Politique générale de protection des données personnelles

Fédération Handicap International – Humanity & Inclusion – 2020

Sommaire

1. Objectifs et champ d'application

Les termes commençant par une majuscule utilisés dans la présente Politique générale de protection des Données personnelles (ci-après la « Politique ») sont définis dans l'Annexe « Définitions ».

1.1 Objectifs de la Politique

HI s'engage à **garantir la protection des Données personnelles** obtenues dans le cadre de son activité, ainsi qu'à se conformer aux lois et réglementations applicables en matière de Traitement de Données à caractère personnel et de Données à caractère personnel sensibles.

Cette Politique a pour objectifs de :

- **définir les engagements de HI** en relation avec les principes imposés par la Législation applicable, et notamment le Règlement européen n°2016/679 relatif à la protection des Données à caractère personnel, en date du 27 avril 2016, applicable depuis le 25 mai 2018 ;
- **définir les rôles et responsabilités** des principaux contributeurs ;
- **assurer la mise en place de méthodes et procédures adéquates** ainsi que des **structures de gouvernance et de contrôle appropriées** pour garantir le respect des engagements et de la Législation applicable.

Les engagements de HI sont résumés dans les encarts de règle **R0X**. La conformité de HI avec ces règles sera auditée dans les conditions définies à la Section « Contrôle de la conformité ».

Cette Politique est complétée par les politiques et procédures suivantes :

- le Règlement Intérieur et les Notes de services y afférentes ;
- la Procédure de gestion des failles de sécurité ;
- la Procédure de gestion des droits des personnes ;
- la Politique de conservation des données ;
- la Charte Informatique.

1.2 Champ d'application

La Politique a vocation à s'appliquer à l'ensemble des collaborateurs (salariés, stagiaires, bénévoles) de la Fédération HI et de HI France, et à l'ensemble des traitements opérés par l'association sur le territoire français.

Les salariés visés sont les salariés en contrat de travail « siège » de droit français et les salariés « personnel international » titulaires d'un contrat de travail international signé avec le siège de la Fédération en France.

En cas de conflit entre la présente Politique et la législation applicable, les règles suivantes s'appliqueront :

- Si la Politique est plus protectrice, elle a vocation à primer sur la législation applicable.
- Si la législation applicable est plus protectrice, elle s'appliquera sur les points concernés en lieu et place de la Politique.

Si un doute subsiste, HI ou l'un de ses collaborateurs sollicitera les conseils du Délégué à la Protection des Données personnelles (*Data Protection Officer* ou DPO).

1.3 Révision

Cette Politique est mise à jour par le DPO de HI en cas de :

- changements significatifs du contexte métier ou de la stratégie de protection des Données à caractère personnel de HI ;
- changements significatifs de l'exposition aux risques (par exemple, nouvelles menaces, nouvelles tendances…) ;
- évolution significative de la législation applicable.

Ces modifications sont soumises à la validation de la Direction générale et une communication adéquate sera effectuée aux collaborateurs de HI le cas échéant.

2. Organisation et gouvernance de la protection des Données personnelles

Chaque personne au sein de HI est partie prenante de la protection des Données personnelles. Cette protection doit être une préoccupation constante. Cette préoccupation se reflète dans les politiques, procédures et pratiques opérationnelles.

Les contributeurs clés identifiés dans cette section acceptent et adoptent les rôles et responsabilités qui leur incombent afin de s'assurer que cette Politique est mise en œuvre de manière cohérente et coordonnée au sein de HI.

2.1 Contributeurs clés

2.1.1 La Direction générale

La Direction générale garantit un engagement fort de HI en faveur de la protection des Données personnelles en tant qu'actif stratégique de l'entreprise. À ce titre, la Direction générale doit :

- s’assurer de la mise en place d’une gouvernance de la protection des Données personnelles appropriée, définissant les rôles et responsabilités de chacun au sein de HI et permettant au DPO d’être associé, d’une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données ;
- communiquer auprès de l’ensemble des collaborateurs sur la nomination d’un DPO, ses missions et les moyens de le contacter ;
- veiller à ce que le DPO :
    - dispose des ressources et moyens appropriés à l’exercice de ses missions ;
    - exerce ses missions de manière indépendante ;
    - reçoive la formation adaptée ;

- soit en mesure de faire directement un rapport à la Direction générale.

2.1.2 Les Directions métiers

Au sein de HI, chaque responsable d'une Direction métier est **Autorité Responsable de Traitement (ART)**, dans la mesure où il est en autorité sur la mise en œuvre d'un ou plusieurs Traitements. (Il peut déléguer cette autorité à un n-1 (manager), dans le cadre d'une délégation de pouvoir formelle.)

Missions de l'ART :

- Elle doit veiller au respect des principes et règles édictés dans la présente Politique et les procédures et politiques complémentaires.
- Elle désigne un ou plusieurs **Responsables Opérationnels de Traitement (ROT)** au sein de sa direction, lesquels sont responsables de la mise en œuvre opérationnelle des Traitement concernés.
- Pendant la période de mise en conformité, elle s'assure de la robustesse des plans d'action de mise en conformité proposés par le ou les ROT, et elle organise une revue semestrielle de ces actions avec le ou les ROT de son équipe. Dans une période stabilisée la fréquence pourra être revue.
- Elle convoque une cellule de crise, dès violation avérée de données personnelles, pour traiter les aspects curatifs et préventifs.

Le Responsable Opérationnel de Traitement (ROT), conjointement avec d'autres (notamment son ART, la DSI…), définit les finalités et met en œuvre les moyens du traitement (chaine stratégique, opérationnelle, mise en conformité et gestion de crise…). Il doit :

- associer le DPO dès la phase de conception dans tous les nouveaux projets impliquant un Traitement de Données personnelles ;
- inscrire tout nouveau Traitement dans le registre des Traitements de HI ;

- définir les durées de conservation, les processus d'anonymisation ou de suppression de la donnée et les présenter à son ART ;
- définir le plan d'action de mise en conformité et suivre sa progression avec son ART ;
- tenir à jour un registre des activités de Traitement effectuées sous sa responsabilité, tel que décrit dans le RGPD ;
- mettre en œuvre des mesures techniques et organisationnelles pour assurer la sécurisation des données personnelles ;
- répondre à l'exercice du droit des Personnes et en particulier à leurs requêtes de droit d'accès selon les directives du RGPD ;
- réaliser si nécessaire une Analyse d'impact relative à la protection des données (dite « AIPD »), avec l'assistance du DPO et de tout autre expert technique ;
- documenter et justifier par écrit les raisons pour lesquelles l'avis du DPO n'a pas été suivi le cas échéant ;
- répondre à toute demande d'information du DPO sur tous les sujets ayant un impact sur la vie privée des personnes ;
- fournir toute documentation relative aux Traitements dans son périmètre d'intervention ;
- prendre en compte la protection des Données personnelles dans la rédaction et la négociation de contrats avec des parties externes (Contrats, NDA, Lettre d'Intention, accords commerciaux, accords de transfert de données, etc.).

2.1.3 Le Délégué à la protection des données (« DPO »)

HI a désigné un **Délégué à la protection des données (*Data Protection Officer* ou DPO)** pour garantir sa conformité à la Législation applicable et le respect des engagements pris aux termes de la présente Politique.

Le DPO a plusieurs missions au sein de HI :

- informer et sensibiliser les collaborateurs aux règles à respecter en matière de protection des Données à caractère personnel ;
- veiller au respect de la Législation applicable ainsi que des engagements pris aux termes de la présente Politique ;

- conseiller les Directions métiers sur l'application concrète des principes aux projets de Traitement ;
- informer et responsabiliser, voire alerter si besoin, la Direction générale de HI des risques que les initiatives des opérationnels ou le non-respect de ses recommandations feraient courir à l'organisme ;
- établir si une Analyse d'impact relative à la protection des données (dite « AIPD ») doit être réalisée et conseiller la Direction métier dans la réalisation des AIPD ;
- assister en cas de Violation de Données personnelles pour évaluer le risque de la Violation et agir en tant que point de contact en cas de notification à l'Autorité de contrôle compétente et/ou aux Personnes concernées ;
- analyser, investiguer, auditer et contrôler le degré de conformité de HI et accompagner les Directions métiers dans la définition et la mise en œuvre d'un plan de remédiation le cas échéant ;
- établir et maintenir une documentation au titre de « l'*Accountability* » (redevabilité) ;
- garantir la gestion adéquate des droits des Personnes concernées telle que définie dans la procédure afférente ;
- présenter un rapport annuel à la Direction générale ;
- interagir avec l'autorité de contrôle.

Le DPO a la possibilité de nommer un ou plusieurs suppléants au sein des collaborateurs de HI. Une communication adéquate est effectuée par le DPO sur cette nomination.

2.1.4 Le Service juridique

Le Responsable juridique apporte son soutien et son expertise sur les sujets suivants :

- compréhension et mise en œuvre des exigences de la Législation applicable ;
- conseils sur les impacts juridiques potentiels ;
- assistance au cours du processus d'AIPD (par exemple, conseils sur le type de Données personnelles collectées, le délai de

conservation des Données, le processus de gestion du consentement) ;
- rédaction de la documentation juridique appropriée.

2.1.5 La Direction des systèmes d'information

Le Directeur des systèmes d'information (dit « DSI ») assure le management du DPO.

Pour chaque projet, il apporte son soutien et son expertise sur les sujets suivants :

- évaluation du contexte et de la criticité du projet ;
- analyse des risques, notamment dans le cadre de l'évaluation préalable à l'AIPD
- conseil sur les mesures de sécurité pour réduire, éviter ou transférer les risques ;
- évaluation du niveau de sécurité des tiers intervenants et négociation avec ces derniers pour intégrer les exigences de HI en la matière dans le contrat ;
- coordination de la surveillance, détection et gestion des incidents de sécurité, avec les conseils du DPO en cas de Violation de Données.

2.2 Rapport annuel du DPO

Le DPO établit et publie un rapport annuel sur les activités liées à la protection de la vie privée au sein de HI. À cette fin, le DPO définit, recueille et publie des indicateurs qui mettent en évidence le niveau de conformité aux politiques et procédures internes en la matière ainsi qu'à la Législation applicable.

3. Les principes à respecter en matière de Traitement des Données personnelles

Conformément à la Législation applicable, HI s'engage à respecter les principes établis ci-après lors de la collecte et du Traitement de Données personnelles.

3.1 Licéité, loyauté et transparence

Les Données à caractère personnel doivent être collectées et traitées de manière **licite, loyale et transparente.**

À ce titre, HI garantit que tout Traitement repose sur une **base légale reconnue** par la Législation applicable telle que :

- la Personne concernée a donné son Consentement au Traitement de ses Données personnelles pour une ou plusieurs finalités spécifiques (sous réserve du respect des exigences supplémentaires détaillées à la section "Consentement") ;
- le Traitement est nécessaire à l'exécution d'un contrat auquel la Personne concernée est partie ou pour prendre les mesures appropriées à la demande de la Personne concernée avant de conclure un contrat ;
- le Traitement est nécessaire au respect des obligations légales auxquelles HI est soumise ;
- le Traitement est nécessaire aux fins d'intérêts légitimes poursuivis par HI ;
- le Traitement est nécessaire afin de protéger les intérêts vitaux de la Personne concernée ;
- le Traitement est nécessaire pour l'exécution d'une mission d'intérêt public.

Lorsqu'un Traitement est basé sur l'intérêt légitime, HI procède à une analyse pour déterminer si cet intérêt légitime prime ou non sur les intérêts ou les droits et libertés fondamentales des Personnes

concernées. Cette évaluation et ses résultats doivent être documentés et consignés à des fins probatoires (*Accountability / redevabilité*).

Exceptionnellement, HI peut traiter des Données personnelles sensibles, auquel cas HI veille à respecter les exigences de la Section « Traitement des Données personnelles sensibles » de la présente Politique.

R01 Tout Traitement repose sur une base légale clairement identifiée et documentée dans le registre.

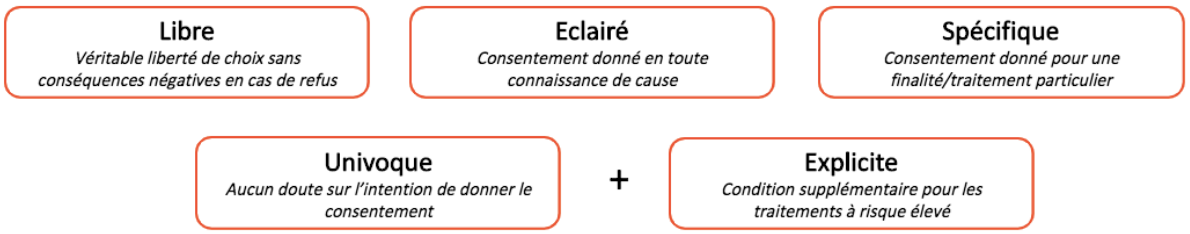
De plus, HI s'assure que les activités de Traitement des Données personnelles sont effectuées de manière **apparente et transparente**. À cette fin, HI fournit des informations accessibles et intelligibles aux Personnes concernées sur la façon dont leurs Données personnelles sont utilisées, conformément aux termes et exigences de la procédure de gestion des droits des personnes (cf. Section « Relations avec les Personnes concernées » de cette Politique).

3.2 Consentement

Lorsque le Traitement est fondé sur le Consentement de la Personne concernée, HI s'assure que ce Consentement a été obtenu légalement (voir Section sur les « Conditions de validité du Consentement ») et est correctement géré pendant toute la durée du Traitement (voir Section « Gestion du Consentement »).

3.2.1 Les conditions de validité du Consentement (caractéristiques et modalités de collecte)

HI s'assure que le Consentement obtenu de la part de la Personne concernée répond aux critères suivants :



En outre, HI doit le cas échéant s'assurer du respect des lois locales sur les conditions de validité du Consentement.

Ce Consentement doit être obtenu avant la collecte des Données et, a *minima*, concomitamment à la collecte des Données. La demande de Consentement doit être distinguée de tout autre demande / sujet, sous une forme intelligible et facilement accessible, dans un langage clair et simple.

R02 Lorsque la base légale est le Consentement, le Consentement obtenu répond aux conditions de validité de fond (caractéristiques) et de forme (collecte).

3.2.2 La gestion du Consentement (durée, preuve)

HI veille au respect de la **durée de validité du Consentement** : lorsque les modalités de Traitement changent ou évoluent, le Consentement original n'est plus valide. Un nouveau Consentement doit alors être obtenu.

HI assure le **suivi**, dans la mesure du possible, **des déclarations de Consentement reçues**, c'est-à-dire qui a donné son Consentement, comment et quand le Consentement a été obtenu, ainsi qu'une copie des informations fournies à la personne concernée à l'époque.

R03 **Les Consentements sont renouvelés en cas de modification significative des modalités de Traitement. .**

R04 **Un suivi des déclarations de Consentement est mis en place.**

3.2.3 Le retrait du Consentement

La Personne concernée doit être en mesure de **retirer son Consentement à tout moment**. HI doit donner à la Personne concernée les moyens de retirer son Consentement aussi facilement qu'il a été donné, dans la mesure du possible par une méthode équivalente à celle utilisée pour obtenir le Consentement.

Une fois le Consentement révoqué, HI doit s'assurer que le **retrait est enregistré dans ses systèmes** et bases de données dès que possible, de telle sorte que les Données personnelles ne soient plus traitées pour la finalité en question (par exemple, un adhérent VIP qui révoque son Consentement pour l'utilisation de son image ne devrait plus voir cette dernière exploitée). En outre, ce changement de statut doit être **relayé chez tous les tiers intervenants**, en particulier les Sous-traitants, de sorte qu'aucun d'entre eux ne traite plus les Données personnelles concernées pour la finalité en question.

Une fois le Consentement révoqué, HI ne peut plus se fonder sur le Consentement comme base légale pour le Traitement. Toutefois, le retrait du Consentement :

- n’affecte pas la licéité du Traitement fondé sur le Consentement avant son retrait, et
- n’exige pas nécessairement la suppression des Données personnelles concernées dans la mesure où elles peuvent encore être utiles pour un autre Traitement et/ou présenter un intérêt administratif.

R05 **La Personne concernée a la possibilité de retirer son Consentement à tout moment aussi facilement qu’il a été donné.**

R06 **Le retrait du Consentement est pris en compte de façon effective dans les outils de Traitement.**

3.3 *Limitation des finalités*

Avant toute collecte de Données personnelles, HI définit de façon claire la ou les finalités poursuivies par la collecte, lesquelles doivent être **déterminées, explicites et légitimes**. HI s’assure également que la ou les finalités ainsi définies sont compatibles avec ses activités.

Les Données personnelles ne doivent pas être traitées pour une finalité ultérieure incompatible avec la finalité initiale pour laquelle les Données ont été collectées. À ce titre, HI effectue un **test de compatibilité** pour vérifier si la finalité ultérieure est compatible avec la finalité initiale. Ce test prend en compte :

- l’existence d’un lien entre les deux finalités ;
- le contexte dans lequel les Données personnelles ont été collectées, en particulier en ce qui concerne la relation entre les Personnes concernées et HI ;
- la nature des Données Personnelles, en particulier si des Données personnelles sensibles sont traitées ;

- les conséquences possibles du Traitement ultérieur envisagé pour les Personnes concernées ;
- l'existence de garanties appropriées.

Lorsque la finalité ultérieure est incompatible avec la finalité initiale, HI s'assure de recueillir le Consentement de la Personne concernée, conformément aux exigences de la Législation applicable (Article 6 (4) du RGPD).

R07 Les Données personnelles ne sont collectées qu'à des fins spécifiques, explicites et légitimes, et ne doivent pas être traitées ultérieurement d'une manière incompatible avec cette ou ces finalités.

.

3.4 *Minimisation et exactitude*

Les Données personnelles collectées doivent être **adéquates, pertinentes et non excessives** par rapport à la finalité poursuivie par le Traitement. En d'autres termes, HI s'assure que la collecte porte uniquement sur les Données **strictement nécessaires** pour atteindre la finalité.

En outre, HI s'assure que les Données personnelles sont **exactes et, le cas échéant, mises à jour**. À cette fin et compte tenu de la finalité pour laquelle elles sont traitées et de la nécessité qui en résulte de disposer de Données exactes, HI prend des **mesures raisonnables** pour effacer ou rectifier sans délai toute Donnée personnelle inexacte.

R08 **Les Données personnelles sont adéquates, pertinentes et non excessives au regard de la finalité poursuivie par le Traitement. Elles sont exactes, complètes et mises à jour si nécessaire.**

3.5 *Conservation limitée*

HI s'assure que les Données personnelles traitées ne sont **pas conservées plus longtemps que nécessaire** au regard des finalités pour lesquelles elles sont collectées.

Les Données personnelles peuvent être conservées :

1) Sous une forme permettant l'identification des personnes concernées pendant une **durée n'excédant pas celle nécessaire au regard des finalités** pour lesquelles elles sont traitées par HI. Une fois la finalité atteinte, les Données doivent donc **être supprimées**.

2) Au-delà de la durée nécessaire à la finalité du Traitement, lorsqu'elles présentent encore un **intérêt administratif**. La durée de conservation des Données peut alors être prolongée au-delà du délai jugé pertinent pour la finalité de collecte initiale. Ce prolongement doit être dûment **justifié et documenté**.

   Les Données peuvent encore être conservées en vue de respecter des **durées légales de prescription**, des **durées de conservation particulières** (conservation des documents comptables et pièces justificatives, archivage des contrats électroniques, etc.), essentiellement à **des fins probatoires**, ou encore afin d'être en capacité de **répondre aux demandes de communication** susceptibles d'être adressées par certains tiers légalement habilités (l'administration fiscale, les organismes sociaux, etc.).

3) Pour des **durées plus longues** dans la mesure où les Données personnelles seront traitées exclusivement par HI à des **fins d'archivage** dans l'intérêt public, à des **fins de recherche scientifique** ou **historique,** pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées afin de garantir les droits et libertés de la personne concernée, telles que **l'anonymisation** ou la **pseudonymisation**.

Afin d'assurer le respect de ce principe, HI définit les durées de conservations applicables à chaque Traitement. Les éléments suivants

doivent être pris en compte pour la détermination de la durée de conservation de chaque catégorie de Données collectées :

- les obligations légales ;
- les recommandations de la CNIL ;
- les meilleures pratiques dans chaque domaine concerné ;
- les besoins opérationnels de l'association.

Ces durées sont **revues et mises à jour en tant que de besoin** pour refléter les évolutions de la Législation applicable et/ou des pratiques au sein de HI.

Au terme de cette durée, les Données sont **supprimées sans délai indu**. Cette suppression peut être opérée par destruction des Données et/ou anonymisation. En cas de suppression par destruction, HI s'assure que les Données sont effectivement détruites des systèmes (en ce inclus lorsque les systèmes concernés sont ceux d'un tiers).

Les exigences et modalités de mise en œuvre du principe de conservation limitée des Données personnelles sont détaillées dans la « Politique de conservation des Données personnelles » de HI.

R09 **Des durées de conservation sont définies et implémentées. Une Politique de conservation des données a été implémentée par HI.**

3.6 Sécurité des Données personnelles

HI prend des **mesures techniques et organisationnelles** dans le but d'assurer **la sécurité, la confidentialité et l'intégrité** des Données personnelles pendant toute la durée du Traitement. Sont pris en compte dans la détermination de ces mesures :

- la gravité et la probabilité du préjudice éventuel pouvant résulter de la perte, de l'altération et/ou de l'accès non autorisé aux Données ;
- les éléments caractéristiques du Traitement concerné ;
- le cas échéant, les résultats de l'Analyse d'impact menée relativement à la protection des données concernées ;
- l'état de l'art ;
- les coûts d'implémentation.

HI s'engage à réviser de façon régulière les mesures de sécurité afin de **tester, d'évaluer et de mesurer leur efficacité et d'entreprendre toute amélioration nécessaire**.

HI s'assure également que toute Violation des Données est gérée correctement conformément à la Section « Gestion des Violations de Données » de la présente Politique.

R10 **Des mesures techniques et organisationnelles appropriées sont mises en œuvre afin d'assurer la sécurité, la confidentialité et l'intégrité des Données personnelles.**

3.7 Transfert des Données personnelles en dehors de l'Union européenne

Les Transferts de Données personnelles exigent une attention et des garanties supplémentaires. HI s'assure que tout Transfert de Données personnelles est **sécurisé de façon adéquate** et **encadré juridiquement** conformément aux exigences de la Législation applicable.

À ce titre, HI veille à :

- **identifier tout Transfert** de Données personnelles, y compris, dans la mesure du possible, les Transferts ultérieurs opérés par les Sous-traitants (de 1er rang) ;
- **encadrer dans le contrat** avec le prestataire les Transferts de Données ainsi que, le cas échéant, le lieu d'hébergement des Données (lequel doit être par principe sur le territoire de l'Union européenne). Le prestataire doit ainsi garantir l'application de mesures permettant d'assurer un niveau de protection des Données personnelles équivalent à celui fourni par le RGPD ;
- **sécuriser tout Transfert** par des mesures techniques et organisationnelles adaptées ;
- lorsque le Transfert n'est pas à destination d'un pays reconnu comme adéquat (en vertu d'une décision d'adéquation de la Commission européenne), encadrer juridiquement le Transfert par un **mécanisme approprié**.

Dans la mesure du possible, les Données à caractère personnel ne doivent pas être transférées dans un pays situé hors de l'Union Européenne de manière automatique sans l'autorisation du DPO de HI.

R11 Tout Transfert de Données personnelles est sécurisé de façon adéquate et encadré juridiquement conformément aux exigences de la Législation applicable.

3.8 Traitement de Données personnelles sensibles

En plus de la base légale générique (voir section « Licéité, loyauté et transparence »), les Données personnelles sensibles ne peuvent être collectées QUE SI l'une des **conditions spéciales** suivantes s'applique :

- la Personne concernée a donné son Consentement explicite ;
- le Traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propre à HI ou à la personne concernée en matière de droit du travail, sécurité sociale et protection sociale ;

- le Traitement est nécessaire à la sauvegarde des intérêts vitaux de la Personne concernée ;
- le Traitement est effectué par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, dans le cadre de leurs activité légitimes et moyennant des garanties appropriées ;
- le Traitement porte sur des Données personnelles qui sont manifestement rendues publiques par la Personne concernée ;
- le Traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;
- le Traitement est nécessaire pour des motifs d'intérêt public importants, sur la base du droit de l'Union européenne ou d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des Données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la Personne concernée ;
- le Traitement est nécessaire aux fins de la médecine préventive, ou de médecine du travail, de l'appréciation de la capacité de travail du travailleur, des diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et services de soins de santé ;
- le Traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique ;
- le Traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ;
- une condition spécifique prévue par une loi locale s'applique.

HI doit prévoir des **mesures de sécurité particulières** pour ces Données au regard du risque qu'elles peuvent représenter pour la Personne concernée.

Les Données relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes ne doivent pas, par principe, être recueillies, sauf dans des cas très exceptionnels et avec la validation du

DPO (par exemple la collecte du casier judiciaire pour vérifier les informations concernant un candidat à un emploi en raison de la nature spécifique de l'offre d'emploi). En tout état de cause, ce type de Données personnelles sensibles ne peut pas être traité (ainsi la copie du casier judiciaire, si elle peut être collectée, ne peut être conservée).

R12 Le Traitement de Données sensibles est par principe interdit. Toute exception doit être réalisée dans les conditions requises par la Législation applicable et validée par le DPO.

4. Documentation et gestions des risques

Toutes les preuves du respect de la règlementation doivent être conservées afin de pouvoir démontrer la conformité de HI à l'Autorité de contrôle.

4.1 *Protection des Données dès la conception et par défaut (« Privacy by Design/by default")*

Pour tout nouveau projet impliquant le Traitement de Données personnelles, HI met en place des mesures visant à protéger les Données personnelles dès la conception du Traitement, mais aussi tout au long du projet et du cycle de vie de la Donnée personnelle (de la collecte à la destruction).

À cette fin, tout salarié de HI responsable d'un projet devra suivre les étapes suivantes :

Etape 1. Vérifier que les principes définis au paragraphe 3 de la présente Politique sont bien respectés.
Etape 2. Lister les mesures techniques et organisationnelles existantes et envisagées permettant d'assurer la sécurité, la confidentialité et l'intégrité des Données personnelles.

Etape 3. Réaliser l'évaluation préalable à l'Analyse d'impact relative à la protection des données.
Etape 4. Réaliser si nécessaire l'Analyse d'impact relative à la protection des données.
Etape 5. Implémenter les mesures de sécurité adaptées au niveau de risque.

Lorsque le projet implique de confier tout ou partie du Traitement à un Sous-traitant, HI s'assure que les exigences de la section "Gestion des tiers intervenant" sont respectées.

R13 Tout projet prend en compte la protection des Données personnelles dès la conception et par défaut.

4.2 L'Analyse d'impact relative à la protection des données

Lorsqu'un Traitement est susceptible d'engendrer un **risque élevé** pour les droits et libertés des Personnes concernées, HI effectue une **Analyse d'impact relative à la protection des données** (AIPD) sur le Traitement, **en amont de la mise en place du Traitement**.

Aussi, HI s'assure qu'une **évaluation préalable** est réalisée pour tout nouveau Traitement afin de déterminer le niveau de risque du Traitement et, partant, si une AIPD doit être conduite. Cette évaluation préalable prend en compte :

- les cas obligatoires définis par le RGPD et l'Autorité de contrôle ;
- les critères établis par le Comité européen de la protection des données ;
- les hypothèses d'exemption prévues par le RGPD et l'Autorité de contrôle.

L'AIPD doit être **documentée** et doit a *minima* :

- décrire la nature, la portée, le contexte et les finalités du Traitement ;
- évaluer la nécessité, la proportionnalité et les mesures de conformité ;
- déterminer et évaluer les risques pour les personnes ;
- déterminer toute mesure supplémentaire visant à atténuer ces risques.

Pour plus de renseignements : Fiche pratique de la CNIL sur l'AIPD et méthode interne de prise en charge des Analyses d'Impact.

R14 La nécessité d'effectuer une Analyse d'impact relative à la protection des données est identifiée pour chaque nouveau projet et une AIPD est effectuée si nécessaire, avant le début du Traitement.

L'AIPD est un **processus continu** et devra être **revue régulièrement** pour assurer que le niveau de **risque reste acceptable** tout au long de la vie du Traitement, dans la mesure où l'environnement, technique notamment, sera amené à évoluer, ce qui nécessitera d'adapter les mesures mises en œuvre.

De même, si un Traitement ne nécessite pas une AIPD dans un premier temps, mais que les opérations de Traitement évoluent, une AIPD pourra devoir être effectuée dans un second temps.

R15 La nécessité de mettre à jour une AIPD existante ou d'effectuer une AIPD est prise en compte pour chaque changement majeur dans une opération de Traitement.

Après approbation de la direction générale, le DPO **consulte l'Autorité de contrôle** si l'AIPD indique que le Traitement entraînerait un risque élevé pour les droits et libertés des personnes concernées, c'est-à-dire si le **risque résiduel est encore élevé** une fois que le plan de remédiation des risques a été défini et implémenté.

R16 **Lorsque l'AIPD montre qu'un risque résiduel élevé persiste, la CNIL est consultée.**

4.3 Le registre des Traitements

En qualité de Responsable de Traitement, HI tient un **registre des Traitements** conforme aux exigences de la Législation applicable.

Chaque Responsable Opérationnel de Traitement (ROT) au sein de HI tient à jour ses fiches de traitements sous le contrôle de son Autorité Responsable de Traitement.

À cette fin, HI détermine les acteurs clés de la tenue et mise à jour du registre, leurs rôles et responsabilités.

R17 **Un registre des Traitements mis en œuvre est tenu à jour.**

5. Formation et sensibilisation du personnel

HI s'assure que l'intégralité de ses collaborateurs est **sensibilisée à la problématique de la protection des Données** personnelles et comprend l'intention et la portée de la Législation applicable ainsi que les risques en cas de non-conformité.

Dans la mesure du possible, HI assure également une **formation spécifique** des collaborateurs qui ont vocation à traiter des Données personnelles au quotidien.

Les collaborateurs sont régulièrement informés et/ou formés des évolutions législatives ou jurisprudentielles en matière de protection des Données à caractère personnel ainsi que des mises à jour des règles internes applicables.

Tout nouveau collaborateur suit une sensibilisation/formation appropriée eu égard à ses missions et à son niveau de connaissance.

R18 L'ensemble des collaborateurs est sensibilisé aux principes et enjeux de la protection des Données personnelles. Une formation plus approfondie est dispensée aux collaborateurs traitant des Données personnelles au quotidien.

6. Relations avec les Personnes concernées

HI s'engage à garantir l'**exercice effectif** des droits des Personnes concernées qui leur sont accordés par la Législation applicable. La Législation applicable accorde aux Personnes concernées les droits suivants :

- **Droit à l'information** : le droit d'avoir une information claire, précise et complète sur l'utilisation des Données personnelles par HI.
- **Droit d'accès** : le droit d'obtenir une copie des Données personnelles que le Responsable de Traitement détient sur le demandeur.
- **Droit de rectification** : le droit de faire rectifier les Données personnelles si elles sont inexactes ou obsolètes et/ou de les compléter si elles sont incomplètes.

- **Droit à l'effacement / droit à l'oubli** : le droit, dans certaines conditions, de faire effacer ou supprimer les Données, à moins que HI ait un intérêt légitime à les conserver.
- **Droit d'opposition** : le droit de s'opposer au Traitement des Données Personnelles par HI pour des raisons tenant à la situation particulière du demandeur (sous conditions).
- **Droit de retirer son Consentement** : le droit à tout moment de retirer le Consentement lorsque le Traitement est fondé sur ce dernier.
- **Droit à la limitation du traitement** : le droit, dans certaines conditions, de demander que le Traitement des Données personnelles soit momentanément suspendu.
- **Droit à la portabilité des Données** : le droit de demander que les Données personnelles soient transmises dans un format ré exploitable permettant de les utiliser dans une autre base de Données.
- **Droit de ne pas faire l'objet d'une décision automatisée** : le droit pour le demandeur de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.
- **Droit de définir des directives post-mortem** : le droit pour le demandeur de définir des directives relatives au sort des Données Personnelles après sa mort.

À cette fin, HI définit et met en œuvre une **procédure de gestion des droits** des personnes conformes aux exigences de la Législation applicable. Cette procédure établit :

- les standards à respecter pour assurer l'information transparente des personnes ;
- les exigences légales qui doivent être respectées ;
- les moyens autorisés pour présenter une demande pour chaque droit, selon la catégorie de Personnes concernées ;

- les processus opérationnels pour traiter ces demandes conformément aux exigences susmentionnées ;
- les parties impliquées dans ces processus, leurs rôles et responsabilités.

Les demandes soumises par les Personnes concernées en application de leurs droits sont **consignées dans un registre** à des fins de preuve de la conformité. La procédure de gestion des droits des personnes susmentionnée définit le contenu et les modalités de tenue de ce registre.

R19 Une procédure relative à la gestion des droits des Personnes concernées est appliquée, les demandes éligibles étant enregistrées dans un registre dédié.

7. Gestion des Violations de Données personnelles

Conformément à son obligation de sécurité, HI définit, documente et met en œuvre un **processus pour détecter, qualifier et répondre aux Violations** de Données personnelles. La procédure documentée doit comprendre :

- une matrice d'évaluation des risques pour les droits et libertés des Personnes concernées, en tenant compte des critères définis par l'Autorité de contrôle et le Comité européen de protection des Données ;
- une répartition des rôles et des responsabilités entre toutes les parties concernées par le plan de réponse, y compris celles des Sous-traitants de HI ;
- les conditions, modalités et délais concernant la notification d'une Violation de Données à l'Autorité de contrôle compétente et/ou aux Personnes concernées.

Des moyens techniques et organisationnels adéquats sont mis en œuvre pour détecter, enquêter et signaler les Violations de Données personnelles. De plus, afin de mieux détecter et gérer les Violations, les salariés de HI sont sensibilisés et formés à la procédure à suivre en cas de Violation avérée ou suspectée.

R20 **Une procédure de gestion des failles de sécurité est définie et mise en œuvre.**

De plus, HI établit un registre des Violations de Données personnelles à des fins d'Accountability, pour notifier l'ensemble des Violations, qu'une notification soit requise ou non.

R21 **Un registre des Violations est tenu à jour.**

8. Gestion des tiers intervenants

Conformément à la Législation applicable, HI s'engage à choisir des prestataires qui présentent des **garanties suffisantes** quant à la mise en œuvre de mesures techniques et organisationnelles appropriées.

À ce titre, HI vérifie **en amont les garanties** présentées par tout prestataire tiers envisagé, au moyen notamment de questionnaires et/ou analyse de documentation. Cette vérification doit permettre d'**évaluer les conditions de mise en œuvre du Traitement chez le prestataire** : modalités de réalisation des opérations de Traitement confiées, sécurité et confidentialité des Données personnelles, maturité du prestataire tiers sur la question de la protection des Données personnelles.

R22 **Un contrôle des garanties offertes par chaque prestataire tiers est réalisé préalablement à la mise en œuvre des activités de Traitement. Une grille d'Évaluation de la conformité des sous-traitants a été implémentée au sein de HI.**

HI s'assure que le tiers intervenant est **correctement qualifié** (Responsable de Traitement distinct, co-responsable ou Sous-traitant) et s'assure qu'un **contrat écrit définit clairement les rôles et responsabilités** de chacune des parties. Ce contrat intègre au minimum les clauses requises par la Législation applicable (notamment le RGPD).

Lorsque le tiers intervient en qualité de Sous-traitant, le contrat signé détaille le ou les Traitements confiés au Sous-traitant en déterminant :

- l'objet et la durée du Traitement ;
- la nature et la finalité du Traitement ;
- la ou les catégories de Données à caractère personnel ;
- la ou les catégories de Personnes concernées ;
- les instructions relatives aux opérations de Traitement.

R23 **Un contrat écrit est signé avec chaque tiers impliqué dans le Traitement des Données. Cet accord comprend des clauses contractuelles adéquates, conformes à la Législation applicable.**

Les Sous-traitants sont **audités régulièrement** pour vérifier leur conformité continue aux obligations contractuelles et réglementaires, selon une récurrence et des modalités définis en fonction de la nature et sensibilité des opérations de Traitement confiées, des coûts nécessaires et des ressources disponibles.

R24 **Les Sous-traitants sont audités régulièrement pour vérifier leur conformité continue aux obligations contractuelles et réglementaires**

9. Relations avec l'Autorité de contrôle

HI coopère **pleinement avec toute Autorité de contrôle** lorsque cela est requis et fournit toutes les preuves de sa conformité avec la Législation applicable.

Le Délégué à la protection des données (DPO) de HI agit en **qualité de point de contact** de l'Autorité de contrôle et pilote à ce titre :

- la consultation de l'Autorité de contrôle concernée dans le cas où un Traitement de Données personnelles implique un risque résiduel élevé pour la vie privée ;
- le signalement d'une Violation de Données à l'Autorité de contrôle lorsque cela est requis ;
- le Traitement de toutes demandes (telles que les demandes d'accès aux registres de Traitements, les demandes d'information, etc.).

HI définit une **procédure en cas d'audit** par une Autorité de contrôle, laquelle définit les rôles et responsabilités des acteurs clés dans le cadre de ces contrôles.

R25 HI coopère avec l'Autorité de contrôle compétente et définit une procédure en cas de contrôle.

10. Contrôle de la conformité

HI garantit le respect de la présente Politique générale de protection des Données personnelles ainsi que des procédures de mise en œuvre et des politiques supplémentaires relatives à la protection des Données personnelles.

À cette fin, un **contrôle annuel de conformité** est réalisé sur le **respect des règles** édictées et la **concordance des activités de Traitement** mises en œuvre avec le registre des Traitements. Ce dispositif de contrôle est porté par le DPO et le Directeur des systèmes d'information au sein de HI.

Lorsque des manquements sont identifiés, un **plan de remédiation** est défini par le DPO et toutes les parties prenantes concernées afin de remédier aux déficiences détectées, en tenant compte des risques encourus, des coûts de mise en œuvre, des contraintes opérationnelles existantes et prévisibles et des ressources humaines disponibles. Les mesures correctives du plan de remédiation sont mises en œuvre **sans retard injustifié** par les parties prenantes concernées, sous la supervision du DPO.

R26 **Un dispositif de contrôle de la conformité est mis en place.**

R27 **Un plan de remédiation est défini et mis en œuvre pour corriger toute non-conformité détectée.**

11. Engagements de HI en qualité de Sous-traitant

11.1 Le registre des Traitements géré par HI en tant que Sous-traitant

Conformément à la Législation applicable, HI s'engage à tenir à jour un **registre des activités de Traitement mis en œuvre pour le compte de tiers Responsables de traitement**. Ce registre doit comporter les informations suivantes :

- le nom et les coordonnées du Sous-traitant, ainsi que du Responsable de Traitement pour le compte duquel il traite des Données personnelles, ainsi que les coordonnées du DPO ;
- la (les) catégorie(s) de Traitement effectué pour le compte de chaque Responsable de Traitement ;
- le cas échéant, les transferts de Données personnelles vers un pays tiers ou une organisation internationale, ainsi que les documents attestant de l'existence de garanties appropriées ;
- une description générale des mesures de sécurités techniques et organisationnelles mises en œuvre.

Ce registre de Traitements doit être actualisé en tant que de besoin pour être **exact et exhaustif**.

R28 Un registre des activités de Traitement mis en œuvre en qualité de Sous-traitant est tenu à jour.

11.2 Obligations additionnelles de HI en qualité de Sous-traitant

Dans le cadre de ses activités, HI intervient en qualité de Sous-traitant de tiers Responsables de traitement. À ce titre, des **obligations spécifiques** s'imposent à HI en application desquelles HI s'assure de :

- **tenir à jour un registre des activités de Traitement** mis en œuvre au nom et pour le compte des Responsables de Traitement (cf. Section précédente) ;
- **agir dans le cadre des instructions licites** du Responsable de traitement ;
- **établir un contrat** avec le Responsable de Traitement conforme aux dispositions de la Législation applicable ;
- **veiller à l'application des principes de protection des Données personnelles dès la conception et par défaut** ;
- soumettre les collaborateurs en charge des activités de Traitement à une **obligation de confidentialité** ;

- respecter les **obligations contractuelles** concernant le recrutement d'un **sous-traitant ultérieur ;**
- intégrer à la procédure de gestion des violations de données les mesures nécessaires pour **notifier toute Violation de Données au(x) Responsable(s)** de traitement concerné(s) ;
- prendre les **mesures techniques et organisationnelles adéquates pour garantir un niveau de sécurité adapté aux risques** ;
- sur les instructions du Responsable de Traitement, **supprimer ou restituer l'ensemble des Données** personnelles du Responsable de Traitement, sauf obligation légale de les conserver (les données non personnelles attestant de la bonne exécution des prestations peuvent être conservées pendant la durée de la prescription des actions commerciales) ;
- **assister, alerter et conseiller** le Responsable de Traitement en :
    - l'informant lorsqu'une instruction est susceptible de constituer une violation de la Législation applicable ;
    - aidant le Responsable de Traitement à répondre aux demandes des Personnes concernées (une compensation financière pouvant être demandée au Responsable de traitement) ;
    - fournissant les informations à sa disposition pour permettre au Responsable de Traitement de conduire une Analyse d'impact relative à la protection des données et de respecter ses obligations en matière de gestion des Violations de Données (une compensation financière pouvant être demandée au Responsable de traitement) ;
- mettre à la disposition du Responsable de Traitement les **preuves de sa conformité** et **permettre la réalisation d'audit** (dans les termes et conditions prévues au Contrat).

R29 **Les obligations additionnelles en qualité de Sous-traitant sont mises en œuvre.**

Annexe 1 Définitions

Analyse d'impact relative à la protection des données (AIPD) : analyse à effectuer par HI pour les Traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Autorité de contrôle : autorité publique indépendante instituée par un État membre en vertu de l'article 51 du RGPD, chargée de surveiller l'application du RGPD, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du Traitement et de faciliter le libre flux des Données à caractère personnel de l'Union européenne. En France il s'agit de la CNIL.

Autorité Responsable de Traitement (ART) – cf. 2.1.2 : chez HI, chaque responsable d'une Direction métier est Autorité Responsable de Traitement (ART), dans la mesure où il est en autorité sur la mise en œuvre d'un ou plusieurs Traitements de Données personnelles.

Consentement : toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la Personne concernée accepte, par une déclaration ou par un acte positif clair, que des Données à caractère personnel la concernant fassent l'objet d'un Traitement.

Délégué à la protection des données (*Data Protection Officer* ou DPO) – cf. 2.1.3: la personne désignée par HI en charge de la protection des Données personnelles au sein de HI et de la conformité de l'association à la Législation applicable.

Destinataire : personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de Données à caractère personnel, qu'il s'agisse ou non d'un Tiers.

Données à caractère personnel/Données personnelles : toute information se rapportant à une Personne concernée notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, un numéro de carte d'identité, un salaire, des dossiers de santé, des informations de compte bancaire, des habitudes de conduite ou de consommation, des Données de localisation, un identifiant en ligne, etc. Le terme « Données personnelles » inclut les Données à caractère personnel sensibles.

Données à caractère personnel sensibles/Données personnelles sensibles : désigne les Données à caractère personnel révélant ou reposant sur :

- l'origine raciale ou ethnique, les opinions politiques, religieuses ou philosophiques ;
- l'appartenance à une organisation syndicale ;
- la santé physique ou mentale ;
- l'orientation sexuelle ou la vie sexuelle ;
- les Données génétiques et biométriques ;
- des Données relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes.

Législation applicable : ensemble de réglementation relative à la protection des Données personnelles et applicable aux Traitements de Données personnelles effectués par HI, à savoir le Règlement européen n°2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données dit « RGPD », la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés telle que modifiée par la loi

n°2018-493 du 20 juin 2018 promulguée le 21 juin 2018 prenant en compte le RGPD et opérant transposition de la Directive « Police-Justice », et toute autre réglementation qui y serait relative, applicable à HI.

Personne concernée : individu sur lequel porte les Données à caractère personnel et qui peut être identifié ou identifiable, directement ou indirectement, grâce à ces Données personnelles. Cela inclut les clients, prospects, et collaborateurs anciens et actuels.

Responsable de Traitement : personne physique ou morale qui, individuellement ou conjointement, décide quelles Données à caractère personnel sont collectées, pourquoi et comment elles sont collectées et traitées.

Responsable Opérationnel de Traitement (ROT) – cf. 2.1.2 : personne physique qui conjointement avec d'autres (notamment son ART, le DPO, la DSI…) définit les finalités et met en œuvre les moyens du Traitement (chaine stratégique, opérationnelle, mise en conformité et gestion de crise…).

RGPD : abréviation du Règlement européen n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Sous-traitant : toute personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des Données à caractère personnel au nom du Responsable de Traitement et selon ses instructions (par exemple des prestataires ou fournisseurs).

Tiers : toute personne physique ou morale, autorité publique, agence ou tout autre organisme autre que la Personne concernée, le Responsable du Traitement, le Sous-traitant et les personnes qui, sous l'autorité directe du Responsable du Traitement ou du Sous-traitant, sont habilités ou autorisés à traiter les Données.

Traitement : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des Données personnelles telle que la collecte, l'accès, l'enregistrement, la copie, le transfert, la conservation, le stockage, le croisement, la modification, la structuration, la mise à disposition, la communication, la destruction, que ce soit de manière automatique, semi-automatique ou autre, cette liste n'étant pas exhaustive.

Transfert de Données : toute communication, toute copie ou tout déplacement de Données par l'intermédiaire d'un réseau ; ou toute communication, toute copie ou tout déplacement de ces Données d'un support à un autre, quel que soit ce support ; toute communication, toute copie ou tout déplacement de Données personnelles vers un pays tiers à l'Union européenne ou à une organisation internationale – Données qui font ou sont destinées à faire l'objet d'un Traitement après ce transfert.

Violation de Données à caractère personnel : violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles Données.