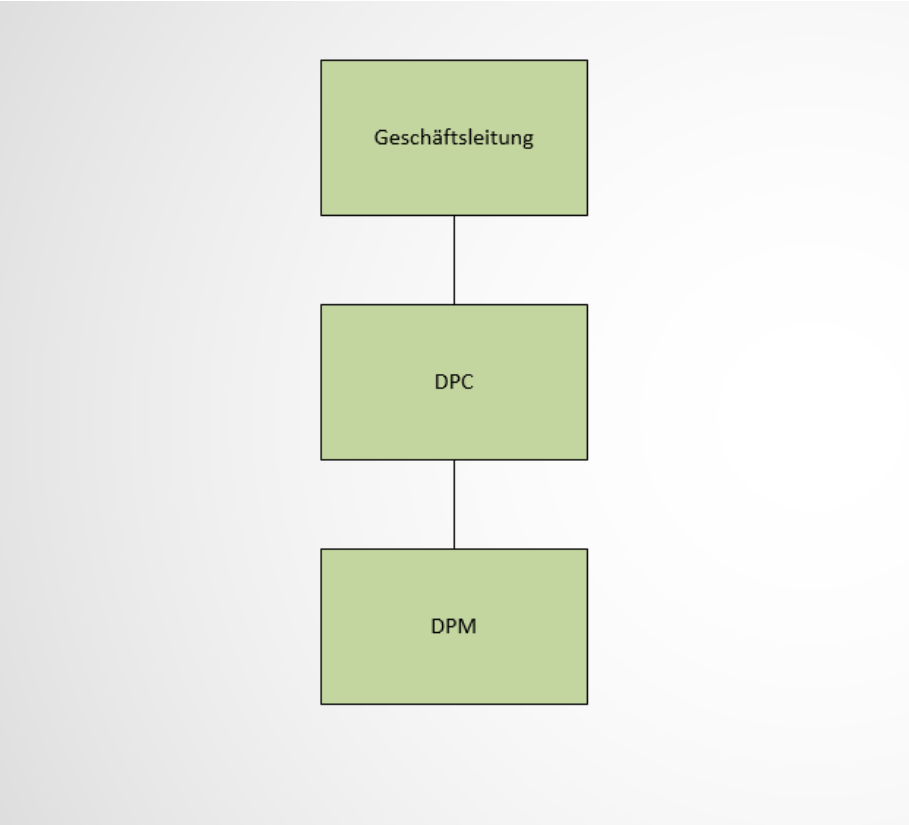

Fig. 1 – Structure de la confidentialité des données chez MIC

5.1 Rôles et responsabilités

Les tâches et responsabilités fondamentales des rôles et fonctions principaux dans l'entreprise sont définies ci-dessous.

5.1.1 Management

Le service du management de MIC est responsable de la conformité au règlement général sur la protection des données et fournit le personnel et les ressources financières nécessaires.

5.1.2 Coordinateur de la protection des données (CPD) (fig. DPC)

Le CPD est le point de contact concernant tous les problèmes relatifs à la confidentialité chez MIC et assume la responsabilité technique. Le CPD est nommé par le management jusqu'à nouvel ordre. Les missions du CPD incluent ce qui suit :

- Être le point de contact principal pour tout ce qui touche à la confidentialité
- Définir les politiques de confidentialité
- Garantir la conformité avec les dispositions statutaires pertinentes en matière de confidentialité
- Enquêter sur les événements touchant la confidentialité, le cas échéant
- Vérifier l'implémentation du règlement sur la protection des données

5.1.3 Responsable de la protection des données (RPD) (fig. DPM)

Le RPD assiste le CPD et agit en qualité de personne de contact dans le groupe MIC. Le RPD est nommé par le management jusqu'à nouvel ordre. Les missions du RPD incluent ce qui suit :

- Être la personne de contact pour tout ce qui touche à la confidentialité
- Collaborer à l'élaboration des politiques de protection des données
- Collaborer à l'élaboration de tous les documents pertinents relatifs à la confidentialité
- Implémenter le règlement sur la protection des données
- Coordonner les domaines protection des données et sécurité des données
- Implémenter les mesures techniques et organisationnelles
- Enquêter sur les événements touchant la confidentialité, le cas échéant

5.2 Exigences

Une qualification appropriée est requise respectivement pour le CPD et le RPD (par ex. délégué à la protection des données). Un bon savoir-faire des processus de MIC est nécessaire en plus d'une qualification spécifique adaptée en matière de protection des données. Le CPD et le RPD doivent se charger de préserver les connaissances requises en coopération avec l'équipe de la MIC academy. Le management de MIC procure les ressources nécessaires en conséquence.

5.3 Reporting

Les rapports concernant l'organisation de la protection des données sont transmis directement au management, selon les besoins ou deux fois par an. De tels rapports doivent inclure tous les incidents, les requêtes ou les modifications relevant de la protection des données.

Il faut clarifier le fait que le CPD et le RPD ne reçoivent aucun ordre quant à l'exercice de leurs tâches. Ils ne seront pas démis ou pénalisés pour l'exécution de leurs tâches.

5.4 Réunions portant sur le RGPD

Le coordinateur de la protection des données et le responsable de la protection des données se réuniront deux fois par an. Les sujets suivants devraient être à l'ordre du jour de ces réunions.

- Discuter les événements passés concernant la protection des données (droit à l'accès, droit à la rectification, ...) quand MIC est le responsable du traitement.
- Discuter les événements passés concernant la protection des données (droit à l'accès, droit à la rectification, ...) quand MIC est le sous-traitant.
- Mettre à jour le présent document et tous les autres documents pertinents relatifs au RGPD si nécessaire.
- Vérifier l'existence éventuelle de toute infraction contre les politiques définies dans le présent document ou dans d'autres documents.

6 Droits de la personne concernée

6.1 Principes généraux

Les informations et communications relatives aux droits des personnes concernées seront traitées et sécurisées de manière appropriée ; par conséquent, elles seront fournies sous une forme concise, transparente, compréhensible et facilement accessible, en utilisant un langage clair et simple.

Les informations seront fournies par voie électronique, à condition que cela soit possible et raisonnable pour la personne concernée ou, sinon, par d'autres voies. La personne concernée a le droit de demander à obtenir les informations verbalement. Quand la personne concernée effectue la demande par voie électronique, les informations sont habituellement fournies par voie électronique.

À moins que l'identité de la personne concernée soit connue de MIC, MIC vérifiera l'identité en observant des normes strictes ; la personne exerçant un tel droit présentera un moyen d'identification (y compris, mais sans s'y limiter, un document d'identité officiel avec photo) pour prouver qu'elle peut légitimement exercer ce droit. En cas d'impossibilité de vérifier clairement l'identité, la personne concernée/le demandeur ne fournira pas de données et informations ; le demandeur sera prié de soumettre une identification appropriée.

L'exercice et le traitement d'un droit de la personne concernée seront documentés, en particulier concernant

- le droit exercé et le moment,
- les données fournies et le moment, et
- le mode de vérification de l'identité et/ou l'impossibilité éventuelle et le motif.

De plus, toute prolongation du délai sera documentée. De tels documents seront conservés en sécurité sous une forme appropriée et protégés contre tout accès de tiers non autorisé pendant une période de 3 ans.

Les droits de la personne concernée seront satisfaits dans les meilleurs délais, mais au plus tard dans le délai d'un mois ; dans des cas spéciaux (complexité particulière et/ou nombre de droits de la personne concernée), la date limite peut être reportée de deux mois. Dans ce cas, la personne concernée sera informée du report de la date limite sous une forme appropriée avant l'expiration de la date limite d'un mois.

Quand la demande d'exercice des droits de la personne concernée n'est pas satisfaite ou ne l'est pas entièrement, la personne concernée sera informée de la possibilité d'engager une réclamation auprès de l'autorité chargée de la protection des données ou d'intenter une action en justice.

Quand les droits de la personne concernée sont exercés raisonnablement, les requêtes seront satisfaites gratuitement ; cela ne sera pas le cas pour les requêtes excessives ou de toute évidence injustifiées. Dans ces cas-là, une requête peut être satisfaite moyennant le paiement des coûts occasionnés effectivement ou la requête peut être rejetée.

Il est interdit de restreindre les droits de la personne concernée, par exemple, en dictant des canaux de communication spécifiques pour le droit d'accès.

Le transfert d'informations par e-mail est permis, à condition que la confidentialité des données transmises soit garantie ; ceci s'applique notamment aux catégories spéciales de données à caractère personnel selon l'article 9 du RGPD (par ex. « Bürgerpostfach » (boîte aux lettres citoyenne), « lettre électronique »).

Si la personne concernée souhaite exercer son droit à la rectification ou à l'effacement ou à la limitation du traitement des données à caractère personnel, MIC informera tous les destinataires auxquels les données à caractère personnel étaient divulguées, sauf si ceci s'avère impossible ou implique un effort disproportionné.

En général, la personne concernée doit aussi coopérer dans une mesure appropriée et raisonnable à l'exercice de son droit de personne concernée (« obligation de coopérer).

6.2 Informations à fournir sur les données à caractère personnel, art. 13 f) du RGPD

Contrairement au droit à l'information qui doit être satisfait à la demande de la personne concernée, MIC doit fournir automatiquement des informations spécifiques à la personne concernée sauf si

- la personne concernée détient déjà les informations ou
- le stockage ou la divulgation des données à caractère personnel est régi(e) expressément par la législation ou
- la fourniture d'informations à la personne concernée est impossible ou impliquerait un effort disproportionné, notamment dans le cas du traitement à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

Les informations rendues accessibles aux personnes concernées soit au cas par cas soit sous forme d'une « politique de protection des données » générale (articles 13 et 14 du RGPD).

Compte tenu de la bonne disponibilité de l'accès internet, on peut donc supposer que l'obligation de fournir des informations aux personnes concernées peut aussi être remplie par le biais de politiques de confidentialité sur le site web du responsable du traitement, à condition que de telles politiques soient faciles à trouver (voir aussi WP260, 2016/679).

Quand les données à caractère personnel sont collectées auprès de la personne concernée, celle-ci devra obtenir toutes les informations suivantes lors de l'obtention des données à caractère personnel :

a) L'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement ;

b) Les buts du traitement et la base légale du traitement ;

c) Quand le processus repose sur des intérêts légitimes, les intérêts légitimes concrets poursuivis ;

d) Les destinataires ou catégories de destinataires des données à caractère personnel, si applicable.

De plus, les informations supplémentaires suivantes seront fournies pour garantir **l'équité et la transparence** du processus :

e) la période pendant laquelle les données à caractère personnel seront conservées ou, si ce n'est pas possible, les critères utilisés pour déterminer cette période ;

f) l'existence du droit de demander au responsable du traitement l'accès et la rectification ou l'effacement des données à caractère personnel ou la limitation du traitement ou de s'opposer au traitement, ainsi que le droit à la portabilité des données ;

g) quand le processus est basé sur le consentement, l'existence d'un droit de révoquer le consentement à tout moment, sans affecter la légalité du traitement basé sur le consentement jusqu'à la révocation.

h) le droit d'engager une réclamation auprès d'une autorité de contrôle ;

i) savoir si la fourniture des données à caractère personnel est une exigence statutaire ou contractuelle ou une exigence nécessaire pour une prise de contact et savoir si la personne concernée est obligée de fournir les données à caractère personnel et les conséquences éventuelles d'un manquement à fournir ces données.

Quand les données à caractère personnel n'ont pas été obtenues auprès de la personne concernée, la personne concernée devra obtenir les informations suivantes au plus tard dans le délai d'un mois ou, en cas de communication ou de divulgation plus tôt à des tiers, en plus des informations mentionnées ci-dessus :

a) Les catégories de données à caractère personnel concernées ;

b) La source d'origine des données à caractère personnel et, le cas échéant, s'il s'agit de sources accessibles publiquement.

L'obligation d'informer peut ne pas s'appliquer quand le stockage ou la divulgation des données à caractère personnel est régie expressément par la législation.

6.3 Droit d'accès par la personne concernée, art. 15 du RGPD

La personne concernée a le droit d'obtenir la confirmation de l'éventuel traitement de données à caractère personnel la concernant et, si tel est le cas, d'accéder à sa demande aux informations spécifiques selon l'art. 15 du RGPD ; il est possible d'utiliser les informations provenant de l'enregistrement des opérations de traitement.

Le droit au renseignement est un droit à deux niveaux :

a) le droit au renseignement sur le stockage éventuel des données à caractère personnel (« informations négatives ») ;

b) dans le cas d'« informations positives », les informations spécifiées ci-dessus seront fournies.

MIC fournit gratuitement une copie des données à caractère personnel faisant l'objet du traitement. MIC facturera des frais raisonnables basés sur les coûts administratifs pour toute copie supplémentaire demandée par la personne concernée. Quand la personne concernée effectue sa demande par voie électronique, la copie des informations sera fournie sous une forme électronique utilisée couramment, sauf si la personne concernée demande de renseignement sous une forme spéciale mais raisonnable.

Lors de la fourniture des informations, il faudra distinguer entre les informations relatives à des données à caractère personnel et l'accès à des documents contenant des données à caractère personnel ; s'il s'agit de ces dernières informations, le RGPD ne donne aucun droit d'accès/droit au renseignement. Par souci d'exhaustivité, il faudrait souligner à cet égard qu'un droit d'inspection des dossiers comme spécifié par le paragraphe 17 de la loi générale sur la procédure administrative (General Administrative Procedure Act AVG), indépendamment du droit d'accès en vertu du RGPD, est en place dans le secteur public.

Il sera également communiqué si le traitement concerne des catégories spéciales de données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que si le traitement concerne des données génétiques et 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 (art 9 RGPD).

De plus, des informations seront fournies sur des informations permettant directement ou indirectement d'identifier des personnes physiques en référant à un identifiant.

Pour permettre à la personne concernée de vérifier que ses données traitées sont exactes, MIC est aussi obligé de fournir le contenu concret des données à caractère personnel, c'est-à-dire d'indiquer par exemple le prénom ou le nom faisant spécifiquement et effectivement l'objet du traitement.

En vertu de l'article 15 paragraphe 3 du RGPD, MIC fournira donc une copie des données à caractère personnel de la personne concernée, c'est-à-dire non seulement la catégorie de données, mais également les données à caractère personnel concrètes.

Quand le traitement en cours porte sur un grand nombre de données de la personne concernée, la personne concernée a l'obligation de spécifier. La personne concernée a le devoir de coopérer !

6.3.1 Comment traiter les demandes relatives au droit au renseignement

La personne concernée doit être informée **dans le délai d'un mois** (cette période peut être prolongée de deux mois), sur le traitement assisté par ordinateur ou le traitement dans des systèmes de dépôt de version papier affectant la personne concernée ; la procédure pour exercer le droit au renseignement est décrit ci-dessous ; **chaque étape ci-dessous sera enregistrée durablement en termes de temps et d'activité et conservée pendant trois ans** :

(1) Date de réception de la demande d'information et de confirmation de la réception

(2) Vérification de l'identité du candidat - une copie du document d'identité officiel avec photo doit être soumis, sauf si MIC connaît le candidat.

(3) Demande d'une adresse électronique à laquelle les informations doivent être envoyées ou tout autre moyen de livraison requis par la personne concernée

(4) **Informations négatives** signifie qu'aucune donnée n'est traitée, ou les informations suivantes (**informations positives**) à l'adresse électronique divulguées sous un format électronique courant ou un autre moyen requis spécifiquement :

a. Les buts du traitement

b. Les données à caractère personnel soumises au traitement et/ou des catégories spéciales de données

c. Les destinataires ou catégories de destinataires des données à caractère personnel

d. les destinataires dans des pays tiers ou organisations internationales

e. Si possible, la période de traitement envisagée ou les critères utilisés pour déterminer cette période

f. Les informations sur la source des données à caractère personnel, quand les données n'ont pas été collectées auprès de la personne concernée ;

g. L'existence d'une prise de décision automatisée, incluant le profilage et, dans ces cas, des informations pertinentes sur la logique impliquée, ainsi que la signification et les conséquences envisagées d'un tel traitement pour la personne concernée

(5) La communication générale suivante :

« Vous avez le droit de demander la rectification ou l'effacement ou la limitation du traitement de vos données à caractère personnel ou de vous opposer à un traitement exécuté à des fins spécifiques.

Vous avez le droit d'engager une réclamation auprès de l'autorité chargée de la protection des données sur le fait, d'après votre avis, d'être traité de manière illicite en vous référant à la protection de vos données à caractère personnel ; ceci s'applique en particulier si vous avez le sentiment d'être désavantagé en lien avec l'exercice du droit au renseignement.

Vous avez le droit de recevoir, une fois par an, une copie gratuite de vos données à caractère personnel faisant l'objet d'un traitement. Nous facturerons des frais raisonnables basés sur les coûts administratifs pour toute copie supplémentaire.

(6) Quand les informations ne sont pas fournies, la personne concernée sera informée dans les meilleurs délais de la non-fourniture ou de la restriction des données et le pourquoi, par exemple, la preuve d'identité inappropriée, la mauvaise utilisation du droit au renseignement.

6.4 Rectification, art. 16 du RGPD

La personne concernée a le droit de demander de

▪ rectifier ou

▪ compléter

promptement (c'est-à-dire dans les meilleurs délais) des données à caractère personnel inexactes ou incomplètes la concernant. Cette règle inclut donc non seulement le fait de rectifier, mais également de compléter des données incomplètes.

Il faut aussi garder la rectification des données à l'esprit au sens du principe de l'« exactitude des données » selon l'article 5, paragraphe 1, point d) du RGPD. Par conséquent, MIC garantit que les données sont exactes à tout moment et, le cas échéant, les actualise.

6.4.1 Comment traiter les demandes de rectification

Une demande de rectification sera traitée dans les meilleurs délais ; chacune des étapes ci-dessous sera enregistrée durablement en termes de temps et d'activité et conservée pendant trois ans :

(1) Date de réception de la demande d'information

(2) Vérification de l'identité du candidat - en demandant une copie d'un document d'identité officiel avec photo, sauf si MIC connaît le candidat

(3) Demande d'un document officiel justifiant que l'enregistrement à rectifier est inexact

(4) Demande d'une adresse électronique ou d'une autre adresse à laquelle les informations sur l'achèvement/le refus devront être envoyées

(5) Notification que la rectification a été achevée ou qu'elle n'a pas été exécutée et pourquoi

6.5 Effacement, art. 17 du RGPD

La personne concernée a le droit d'obtenir de MIC dans les meilleurs délais l'effacement de données à caractère personnel la concernant quand il n'y a plus de base légale à la poursuite du traitement (y compris, mais sans s'y limiter, contrat, intérêt légitime, obligation légale/statutaire).

Quand MIC a rendu les données publiques, MIC, en tenant compte de la technologie disponible et des coûts de mise en œuvre, prendra les mesures raisonnables, y compris techniques, pour informer d'autres sous-traitants que la personne concernée a demandé l'effacement de tout lien vers ces données à caractère personnel ou toute copie ou reproduction de celles-ci.

Le droit à l'effacement ne s'appliquera pas aux opérations de traitement nécessaires à l'exercice du droit de la liberté d'expression ou à la conformité avec une obligation légale ou à l'exécution d'une tâche accomplie dans l'intérêt public ou à la constatation, à l'exercice ou à la défense de droits en justice.

L'effacement ne signifiera pas obligatoirement une suppression physique, mais inclura également une suppression logique. Selon une jurisprudence constante, la cour suprême de justice OGH demande l'effacement physique de toute façon quand les données sont/ont été collectées/traitées de manière illicite.

Dans la plupart des cas une « demande d'effacement » par la personne concernée devrait être comprise/interprétée comme un changement de but car certains autres motifs de justification du traitement (y compris, mais sans s'y limiter, l'intérêt public, des intérêts légitimes du sous-traitant/tiers ou des obligations légales) continuent d'exister. Dans ces cas, l'effacement physique des données sera impossible ; l'autorisation d'accès aux données sera plutôt adaptée au changement de but (« suppression logique »).

6.5.1 Comment traiter les demandes d'effacement

Une demande d'effacement sera traitée dans les meilleurs délais ; chacune des étapes ci-dessous sera enregistrée durablement en termes de temps et d'activité et conservée pendant trois ans :

(1) Date de réception de la demande d'information

(2) Vérification de l'identité du candidat - en demandant une copie d'un document d'identité officiel avec photo, sauf si MIC connaît le candidat

(3) Demande d'une adresse électronique ou d'une autre adresse à laquelle les informations sur le complément/le refus devront être envoyées

(4) Vérification de la demande d'effacement concernant ce qui suit :

a. **Données collectées et traitées légalement :**

   Dans ce cas, les buts du traitement sont en fait modifiés :

   Exemple : Licenciement d'un employé => retrait de la base de données active, c.-à-d. que les données seront marquées techniquement « supprimées », mais continueront d'être conservées dans la mesure nécessaire à d'autres fins prévues par la loi (par ex. délivrance d'un témoignage, périodes de garantie) ; changement du concept d'autorisation.

b. **Données collectées et traitées de manière illicite :**

   i. Les données doivent être « supprimées physiquement ».

   ii. Cette suppression physique sera aussi implémentée dans les sauvegardes : Les demandes d'effacement ne seront pas implémentées immédiatement dans les sauvegardes, mais dès que possible d'un point de vue économique et technique ; jusqu'à ce moment, l'effacement logique est possible dans les sauvegardes (accès restreint) (article 4, paragraphe 2 de la loi sur la protection des données DSG). Il faut garantir toutefois que les données devant être supprimées physiquement ne soient pas réintégrées (activées) dans le système actuel si la sauvegarde est rechargée.

(5) La **demande d'effacement ne sera pas acceptée notamment** si les données sont requises pour

a. la conformité avec une obligation légale ou

b. l'exécution d'une tâche à accomplir dans l'intérêt public ou

c. l'exercice d'une autorité officielle ou

d. des raisons étant dans l'intérêt public dans le domaine de la santé publique ou à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

(6) Communication à la personne concernée de l'acceptation ou non de la demande d'effacement ; les motifs du refus doivent être fournis si la demande est refusée.

6.6 Droit à la limitation du traitement, art. 18 du RGPD

La personne concernée aura le droit d'obtenir la limitation du traitement dans l'un des cas suivants :

a) L'exactitude des données à caractère personnel de la personne concernée est contestée,

b) Le traitement est illicite et la personne concernée requiert la limitation de l'utilisation des données,

c) MIC n'a plus besoin des données à caractère personnel aux fins du traitement, mais celles-ci sont requises par la personne concernée pour la constatation, l'exercice ou la défense de droits en justice, ou

d) La personne concernée s'est opposée au traitement et il n'a pas encore été confirmé si les raisons légitimes de MIC prévalent sur celles de la personne concernée.

Quand le traitement est limité, ces données à caractère personnel ne seront traitées, à l'exception du stockage, qu'avec le consentement de la personne concernée ou pour la constatation, l'exercice ou la défense de droits en justice. La personne concernée sera informée avant la levée de la limitation du traitement. D'autres destinataires seront informés de la limitation du traitement.

6.7 Droit à la portabilité des données, art. 20 du RGPD

La personne concernée aura le droit de recevoir les données à caractère personnel la concernant, qu'elle a fournies à MIC, dans un format structuré, utilisé couramment et lisible par machine ou de demander à MIC de transmettre ces données à un autre responsable du traitement, à condition que

a) le traitement soit basé sur un consentement ou un contrat, et

b) le traitement soit exécuté par des moyens automatisés.

Le droit à la portabilité des données ne s'appliquera donc pas vis-à-vis de responsables du traitement traitant les données à caractère personnel pour exécuter des tâches à accomplir dans l'intérêt public. Ceci ne s'appliquera pas non plus quand le traitement des données à caractère personnel est nécessaire à la conformité avec une obligation légale à laquelle MIC est soumis ou pour exécuter une tâche à accomplir dans l'intérêt public attribuée à MIC ou dans l'exercice d'une autorité officielle dont MIC est investi.

6.8 Droit d'opposition/prise de décision individuelle automatisée, art. 21 f) du RGPD

La personne concernée aura le droit de s'opposer à tout moment, pour des motifs spéciaux, au traitement des données à caractère personnel sur la base d'un intérêt légitime ou dans l'exercice d'une autorité publique, y compris au profilage basé sur ces dispositions.

Le traitement sera arrêté, à moins que MIC ne démontre des motifs légitimes sérieux d'effectuer le traitement qui prévalent sur les intérêts, les droits et les libertés de la personne concernée, en particulier pour la constatation, l'exercice ou la défense de droits en justice.

Quand les données à caractère personnel sont traitées à des fins de marketing direct, la personne concernée aura le droit de s'opposer à tout moment au traitement, y compris au profilage dans la mesure où il est en lien avec ce marketing direct.

Le droit d'opposition sera porté à l'attention de la personne concernée au plus tard au moment de la première communication. Ces informations seront présentées clairement et distinctement de toute autre information.

6.9 Obligation de notification aux destinataires, art. 19 du RGPD

Il faut garantir que toute limitation du traitement ou effacement ou rectification des données est communiqué(e) à chaque destinataire des données, sauf si cela s'avère impossible ou implique des efforts disproportionnés. Il faudra documenter la portée de la notification et/ou le motif pour lequel une notification aux destinataires est impossible ou implique des efforts disproportionnés dans un cas spécifique.

La personne concernée sera informée sur les destinataires auxquels les données ont été divulguées si la personne concernée le requiert (voir enregistrement du traitement - Appendice) ; toute impossibilité sera documentée de manière appropriée.

6.10 Notification d'une violation des données à caractère personnel, art. 33 du RGPD

En cas de violation des données à caractère personnel susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, l'autorité chargée de la protection des données sera notifiée (« **Notification d'une violation des données** »). Concernant l'obligation de notification et/ou de communication telle que définie par les articles 33 et 34 du RGPD, ce qui suit s'applique (voir aussi WP250, 2016/679) :

Selon l'article 33 du RGPD, la notification d'une violation de données à caractère personnel à l'autorité chargée de la protection des données est nécessaire dans les meilleurs délais et, si possible, dans les 72 heures après en avoir pris connaissance, à moins que la violation des données à caractère personnel ne soit pas susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Le sous-traitant informera MIC dans les meilleurs délais s'il prend connaissance d'une violation de données à caractère personnel.

Dans le cas d'une notification, les informations suivantes seront fournies à l'autorité chargée de la protection des données :

a) une description de la nature de la violation de données à caractère personnel mentionnant, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;

b) le nom et les coordonnées d'un point de contact interne auprès duquel des informations supplémentaires peuvent être obtenues ;

c) une description des conséquences probables de la violation de données à caractère personnel ;

d) une description des mesures prises ou que MIC propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Selon l'article 34 du RGPD, une violation de données à caractère personnel devra être communiquée aussi à la personne concernée si la violation des données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des **personnes physiques**. La communication devra avoir lieu dans les meilleurs délais et décrire dans un langage clair et simple la nature de la violation des données à caractère personnel.

La communication ne sera pas nécessaire, si

a) MIC a implémenté des mesures techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel concernées par la violation, notamment celles qui

rendent les données à caractère personnel inaccessibles à toute personne non autorisée à y accéder, telle que le **cryptage** ou chiffrement ;

b) MIC a pris des mesures appropriées garantissant que le risque élevé pour les droits et libertés des personnes concernées auquel il est référé au paragraphe 1 violation n'est plus susceptible de se produire ; ou

c) il impliquerait des efforts disproportionnés. Dans un tel cas, il sera recouru à une communication publique ou à une mesure similaire, les personnes concernées étant informées d'une manière tout aussi efficace.

Quand une notification à la personne concernée est nécessaire, les informations mentionnées aux points b, c et d doivent être fournies.

6.10.1 Procédure de notification d'une violation des données

Selon les articles 33 et/ou 34 du RGPD, une violation de données à caractère personnel doit être notifiée dans certaines conditions à l'autorité chargée de la protection des données **au plus tard dans les 72 heures après en avoir pris connaissance** et/ou notifiée à la personne concernée **dans les meilleurs délais** après en avoir pris connaissance comme suit :

1. Dans le cas d'une violation de données à caractère personnel (par ex. à cause de la perte d'une clé USB ou de tout autre appareil de stockage ou le vol d'un ordinateur portable) **qui n'engendre pas de risque** pour les droits/libertés des personnes concernées, **aucune notification ne sera nécessaire**, c.-à-d. ni à l'autorité ni à la personne concernée. Par exemple, en cas de perte ou de vol d'appareils contenant des données à caractère personnel, mais pourvus d'une protection appropriée contre tout accès non autorisé (par ex. chiffrement ou mot de passe sécurisé).

2. Dans le cas d'une violation de données à caractère personnel (par ex. à cause de la perte d'une clé USB ou de tout autre appareil de stockage ou le vol d'un ordinateur portable) **qui n'engendre pas de risque** pour les droits/libertés des personnes concernées, **une telle violation sera notifiée à l'autorité chargée de la protection des données, mais ne sera pas communiquée aux personnes concernées (article 33 du RGPD)**. Par exemple, dans le cas où aucune protection raisonnable n'est en place contre tout accès non autorisé aux données à caractère personnel, mais les données concernées ne constituent pas une catégorie spéciale de données (article 9 du RGPD = données relatives à la santé etc.) ou des données allant au-delà de simples données du fichier maître ou des données qui sont particulièrement importantes pour une personne concernée par leur association à d'autres données accessibles.

3. Dans le cas d'une violation de données à caractère personnel (par ex. à cause de la perte d'une clé USB ou de tout autre appareil de stockage ou le vol d'un ordinateur portable) **qui engendre un risque** pour les droits/libertés des personnes concernées, **la violation sera notifiée à l'autorité chargée de la protection des données (article 33 du RGPD) et dans les meilleurs délais aux personnes concernées (article 34 du RGPD)**. Par exemple, dans le cas où aucune protection raisonnable n'est en place contre tout accès non autorisé aux catégories spéciales de données à caractère personnel (article 9 du RGPD = données relatives à la santé etc.) ou à des données allant au-delà de simples

données du fichier maître ou à des données qui sont particulièrement importantes pour une personne concernée par leur association à d'autres données accessibles (par ex. parce qu'elles pourraient être utilisées pour créer des modèles de comportement ou des profils des personnes concernées).

Les informations suivantes seront notifiées à l'autorité chargée de la protection des données au plus tard dans les 72 heures après avoir pris connaissance d'une violation s'il existe un risque pour les personnes concernées :

a) une description de la nature de la violation de données à caractère personnel mentionnant, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;

b) le nom et les coordonnées d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;

c) une description des conséquences probables de la violation de données à caractère personnel ;

d) une description des mesures prises ou que MIC propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Les informations suivantes seront notifiées à la personne concernée dans les meilleurs délais après avoir pris connaissance d'un risque élevé pour les personnes concernées :

a) le nom et les coordonnées d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;

b) une description des conséquences probables de la violation de données à caractère personnel ;

c) une description des mesures prises ou que MIC propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Les considérations menant à une notification ou à l'absence de notification à l'autorité chargée de la protection des données et/ou aux personnes concernées seront enregistrées durablement et conservées pendant au moins trois ans.

7 Évaluation de l'impact

Selon l'article 35 du RGPD, il faudra réaliser une évaluation de l'impact dans le cas où un type de traitement

- utilisant en particulier de nouvelles technologies
- et tenant compte de la nature, de la portée, du contexte et des buts du traitement
- est susceptible d'engendrer un risque élevé pour les droits et libertés de personnes physiques

Pour le moment, il n'est pas nécessaire de réaliser d'évaluation de l'impact au sein de MIC, ceci est également documenté dans notre registre du traitement des données. Si toute protection des données nécessitant une évaluation de l'impact devient pertinente, ceci sera réalisé par l'organisation de traitement des données de MIC en coopération avec notre spécialiste externe des questions relatives à la protection des données.