FABDEC LTD

REGLES DE PROTECTION DES DONNEES

Introduction

Fabdec Ltd (ci-après « Fabdec ») s'engage à protéger les droits et libertés des personnes concernées et à traiter leurs données en sécurité et à l'abri des influences externes, dans le respect de toutes les obligations légales qui nous frappent.

Nous détenons des données à caractère personnel au sujet de nos employés, clients, fournisseurs et autres personnes à des finalités commerciales diverses.

Les présentes règles définissent comment nous nous appliquons pour protéger les données à caractère personnel et assurer que nos employés connaissent les dispositions régissant l'utilisation qu'ils font des données à caractère personnel auxquels ils ont accès dans l'exécution de leur travail. Notamment, les présentes règles disposent que les employés abordent le délégué à la protection des données avant la mise en place de toute nouvelle activité de traitement importante afin d'assurer que les mesures pertinentes s'imposant éventuellement pour observer les règlements soient prises.

Définitions

Finalités commerciales	Les finalités auxquelles nous pourrions utiliser les données à caractère personnel comprennent : Finalités associées à la gestion salariale, administrative, financière, réglementaire, de paie et de développement commercial. *Les finalités commerciales comprennent :* - *Observer nos obligations découlant des lois, règlements, gouvernance sociale et bonnes pratiques* - *Collecter des informations dans le cadre d'une ins-*

	truction par une autorité compétente ou eu égard à une action ou une sollicitation légale - *Assurer que les règles internes sont observées (par exemple celles régissant l'utilisation du courrier électronique ou d'internet)* - *Exécuter le commerce, par exemple enregistrement des transactions, formation et contrôle qualité, respect de la confidentialité des informations commerciales sensibles, vérification de sûreté, vérification et analyse de solvabilité* - *Faire suite à des réclamations* - *Contrôler des références, assurer la sécurité au travail, superviser et gérer l'accès des employés aux systèmes et dispositifs, gérer leurs absences, gérer et évaluer les mêmes* - *Superviser le comportement des employés, mesures disciplinaires* - *Positionner notre commerce sur le marché* - *Améliorer le service*

Données à caractère personnel	« Données à caractère personnel » signifie toute information se rapportant à une personne physique identifiée ou identifiable (« personne concernée ») ; est réputée être une personne physique identifiable une personne physique 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 à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. *Font partie des données à caractère personnel que nous pourrions collecter, numéro de téléphone, adresse électronique, niveau de formation, coordonnées financières et salariales, informations sur certificats et diplômes, connaissances et savoir-faire, état civil, nationalité, description de poste et curriculum vitae d'une personne.*
Catégories particulières de données à caractère personnel	Sont d'une catégorie particulière de données à caractère personnel les informations sur l'origine raciale ou ethnique, opinions politiques, convictions religieuses ou semblables, appartenance (ou non-appartenance) syndicale, santé ou maladie physique ou mentale, antécédents judiciaires ou actions en la matière d'une personne ainsi que les informations génétiques et biométriques sur elle – informations relevant d'une catégorie

	spéciale dont le traitement dans le respect des présentes règles sera strictement contrôlé.
Responsable du traitement des données	« Responsable du traitement » est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement, ces finalités et moyens du traitement étant définies, quant à elles, par la loi.
Traitant des données	« Traitant » est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.
Traitement	« Traitement » signifie toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction
Autorité de contrôle	Il s'agit là de l'autorité nationale responsable de la protection des données. L'autorité de contrôle pour le cas de notre société est l'Information Commissioner's Office britannique.

Domaine d'application

Les présentes règles s'appliquent à tous nos employés, qui doivent s'être familiarisés avec elles et les observer.

Les présentes règles complètent celles que nous nous sommes données concernant l'utilisation d'internet et du courrier électronique. De temps en temps, nous pourrions compléter ou modifier ces règles, à leur tour, par d'autres règles ou principes directeurs. D'éventuelles règles modifiées ou nouvelles seront portées à l'attention des employés avant qu'elles soient adoptées.

Qui est-ce qui a la responsabilité des présentes règles ?

De par sa qualité de notre délégué à la protection des données, M. Graham Prince a la responsabilité générale de la mise en pratique quotidienne des présentes règles. Au besoin, n'hésitez pas à contacter le délégué à la protection des données concernant tout complément d'information relatif aux présentes règles.

Principes

Fabdec observe les principes de protection des données (ci-après « les principes ») présentés par le Règlement général de protection des données de l'U.E. Nous nous efforçons au plus haut degré possible de respecter ces principes dans tout ce que nous faisons. Ces principes sont les suivants :

1. Licite, loyal, transparent

La collecte des données doit être respectueuse de la loyauté, pour une finalité licite dans la loi, et nous devons dire de façon transparente comment elles seront utilisées.

2. Limité à sa finalité

Les données ne devront être collectées qu'à une finalité déterminée.

3. Minimisé

La collecte des données doit être nécessaire au regard de sa finalité et ne doit pas dépasser ce qui est adéquat.

4. Exact

Les données que nous détenons doivent être exactes et, au besoin, mises à jour.

5. Détenu temporairement

Nous n'avons pas le droit de détenir les données plus longtemps que nécessaire.

6. Intègre et responsable

Les données que nous détenons doivent être tenues en sécurité et à l'abri des influences externes.

Responsabilité et transparence

Dans toutes les utilisations des données à caractère personnel, nous devons assumer nos responsabilités et agir de façon transparente. Nous devons démontrer comment nous respectons chaque principe. Vous êtes responsable de dresser un registre écrit des activités de traitement dont vous avez la responsabilité, qui démontre comment lesdites activités sont conformes aux principes. Il sera tenu à jour et approuvé par le délégué à la protection des données.

L’observation des dispositions relatives à la protection des données dans la loi et de la responsabilité et de la transparence au titre du principe du RGPD passe par notre capacité de démontrer que nous les respectons. Vous personnellement êtes responsable de saisir ce qui vous est demandé pour que nous puissions répondre aux obligations suivantes concernant la protection des données qui sont les nôtres :

- Mise en pratique intégrale des mesures techniques et organisationnelles appropriées
- Maintien d’une documentation à jour et pertinente de toutes les activités de traitement
- Exécution d’analyses d’impact relative à la protection des données
- Mise au point de mesures susceptibles d’assurer la protection des données dès la conception et par défaut :
    - Minimisation des données
    - Pseudonymisation
    - Transparence
    - Occasion pour les personnes concernées de contrôler le traitement
    - Création et amélioration constantes des procédés de sécurité et de protection renforcée

Nos procédés

Traitement loyal et licite

En application du premier principe, nous traiterons les données à caractère personnelle de façon loyale et licite et dans le respect des droits de la personne concernée. En général, cela signifie que nous ne traitons pas les données à caractère personnel à moins que la personne concernée consente à ce traitement.

S'il ne nous est pas possible de lui trouver une base licite (voir ci-après), notre traitement n'est pas conforme au premier principe, donc illicite. Les personnes concernées ont le droit de demander l'effacement de toute donnée illicitement traitée.

Responsabilité relative aux et traitement des données

Fabdec est à interpréter tant comme responsable que comme traitant des données. Il convient que nous maintenions dûment notre enregistrement comme tels auprès de l'Information Commissioner's Office, afin d'être en mesure de continuer à détenir des données de façon licite comme responsable et comme traitant.

En tant que (sous-) traitant des données, il nous faut observer nos obligations contractuelles et agir exclusivement dans le respect des instructions documentées émanant du responsable du traitement. Si, à quelque moment que ce soit, nous définissons nous-mêmes les finalités et les moyens du traitement indépendamment des instructions du responsable, nous serons réputés être responsables nous-mêmes pour autant que cela constitue une rupture de notre contrat signé avec le responsable et que nous assumions dès lors les mêmes responsabilités que le responsable du traitement. Étant (sous-) traitant, il est de notre devoir de :

- Ne pas engager de sous-traitant à nous sans l'autorisation préalable du responsable du traitement
- Coopérer sans restriction avec l'autorité de contrôle qu'est l'ICO
- Assurer la sécurité du traitement
- Tenir des registres exacts des activités de traitement
- Notifier le responsable du traitement de toute violation des données à caractère personnel

Si vous avez le moindre doute concernant nos modes de gestion des données, veuillez prendre contact avec le délégué à la protection des données.

Base licite du traitement des données

Il nous faut veiller à ce que nous ayons une base licite du traitement des données. Assurez-vous que pour toutes les données dont la gestion vous est attribuée, il existe une base licite du traitement écrite et approuvée par le délégué à la protection des données. Il est de votre responsabilité de vérifier qu'une base licite existe concernant toutes les données avec lesquelles vous travaillez, et de vous assurer que vos activités sont conformes à ce que cette base licite prévoit. Au moins une des conditions suivantes doit être remplie chaque fois que nous traitons des données à caractère personnel.

1. **Consentement**

   Nous disposons du consentement récent, clair, sans ambiguïté et déterminé de la personne concernée concernant le traitement de ses données à une finalité spécifique.

2. **Contrat**

Le traitement est nécessaire à l'exécution ou à la préparation d'un contrat signé avec la personne.

3. **Obligation légale**

   Nous sommes sous une obligation légale (autre qu'un contrat) de traiter les données.

4. **Intérêts vitaux**

Le traitement des données est nécessaire à la protection de la vie d'une personne ou dans un contexte médical.

5. **Mission publique**

Le traitement est nécessaire à l'exécution d'une mission d'intérêt public, à l'exercice de l'autorité publique ou ce dont elle est fonction trouve une base claire dans la loi.

6. **Intérêt légitime**

Le traitement est nécessaire à des finalités découlant de notre intérêt légitime. Pourtant, cette condition n'est pas acceptable s'il existe des raisons de protéger les données à caractère personnel de la personne, qui prévalent au regard de cet intérêt légitime.

Décision de la condition sur laquelle se baser

Lors de l'évaluation de l'existence, ou non, d'une base licite, il faut d'abord établir que le traitement est nécessaire. Cela signifie que le traitement constitue un mode ciblé et adéquat de réaliser la finalité formulée. Vous ne pouvez pas vous prévaloir d'une base licite si vous pouvez atteindre le même objectif raisonnablement par d'autres moyens.

Rappelez-vous que plusieurs bases pourraient convenir ; vous retiendrez la base qui convient le mieux à la finalité concrète, non pas celle qui serait la plus facile.

Prenez en considération ce qui suit et documentez les réponses que vous donnez :

- Quelle est la finalité du traitement des données ?
- Peut-on le réaliser raisonnablement d'une autre façon ?
- Existe-t-il un choix de traiter ou ne pas traiter les données ?
- Au profit de qui le traitement intervient-il ?
- La base licite retenue, est-ce que celle-ci est bien la même base licite que la personne concernée est susceptible d'avoir attendu ?
- Quel impact le traitement représente-t-il pour la personne ?
- Êtes-vous dans une position dominante par rapport à elle ?
- Est-ce qu'elle est une personne vulnérable ?
- Est-elle susceptible de s'opposer au traitement ?
- Êtes-vous capable à tout moment d'arrêter le traitement sur demande, et avez-vous retenu aussi la façon dont cela serait fait ?

Notre engagement d'observer le premier principe demande que nous documentions ce processus et démontrions que nous avons évalué les bases licites pour trouver celle qui va le mieux avec chacune des finalités dont relève le traitement, et qu'elles justifient pleinement de nos décisions en la matière.

Nous devons assurer aussi que les personnes dont les données sont traitées par nous sont informées de la base licite dudit traitement de leurs données et de la finalité prise en compte. Le moyen pour le faire sera une déclaration relative à la protection des données. Cela vaut peu importe que nous ayons collecté les données directement auprès de la personne ou d'une autre source.

S'il est de vos responsabilités d'évaluer l'existence, ou non, d'une base licite et d'exécuter les dispositions de la déclaration relative à la protection des données en ce qui est d'une activité de traitement concrète, il vous faudra le faire approuver par le délégué à la protection des données.

Catégories particulières de données à caractère personnel

Qu'est-ce que sont des catégories particulières de données ?

Appelées sensibles ou confidentielles dans le passé, les données couvertes par cette signification sont celles sur une personne qui sont plus sensibles que d'autres et méritent une protection renforcée. Ce type de données peut signifier un plus grand risque pour les droits et libertés fondamentaux de la personne, par exemple en l'exposant à une discrimination illégale. Font partie des catégories spéciales les données sur une personne concernant sa :

- Race
- Origine ethnique
- Conviction politique
- Religion
- Appartenance syndicale
- Information génétique
- Biométrie (telle qu'utilisée sur la carte d'identité)
- Santé
- Orientation sexuelle

Dans la plupart des cas où nous traitons des données à caractère personnel relevant d'une catégorie particulière, il nous faut le consentement *exprès* audit traitement de la personne concernée, à moins que des circonstances exceptionnelles se présentent ou que nous soyons obligés à le faire par la loi (par exemple afin de respecter notre obligation d'assurer la sécurité au lieu de travail). Dans le cas du consentement, seront identifiés clairement quelles sont les données sur lesquelles il porte, pourquoi elles sont traitées et à qui elles seront communiquées.

La condition qui est à l'origine du traitement des données à caractère personnel relevant des catégories particulières doit avoir une base juridique. Si la base licite du traitement des données relevant d'une catégorie particulière nous fait défaut, l'activité de traitement concernée doit être terminée.

Responsabilités

Nos responsabilités

- Évaluer et documenter le type de données à caractère personnel détenues
- Examiner les procédés afin d'assurer qu'ils donnent tous ses droits à la personne
- Identifier la base licite du traitement des données
- Assurer que les procédés concernant le consentement sont licites
- Mettre en pratique et contrôler des procédés susceptibles de permettre de détecter, remonter et examiner les violations des données à caractère personnel
- Conserver les données en sécurité et à l'abri des influences externes
- Évaluer les risques auxquels les droits et libertés de la personne seraient éventuellement exposé si des données se trouvaient compromises

Vos responsabilités personnelles

- Avoir une vision globale de vos obligations en matière de protection des données
- Vérifier que toutes les activités de traitement des données auxquelles vous avez affaire, sont conformes à nos règles et justifiées
- N'utiliser aucune donnée d'une façon illicite
- Ne pas conserver les données de façon incorrecte, ne pas être négligent à leur égard ni provoquer d'une autre manière une violation par nous-mêmes des lois relatives à la protection des données ou de nos règles, due à une activité de votre part
- Respecter les présentes règles à tout moment
- Sans tarder soulever toutes les questions, notifier de toute violation ou erreur, et remonter tout ce qui serait suspect ou à l'encontre des présentes règles et de nos obligations légales

Responsabilités du délégué à la protection des données

- Tenir informée la direction en ce qui est des responsabilités, risques et questions associés à la protection des données
- Surveiller régulièrement les procédés et les règles de protection des données
- Organiser les formations et initiations à la protection des données pour tous les employés et les personnes citées dans les présentes règles
- Répondre aux questions concernant la protection des données posées par les employés, la direction, d'autres intéressés

- Faire suite aux demandes émanant des personnes telles que nos clients et fournisseurs, de savoir quelles données nous détenons sur elles
- Contrôler et approuver les contrats et accords sur la protection des données signés avec des tiers gérant les données de la société

Responsabilités du responsable NTIC

- Assurer que tous les systèmes, services, logiciels et matériels sont conformes aux standards de sécurité adéquats
- Contrôler et mettre à l'essai régulièrement les matériels et logiciels devant assurer la sécurité afin de s'assurer qu'ils fonctionnent comme prévu
- Analyser des services tiers, par exemple les services dits en nuage, que la société se propose d'utiliser pour la conservation et le traitement des données

Responsabilités du responsable commercial

- Approuver les déclarations relatives à la protection des données insérées dans les courriels et se trouvant dans d'autres supports commerciaux
- Faire suite à des demandes en matière de protection des données en provenance des clients, groupes cibles ou rédactions de presse
- Se coordonner avec le délégué à la protection des données pour que toutes les actions commerciales soient conformes aux lois relatives à la protection des données et aux règles de protection des données de la société

Exactitude et pertinence

Nous assurerons que toutes les données à caractère personnel que nous traitons sont exactes, adéquates, pertinentes et limitées à ce qui est nécessaire au regard de la finalité à laquelle elles ont été collectées. Nous ne traiterons pas des données collectées à une finalité, dans le but d'une autre finalité non associée à celle-là, à moins que la personne concernée y ait consenti ou puisse raisonnablement l'attendre pour une autre raison.

Des personnes ont le droit de nous demander la rectification des données à caractère personnel les concernant qui seraient inexactes. Si vous pensez que des informations sont inexactes, notez le fait que l'exactitude de l'information se trouve mise en question et notifiez-en le délégué à la protection des données.

Sécurité des données

Vous devez garder les données à caractère personnel à l'abri de la perte et de l'abus. Pour autant que d'autres sociétés traitent des données à caractère personnel à notre demande, fournissant un service, le délégué à la protection des données détermine les dispositions supplémentaires, spécifiques en matière de sécurité des données à ajouter éventuellement aux contrats signés avec ces sociétés tierces.

Conservation des données en sécurité

- Au cas où des données sont conservées au format imprimé sur papier, elles seront gardées dans un local à l'abri de l'accès des employés non autorisés.
- Les données imprimées seront détruites lorsqu'elles ne sont plus nécessaires.
- Les données conservées sur des ordinateurs seront protégées par des mots de passe forts changés régulièrement. Nous encourageons tous les employés de faire créer et gérer les mots de passe à un gestionnaire de mots de passe.
- Les données conservées sur cédérom ou clé de mémoire seront cryptées ou protégées par mot de passe, puis le support mis sous clé à l'abri de l'accès non autorisé chaque fois qu'il n'est pas en cours d'utilisation.
- Toute conservation dite en nuage sera approuvée par le délégué à la protection des données
- Des serveurs avec des données à caractère personnel seront mis en place dans un local à l'abri et hors de la zone générale des bureaux.
- Les données seront sauvegardées régulièrement dans le respect des principes directeurs de sauvegarde de la société.
- Les données ne seront jamais enregistrées directement sur un appareil mobile, par exemple ordinateur portable, tablette, téléphone intelligent.
- Tous les serveurs avec des données sensibles/particulières seront approuvés et protégés au moyen des logiciels de sécurité.
- Toutes les mesures techniques possibles doivent être prises pour mettre les données à l'abri de la violation.

Conservation des données dans la durée

Nous ne conserverons pas les données à caractère personnel plus longtemps qu'il est nécessaire de le faire. Que ce soit nécessaire ou non, dépend des circonstances individuelles, prenant en compte la finalité à laquelle les données ont été collectées, et sera déterminé d'une façon qui soit respectueuse de nos règles en la matière.

Transmission internationale des données

La transmission internationale des donnés à caractère personnel est soumise à des restrictions. Sans la permission expresse du délégué à la protection des données, vous ne transmettrez des données ni à l'étranger ni d'une autre façon non conforme aux règles et procédés normaux.

Droits des personnes concernées

Concernant leurs données, les personnes ont des droits que nous respecterons et observerons au maximum de nos facultés. Nous ferons en sorte que les personnes puissent exercer leurs droits comme suit :

1. Droit de se faire informer

- Présentation de déclarations relatives à la protection des données qui sont concises, transparentes, compréhensibles et facilement accessibles ainsi que gratuites, lesquelles sont rédigées avec des termes clairs et simples, en particulier si elles sont destinées à des enfants
- Documentations montrant comment nous utilisons les données à caractère personnel, afin de démontrer la conformité aux obligations de responsabilité et de transparence

2. Droit d'accès

- Occasion pour les personnes d'avoir accès à leurs données à caractère personnel et à des informations supplémentaires
- Possibilité pour les personnes d'avoir connaissance de la licéité des activités de traitement et de la vérifier

3. Droit de rectification

- Obligation pour nous de rectifier ou compléter les données à caractère personnel d'une personne sur demande, si inexactes ou incomplètes
- À réaliser sans tarder, sous un mois maximum ; possibilité d'une prorogation à deux mois avec permission du délégué à la protection des données

4. Droit à l'effacement

- Obligation pour nous d'effacer ou retirer les données d'une personne sur demande à moins d'une raison contraignante légitimant à continuer le traitement

5. Droit à la limitation du traitement

- Obligation pour nous de faire suite à une demande de limiter, bloquer ou annuler d'une autre façon le traitement des données à caractère personnel
- Permission à nous de conserver les données à caractère personnel dont le traitement a été limité, mais non de continuer à les traiter ; obligation pour nous de conserver assez de données dans la durée pour être en mesure d'assurer que le droit à la limitation sera observé aussi à l'avenir

6. Droit à la portabilité des données

- Obligation pour nous de restituer leurs données à des personnes pour leur permettre de les réutiliser à leurs propres finalités et à travers plusieurs services
- Obligation pour nous de les restituer à un format couramment utilisé, lisible par machine et de les envoyer sur demande à un autre responsable du traitement

7. Droit d'opposition

- Obligation pour nous de respecter le droit d'une personne de s'opposer au traitement des données dans son intérêt légitime ou dans le cadre de l'exécution d'une mission d'intérêt public
- Obligation pour nous de respecter le droit d'une personne de s'opposer à la prospection directe, y compris le profilage.
- Obligation pour nous de respecter le droit d'une personne de s'opposer au traitement de leurs données dans le cadre de la recherche et statistique scientifique et historique

8. Droits dans le domaine des décisions automatisées et du profilage

- Obligation pour nous de respecter les droits qu'ont les personnes dans le domaine des décisions automatisées et du profilage
- Conservation par et chez la personne de son droit de s'opposer au traitement automatisé visé, de demander que son fondement lui soit expliqué et d'exiger une intervention humaine

Déclarations relatives à la protection des données

Nécessités de préparer une telle déclaration

Une déclaration relative à la protection des données doit être mise à disposition au moment où des données sont demandées directement à la personne concernée. Si les données ne sont pas acquises depuis la personne concernée, la déclaration doit lui être fournie sous un délai raisonnable à compter de l'obtention des données, ce qui signifie sous un mois.

Si les données sont utilisées pour communiquer avec la personne, la déclaration relative à la protection des données doit être fournie lorsque la première communication intervient.

Si la communication à un destinataire tiers est envisagée, la déclaration relative à la protection des données doit être fournie avant la communication des données.

Contenu d'une déclaration relative à la protection des données

Une déclaration relative à la protection des données doit être concise, transparente, compréhensible et facilement accessible. Elle sera fournie gratuitement et sera écrite avec des termes clairs et simples, en particulier lorsqu'elle est destinée à des enfants.

Les informations suivantes doivent être contenues dans une déclaration relative à la protection des données à l'intention de toutes les personnes concernées :

- Identification et coordonnées de contact du responsable du traitement et de son délégué à la protection des données
- Finalité du traitement et base licite de sa réalisation
- Intérêt légitime du responsable du traitement et, au besoin, des tiers
- Précision, au besoin, du droit de retrait à tout moment du consentement
- Catégorie des données à caractère personnel (seulement données non collectées directement auprès de la personne concernée)
- D'éventuels destinataires ou catégories de destinataires des données à caractère personnel

- Détails sur les éventuelles transmissions vers des pays tiers et les mesures de sécurité prises
- Période de conservation dans la durée ou critères définissant cette période, y compris informations sur la destruction des données après cette période
- Précision du droit de soumettre des réclamations à l'ICO et des procédés internes de gestion des réclamations
- Source des données à caractère personnel, précisant s'il s'agit d'une source publiquement disponible (seulement données non acquises directement auprès de la personne concernée)
- Précision d'éventuelles décisions automatisées, y compris profilage, et informations sur les manières dont les décisions sont prises et la signification et les conséquences qu'elles ont pour la personne concernée
- Précision disant si les données à caractère personnel sont mises à disposition dans le cadre d'une nécessité ou obligation réglementaire ou contractuelle et quelles sont les conséquences possibles de ne pas les mettre à disposition (seulement données non acquises directement auprès de la personne concernée)

Demande d'accès par la personne concernée

Qu'est-ce qu'une demande d'accès par la personne concernée ?

Toute personne a le droit de se faire confirmer que ses données sont traitées et d'accéder aux données à caractère personnel et informations connexes, ce qui vise les informations à fournir dans une déclaration relative à la protection des données.

Notre protocole pour faire suite aux demandes d'accès

Nous devons fournir gratuitement à la personne une copie des informations qu'elle a demandées. Cela doit se faire sans tarder, sous un mois maximum à compter de la réception. Nous nous appliquons pour donner aux personnes concernées l'accès à leurs informations utilisant un format électronique couramment utilisé et, si possible, fournir l'accès direct et à distance aux informations par un système sécurisé.

S'il est complexe ou lourd de faire suite à la demande, la date limite peut être prorogée de deux mois, mais la personne doit être informée sous un mois. Vous devez vous faire approuver la prorogation de la date limite par le délégué à la protection des données.

À certaines demandes, nous pouvons refuser de faire suite ou, dans les cas où la demande serait manifestement infondée ou excessive, facturer des frais de traitement. Si la demande porte sur une grande quantité de données, nous pouvons prier la personne de préciser les informations concrètes qu'elle demande. Cela ne peut se faire qu'avec l'autorisation expresse du délégué à la protection des données.

Du moment où une demande d'accès a été faite par une personne concernée, vous ne devez ni modifier ni compléter les données sur lesquelles la demande porte. Cela constituerait un délit passible d'une peine.

Demande de portabilité de données

Nous devons restituer les données demandées à un format structuré, couramment utilisé et lisible par machine. C'est en général un fichier CSV, étant entendu que d'autres formats sont acceptables. Nous devons fournir ces données soit à la personne les ayant demandées, soit à un responsable du traitement à qui elle nous demande de les envoyer. Cela doit intervenir gratuitement et dans les meilleurs délais, sous un mois maximum. Une prorogation à deux mois est possible en cas de demande complexe ou lourde, mais la personne sera informée de la prorogation sous un mois, et il vous faut la permission expresse de la part du délégué à la protection des données.

Droit à l'effacement

Qu'est-ce que le droit à l'effacement ?

Les personnes ont le droit de demander l'effacement de leurs données et la fin de leur traitement dans les circonstances suivantes :

- Les données à caractère personnel ne sont plus nécessaire au regard de la finalité à laquelle elles ont été collectée et/ou traitées au départ
- Le consentement est retiré.
- La personne s'oppose au traitement et il n'existe pas d'intérêt légitime prévalant qui demanderait de continuer à les traiter.
- Les données à caractère personnel ont été traitées illicitement ou des lois relatives à la protection des données ont été violées d'une autre manière.
- Une obligation légale le demande.
- Le traitement se rapporte à un enfant.

Notre protocole pour respecter le droit à l'effacement

Nous ne saurions refuser de donner suite au droit à l'effacement que dans les circonstances suivantes :

- Exercice du droit à la liberté d'expression et d'information
- Respect d'une obligation légale relative à l'exécution d'une mission d'intérêt public ou exercice de l'autorité publique
- À une finalité d'intérêt public relevant de la santé publique
- À une finalité d'archivage d'intérêt public, de recherche scientifique, de recherche historique ou à des fins statistiques
- À l'exercice ou à la défense de droits en justice

Dans la mesure où des données à caractère personnel devront être effacées qui ont été transmises à d'autres impliqués ou destinataires, ceux-ci seront contactés et renseignés de leur obligation d'effacer lesdites données. Si la personne pose cette question, elle sera renseignée de ces destinataires.

Droit à l'opposition

Les personnes ont le droit de s'opposer, pour des raisons tenant à leur situation particulière, à l'utilisation de leurs données. Nous ne traiterons plus ces données, à moins que :

- Nous ayons des motifs légitimes du traitement prévalant sur les intérêts, droits et libertés de la personne ;
- Le traitement se rapporte à la constatation, l'exercice ou la défense de droits en justice.

Dans tous les cas, nous renseignerons la personne de son droit à l'opposition lors de la première occasion de communication, c'est-à-dire la déclaration relative à la protection des donnés. Nous devons proposer aux personnes une possibilité en ligne de faire opposition.

Droit à la limitation des décisions automatisées et du profilage

Nous pouvons réaliser du profilage ou des décisions automatisés dont découle une conséquence légale ou un effet d'une signification similaire pour une personne, seulement dans les circonstances suivantes :

- Il est nécessaire à la conclusion ou à l'exécution d'un contrat.
- Il est fondé sur le consentement explicite.
- Il est autorisé par la loi d'une autre façon.

Dans ces circonstances, nous devons :

- Donner aux personnes des informations détaillées concernant le traitement automatisé ;
- Leur proposer des modalités simples de demander une intervention humaine ou de contester d'éventuelles décisions sur elles ;
- Réaliser des vérifications et des essais utilisateurs réguliers afin d'assurer que nos systèmes fonctionnent comme prévu.

Tiers

Coopération avec responsables de traitement et traitants tiers

En qualité de responsable du traitement ou de traitant des données, nous devons avoir signé des contrats écrits avec tous les responsables du traitement et (sous-) traitants tiers avec lesquels nous coopérons. Ce contrat doit contenir des dispositions spécifiques définissant nos et leurs responsabilités, obligations et compétences.

En qualité de responsable du traitement, nous confieront la tâche uniquement à des (sous-) traitants en mesure de présenter des garanties suffisantes, aux termes du RGPD, assurant que les droits des personnes concernées seront respectés et protégés.

En qualité de (sous-) traitant, nous agirons exclusivement dans le respect des instructions documentées émanant du responsable du traitement. Nous assumons nos responsabilités de sous-traitant aux termes du RGPD et nous respecterons et protègerons les droits des personnes concernées.

Contrats

Nos contrats doivent être conformes aux normes établies par l'ICO et, dans la mesure du possible, s'aligner sur les dispositions contractuelles standardisées qui sont disponibles. Nos contrats avec les responsables du traitement et les sous-traitants doivent définir l'objet et la durée du traitement, la nature et la finalité expresse des activités de traitement, les types de données à caractère personnel et catégories de personnes concernées et les obligations et les droits du responsable du traitement.

Au minimum, nos contrats doivent contenir des dispositions sur :

- Action seulement sur instruction écrite
- Obligation de confidentialité frappant tous ceux impliqués dans le traitement des données
- Mise en place de mesures adéquates pour assurer la sécurité du traitement
- Recrutement d'autres sous-traitants seulement avec le consentement préalable du responsable du traitement et sur la base d'un contrat écrit
- Coopération du responsable du traitement avec le sous-traitant dans la gestion des demandes d'accès par des personnes concernées et l'ouverture de l'exercice de leurs droits au titre du RGPD

- Coopération du sous-traitant avec le responsable du traitement visant à permettre à ce dernier de respecter ses obligations au titre du RGPD relatives à la sécurité du traitement, la notification des violations des données et l'exécution des analyses d'impact relative à la protection des données
- Suppression ou renvoi de toutes les données à caractère personnel au terme du contrat
- Observation d'audits et inspections réguliers et mise à disposition de toute donnée nécessaire à ce que le responsable du traitement et le sous-traitant respectent leurs obligations légales
- Engagement tant du responsable du traitement que du sous-traitant à ne rien faire qui violerait le RGPD

Données sur des délits passible d'une peine

Restitution d'une fiche pénale

Toute demande de restitution d'une fiche pénale aura une base légale. Une telle demande de restitution ne peut pas se fonder uniquement sur le consentement de la personne concernée. Nous n'avons pas le droit d'accumuler un registre complet de données sur des délits passible d'une peine. Toutes les données sur les délits passible d'une peine sont réputées relever d'une catégorie particulière de données à caractère personnel et seront traitées comme telles. Pour demander la restitution d'une fiche pénale, il vous faut l'autorisation préalable du délégué à la protection des données.

Audit, surveillance et formation

Audit de données

Des audits de données réguliers destinés à gérer et modérer les risques seront consignés dans le registre des données. Il comprend des informations concernant les données qui sont détenues, les lieux où elles sont conservées, les façons de les utiliser, les responsables et toute règle ou période de conservation dans la durée éventuellement pertinente. Vous devez mener des audits de données réguliers tels que les définissent le délégué à la protection des données et les procédés normaux.

Surveillance

Chacun observera les présentes règles. Le délégué à la protection des données est investi de la responsabilité générale en la matière. Notre société les surveillera constamment et les modifiera ou complétera au besoin. Vous notifierez le délégué à la protection des données de toute violation des présentes règles. Vous personnellement observerez les présentes règles intégralement et constamment.

Formation

Des formations adéquates au regard de vos attributions, sur les dispositions dans les lois relatives à la protection des données vous seront proposées. Vous suivrez toutes les formations telles qu'elles vous seront demandées. Si vous changez d'attribution ou de responsabilités, il est de votre responsabilité de demander une nouvelle formation concernant la protection des données adéquate au regard de vos nouvelles attributions ou responsabilités

S'il vous faut des formations supplémentaires sur des sujets relevant de la protection des données, consulter le délégué à la protection des données.

Notification de violations

Toute violation des dispositions dans les présentes règles et les lois relatives à la protection des données doit être remontée aussi rapidement que possible en pratique. Cela signifie, dès que vous avez connaissance de la violation. Une obligation légale frappe Fabdec de notifier l'Information Commissioner's Office (ICO) de toute violation des données sous 72 heures.

Tous les membres de nos effectifs sont sous l'obligation de remonter le non-respect réel ou potentiel des règles régissant la protection de données. Cela nous permet :

- L'instruction du cas de non-respect et des actions de correction au besoin
- L'établissement d'un registre des cas de non-respect
- La notification à l'ICO de tous les cas de non-respect matériels soit en tant que cas isolé, soit en tant qu'instance individuelle d'un enchaînement de cas de non-respect

À l'encontre d'un membre des effectifs qui négligerait de remonter une violation ou s'avérerait connaître ou soupçonner la présence d'une violation sans pour autant suivre le procédé correct de notification, des mesures disciplinaires seront prises.

Notifiez, s'il vous plaît, le délégué à la protection des données immédiatement d'une violation.

Non-respect

Nous prenons le respect des présentes règles très au sérieux. Le non-respect expose à des risques tant vous-même que la société.

L'importance des présentes règles se traduit par le fait que le manquement à quelque disposition que soit peut provoquer des mesures disciplinaires définies par nos règlements internes, dont un résultat possible est le licenciement.

Si vous avez des questions ou remarques concernant quoi que ce soit dans les présentes règles, n'hésitez surtout pas à consulter le délégué à la protection des données.