



28 MARS 2018


POLITIQUE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

SIACI SAINT HONORÉ

S2H

Season, 39 rue Mstislav Rostropovitch - 75815 Paris cedex 17 - France

Tél : +33 (0)1 4420 9999 Fax : +33 (0)1 4420 9500



INFORMATIONS GENERALES

Date	28/03/2018
Libellé	Politique de Protection des Données à Caractère Personnel (PPDCP)
Direction émettrice	Direction des Risques et de la Conformité
Validation	Direction des Risques et de la Conformité & Direction Juridique
Responsable(s) du document	Samanta Le Pont
Diffusion	Information Publique Ce document est diffusé à l'ensemble des services internes de S2H et peut être diffusé dans le cadre de relations commerciales (clients, porteurs de risques, sous-traitants).
Versions	1 ^{ère} version : 28/03/2018

SOMMAIRE

1. CONTEXTE	5
1.1 Contexte réglementaire	5
1.2 Contexte interne	5
2. DOMAINE D'APPLICATION	6
2.1 Définitions	6
2.2 Etendue de la Politique	6
3. OBJET DE LA POLITIQUE	7
4. ORGANISATION DETAILLEE DEDIEE A LA PROTECTION DES DONNEES PERSONNELLES	7
4.1 Organisation dédiée à la protection des données personnelles	7
4.2 Les rôles et responsabilités de l'organisation dédiée à la protection des données personnelles	7
a. <i>Le DPO</i>	7
b. <i>Les Correspondants « Protection des Données » (CPD)</i>	9
c. <i>Les IT Risk Managers (ITRM)</i>	10
d. <i>La Direction des Risques et de la Conformité</i>	10
e. <i>La Direction Juridique</i>	10
f. <i>La Direction des Systèmes d'Information</i>	10
4.3 Dispositifs de pilotage et de suivi	10
5. LES PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL	11
5.1 Collecte	11
5.2 Déclarations des traitements	12
5.3 Etude d'Impact sur la Vie Privée	13
5.4 Sécurité des traitements	14
5.5 Le cas particulier du NIR et des données de santé	14
5.6 Les droits des personnes concernées	15
5.7 Transferts de données à caractère personnel	16
5.8 Sous-traitance	17
5.9 Contrôle	17
5.10 Protection des données dès la conception des projets et au plus haut niveau de protection	17
5.11 Gestion des violations de données	18
5.12 Le sort des données après réalisation de la prestation	18
6. EXAMENS DE CONFORMITE PERIODIQUES	18
ANNEXE 1	20
ANNEXE 2	23

ANNEXE 3	24
ANNEXE 4	25

GLOSSAIRE

CNIL	Commission Nationale de l'Informatique et des Libertés.
Donnée à caractère personnel	Toute information se rapportant à une personne physique identifiée ou identifiable.
Donnée de santé	Donnée à caractère personnel relative à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèle des informations sur l'état de santé de cette personne.
Donnée sensible :	<p>Au sens du RGPD, la donnée sensible est une donnée qui à trait :</p> <ul style="list-style-type: none"> - aux origines raciales ou ethniques ; - aux opinions politiques, philosophiques ou religieuses ou à l'appartenance syndicale des personnes ; - à la santé, à la vie sexuelle ou à l'orientation sexuelle ; - aux données génétiques ; - aux données biométriques aux fins d'identifier une personne physique de manière unique. <p>Le Groupe Siaci Saint Honoré a fait le choix de considérer le NIR comme une donnée sensible et de lui appliquer une telle protection.</p>
DPO	<i>Data Protection Officer</i> ou Délégué à la Protection des Données
NIR	Numéro d'Inscription au Répertoire national, également nommé « numéro de sécurité sociale »
Responsable de traitement	Le responsable de 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.
RGPD	Règlement Général sur la Protection des Données à caractère Personnel. S'agissant d'un Règlement européen, il est d'application directe dans l'ordre juridique des pays membres de l'Union européenne.
Sous-traitant	Le sous-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.
Utilisateur	Toute personne qui est amenée à manipuler des données à caractère personnel informatisées ou non ainsi que toute personne qui procède à des traitements automatisés ou non de ce type de données et ce, quel que soit le statut de cet Utilisateur.

1. CONTEXTE

1.1 *Contexte réglementaire*

En France, la législation applicable à la protection des données à caractère personnel* est issue de la loi « Informatique et Libertés » du 6 janvier 1978¹ régulièrement modifiée depuis. La protection des données à caractère personnel est un enjeu tant au niveau européen, avec la Directive du 24 octobre 1995², qu'au niveau national puisque cette Directive a été transposée en France par la loi du 6 août 2004³ (qui modifia la Loi « Informatique et Libertés »).

Plus récemment, le Règlement Général sur la Protection des Données à caractère personnel (ci-après désigné par : « le RGPD »), aussi connu sous le nom de *General Data Protection Regulation* (GDPR), entré en vigueur le 24 mai 2016 et applicable le 25 mai 2018 dans tous les Etats membres de l'Union Européenne, remplace la Directive européenne sur la protection des données personnelles (Directive 95/46/CE).

Les personnes sont aujourd'hui très attentives à leurs données personnelles et à leur protection afin d'en préserver la confidentialité (notamment les données financières ou de santé). Ils attendent que leur vie privée soit respectée et que les entreprises auxquelles elles confient leurs données soient en mesure de les protéger.

Ce sont pour ces raisons que Siaci Saint Honoré (ci-après désigné par « le Groupe ») travaille à garantir la sécurité des données qui lui sont confiées. Au-delà du respect de la réglementation en la matière, il s'agit de l'essence même des activités qui lui sont confiées.

Les risques suivants peuvent être encourus dans le cadre de procédures de protection déficientes :

- risques d'image, de réputation ;
- risques légaux, sanctions du marché, du régulateur, responsabilité en cas d'usurpation d'identité ;
- décrédibilisation de l'entreprise vis-à-vis de ses clients ou de ses salariés ;
- perte d'affaires et ses conséquences sur la réduction des profits et la part de marché.

Les impacts sont également conséquents en cas d'amende administrative prononcée par une autorité de contrôle telle que la Commission de l'Informatique et des Libertés (ci-après-désigné par « CNIL ») pouvant aller, pour une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent⁴.

1.2 *Contexte interne*

Siaci Saint Honoré est le groupe leader en France de conseil et de courtage en assurance de biens et de personnes pour les entreprises.

Le Groupe peut, dans certaines situations, être responsable de traitement* et dans d'autres, sous-traitant*. Conscient des enjeux que soulèvent ces différentes qualifications, le Groupe Siaci Saint Honoré a mis en place la présente Politique de Protection des Données à Caractère Personnel (ci-après désignée par « PPDCP ») reprenant l'ensemble des principes applicables aux données à caractère personnel collectées et traitées dans le cadre de ses activités.

¹ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

² Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

³ Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

⁴ Article 83 RGPD.

2. DOMAINE D'APPLICATION

2.1 Définitions

- *Donnée à caractère personnel*

Selon le RGPD, une donnée à caractère personnel est « *toute information se rapportant à une personne physique identifiée ou identifiable* »⁵.

Dans le cadre de ses activités, notamment de santé et de prévoyance, mais aussi en cas de sinistre corporel, le Groupe est amené à collecter et manipuler des données à caractère personnel telles que le nom, le prénom, l'âge ou encore l'adresse mais également des données dites « sensibles ».

- *Donnée sensible*

Au sens du RGPD, la donnée sensible* est une donnée qui à trait :

- aux origines raciales ou ethniques ;
- aux opinions politiques, philosophiques ou religieuses ou à l'appartenance syndicale des personnes ;
- à la santé⁶, à la vie sexuelle ou à l'orientation sexuelle ;
- aux données génétiques ;
- aux données biométriques aux fins d'identifier une personne physique de manière unique.

Le Groupe, dans le cadre de ses activités est également amené à traiter le Numéro d'Identification au Registre national (ci-après désigné « NIR »). Bien que ne faisant pas partie de la définition de la « donnée sensible » au sens de la Commission Nationale de l'Informatique et des Libertés (ci-après désignée « CNIL »), Siaci Saint Honoré a choisi d'appliquer au NIR les mêmes règles qu'aux données sensibles.

2.2 Etendue de la Politique

La présente PPDCP s'applique à l'ensemble des Utilisateurs* de données à caractère personnel au sein du Groupe. L'Utilisateur est toute personne qui est amenée à manipuler des données à caractère personnel informatisées ou non ainsi que toute personne qui procède à des traitements automatisés ou non de ce type de données et ce, quel que soit le statut de cet Utilisateur.

De manière contractuelle, la présente PPDCP s'applique donc également aux partenaires et fournisseurs de prestations de services ainsi qu'à l'ensemble des sous-traitants qui sont ou seront amenés à collecter et/ou traiter des données à caractère personnel pour le compte et sur instruction du Groupe.

De plus, toute utilisation des données à caractère personnel est réalisée dans un cadre professionnel et responsable, c'est-à-dire dans le cadre exclusif des attributions de l'Utilisateur et de ses fonctions définies par le Groupe. Les instructions du responsable de traitement doivent être respectées et ce respect doit être contrôlé⁷. A ce titre, l'Utilisateur est responsable de l'usage qu'il fait des ressources du Groupe dans l'exercice de ses fonctions.

En ce sens, la **Politique de Sécurité des Systèmes d'Information** du Groupe (ci-après désignée « PSSI ») indique que tout nouvel arrivant prend connaissance de la *Charte d'utilisation des ressources informatiques et services Internet*.

Le Groupe s'engage à traiter les données de manière confidentielle et pour cela les accès au système d'information sont soumis à habilitation et sont contrôlés.

⁵ Article 4, 1° RGPD.

⁶ Art. 4, 15° RGPD : une donnée de santé est une « *donnée à caractère personnel relative à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèle des informations sur l'état de santé de cette personne* ».

⁷ Art. 32,4° RGPD.

En effet, selon la PSSI du Groupe, quatre (4) types de directives - concernant l'identification, l'authentification, les habilitations, et la responsabilité de la gestion des droits attribués aux profils - ont été mises en place. Le respect de ces principes permet d'attribuer aux utilisateurs, uniquement les droits dont ils ont réellement besoin dans le cadre de leur activité afin d'éviter tout accès inutile et de limiter les conséquences d'une faille des systèmes d'authentification.

3. OBJET DE LA POLITIQUE

De part sa présence internationale, le Groupe doit être conforme à la Loi française « Informatique & Libertés », au RGPD et aux directives européennes (comme celle relative aux échanges transfrontaliers des données⁸ par exemple), et également aux législations locales applicables.

La PPDCP a donc pour objectif de déterminer une trame globale et commune à l'action concernant la protection des données personnelles qui sont confiées au Groupe, tout en préservant les particularités de chaque entité, liées aux risques encourus et aux lois et contextes s'y appliquant.

La PSSI prévoit d'ailleurs que le Groupe intègre les contraintes liées :

- Au nouveau RGPD ;
- A l'hébergement des données de santé ;
- Aux informations classifiées défense.

4. ORGANISATION DETAILLEE DEDIEE A LA PROTECTION DES DONNEES PERSONNELLES

4.1 Organisation dédiée à la protection des données personnelles

Le RGPD impose au Groupe Siaci Saint Honoré de désigner un Data Protection Officer (DPO) compte tenu des volumes importants de traitements de données et particulièrement de données sensibles⁹.

Afin de gérer au mieux la conformité de l'ensemble de ses sociétés vis-à-vis de la réglementation applicable aux données personnelles, le Groupe a décidé de désigner un DPO ainsi qu'un réseau de « Correspondants Protection des Données » (ci-après désignés « CPD ») et d'IT Risk Managers (ci-après désignés « ITRM ») afin de dynamiser et rendre effective la protection des données dans l'ensemble du Groupe.

Un Comité « Données Personnelles » a également été mis en place.

4.2 Les rôles et responsabilités de l'organisation dédiée à la protection des données personnelles

a. Le DPO

Le Groupe a désigné Samanta Le Pont, à la tête de la Direction des Risques et de la Conformité, en tant que CIL :

- Pour S2H, MSH International, Assurance et Réassurances Techniques, GA Prévoyance Conseils et S2H Consulting : à effet du 13/07/2017 (Référence CIL 111540).
- Pour Cap Marine Assurance et Réassurance : à effet du 19/08/2017 (Référence CIL 171753).
- Pour MyP.

⁸ Directive 2011/82/UE du parlement européen et du Conseil du 25 octobre 2011 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière.

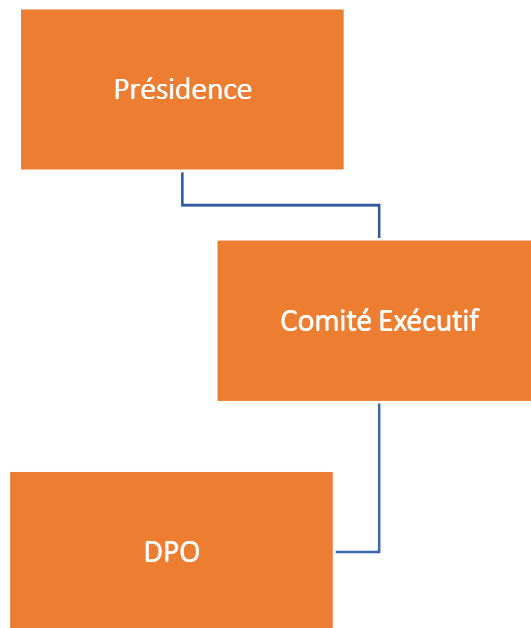
⁹ Art. 37, 1° c) RGPD.

La CNIL a indiqué, par courriers adressés aux CILs actuellement désignés, qu'ils n'avaient pas obligatoirement vocation à devenir DPO. Il s'agit d'un choix appartenant au Responsable de Traitements* devant prendre en compte plusieurs critères tels que :

- L'absence de conflit d'intérêts ;
- Les compétences professionnelles requises pour exercer les activités de DPO (connaissances juridiques, connaissances techniques, connaissances du secteur de l'assurance, etc.) ;
- L'indépendance ;
- Les qualités personnelles indispensables à l'exercice des missions (probité, loyauté, etc.).

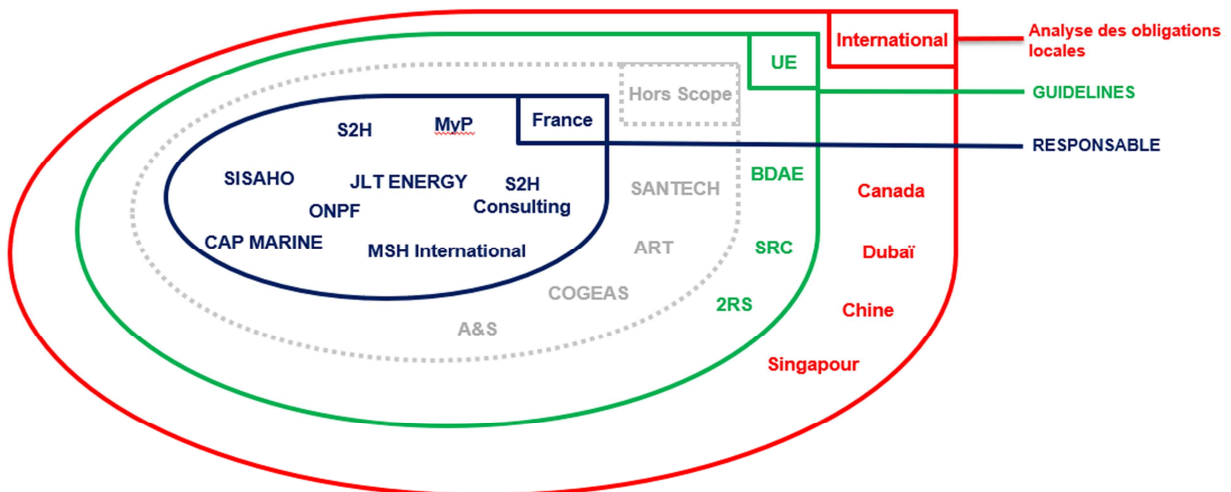
Le Groupe, après étude de ces différents critères, a choisi de désigner le CIL actuel en tant que DPO.

Le DPO est rattaché au Secrétaire Général, membre du Comité Exécutif du Groupe Siaci Saint Honoré, et directement rattaché à la Présidence.



Son rôle est central.

Le périmètre déterminé pour l'implication du DPO est le suivant :



Le DPO tient un registre des traitements dans lequel figure l'ensemble des traitements réalisés dans les filiales et les entités du Groupe en France.

Bien que le RGPD ne formule aucune exigence quant à la tenue d'un registre pour le DPO, le DPO du Groupe, continuera à le tenir dans un souci de suivi des traitements et d'*accountability* (preuve de la conformité).

Le DPO diffuse des guides et des recommandations dans les filiales hors France pour la bonne tenue des registres en local.

Le DPO doit être consulté avant la mise en œuvre de tout traitement (formulaire « Nouveau Projet » en ANNEXE 1). Ainsi, il veille au respect de la législation applicable, dans l'Espace Economique Européen (EEE), en matière de protection des données. Ses avis et recommandations doivent être recherchés avant toute mise en œuvre d'un nouveau projet.

Le DPO est amené à échanger avec les différentes directions (Direction des Systèmes d'Information, Direction Juridique, Direction des Risques et de la Conformité, etc.) ainsi qu'avec les différents Correspondants à la Protection des Données (CPD) et IT Risk Managers (ITRM) nommés au sein de chaque ligne métier ou département dans les entités du Groupe en France.

Le DPO diffuse des instructions aux officiers de compliance dans les entités du Groupe hors France.

Il est principalement chargé :

- D'animer et de coordonner le dispositif de protection des données personnelles ;
- De garantir la conformité au RGPD et aux règles internes ;
- D'interagir et de coopérer avec l'autorité de contrôle.

Il est à noter que le DPO n'est pas personnellement responsable en cas de non-conformité de son organisme avec le RGPD.

Le DPO analyse la conformité des traitements au regard de la réglementation relative à la protection des données. Cette analyse porte notamment sur : la finalité, la proportionnalité du traitement, la pertinence des données au regard de la finalité, la durée de conservation des données, les destinataires des données, l'encadrement des relations avec les sous-traitants, les mesures de sécurité, l'information des personnes concernées et les modalités d'exercice de leurs droits et le cas échéant, l'encadrement des flux transfrontières de données.

Il a également un rôle d'alerte car il informe le Groupe des manquements constatés et le conseille dans la réponse à apporter pour y remédier.

Le DPO et son équipe assurent la sensibilisation des salariés du Groupe Siaci Saint Honoré et si nécessaire leur formation au travers de sessions *ad hoc*.

Afin d'assurer l'ensemble de ses missions, le DPO veille au maintien de ses compétences en se tenant informé des dernières évolutions en matière de protection des données à caractère personnel. Il est ainsi amené à assister régulièrement à des formations ou à des conférences portant sur cette thématique.

b. Les Correspondants « Protection des Données » (CPD)

Ils sont nommés au sein de chaque ligne métier et sont chargés d'être le « référent protection des données » sur leur périmètre respectifs. Ils sont le point de contact du DPO sur leur périmètre de responsabilité. Ils peuvent être sollicités par les opérationnels sur des questions portant sur la protection des données.

En sus de leurs activités opérationnelles, leurs principales missions sont :

- D'organiser la remontée des informations relatives à tous nouveaux projets de traitements de données pour permettre l'échange avec le DPO et la Direction des Systèmes d'Information ;

- De sensibiliser sa Direction à la protection des données personnelles ;
- De participer aux projets relatifs à la protection des données personnelles ;
- D'assurer un niveau d'alerte continu sur la conformité à la protection de la data dans sa Direction.

c. Les IT Risk Managers (ITRM)

Les ITRM sont garants au quotidien du respect des obligations de protection des données à caractère personnel au sein du Système d'Information (SI). Ils :

- Animent la démarche de protection des données à caractère personnel dans les systèmes d'information (SI) ;
- Dynamisent la remontée et la descente d'informations avec le DPO ;
- Participent aux échanges réguliers avec les Correspondants à la Protection des Données (CPD).

d. La Direction des Risques et de la Conformité

La Direction des Risques et de la Conformité (ci-après désignée « DRC ») assiste le DPO dans la réalisation de ses missions et apporte son expertise sur l'analyse des risques et de la conformité. Ainsi, elle est chargée de participer à la mise à jour de la documentation interne (cartographie des risques, politique de contrôle interne, plan de contrôle interne, etc.).

La DRC contribue également aux analyses d'impact sur la vie privée avec les opérationnels et le DPO.

e. La Direction Juridique

La Direction Juridique (ci-après désignée « DJ ») apporte son support et son expertise juridique pour la réalisation des missions du DPO. Elle participe notamment à la mise à jour de procédures de contractualisation et de pré-contractualisation ou encore à la rédaction des clauses contractuelles types.

La DJ est également chargée de suivre les évolutions réglementaires et législatives en France en matière de protection des données.

f. La Direction des Systèmes d'Information

La Direction des Systèmes d'Information (ci-après désignée par « DSI ») assiste le DPO dans la réalisation de ses missions et apporte son expertise sur la sécurisation des applicatifs et les principes d'architectures.

Les principaux rôles de la DSI en matière de protection des données personnelles sont décrits dans la PSSI du Groupe.

Comme indiqué dans la **PSSI du Groupe**, différents rôles et responsabilités doivent être clairement définis. La note d'organisation, rédigée en commun avec la DSI, détermine l'organisation de la SSI au sein du Groupe et définissent les rôles et responsabilités de la société en matière de gestion de la sécurité du système d'information.

4.3 Dispositifs de pilotage et de suivi

Le Groupe s'est doté d'un Comité « Données Personnelles » qui :

- Pilote l'avancement des travaux du projet ;
- Valide les options structurantes et les arbitrages attendus ;
- Valide les livrables clés du projet ;
- Coordonne les différentes parties prenantes du projet tout au long de ce dernier ;

- Fixe les objectifs et les orientations du projet.

Ce Comité comprend :

- Le Secrétaire Général ;
- La Direction des Systèmes d'Information ;
- La Direction Ressources Humaines ;
- La Direction Communication ;
- La Direction Juridique ;
- La Direction Générale MSH ;
- La Direction des Risques et de la Conformité ;
- La Direction Développement Vie ;
- La Direction IARDT.

Il se réunit au minimum deux (2) fois par an et garde la possibilité de réunir un Comité d'urgence en cas de problématique devant être résolue rapidement.

Le Groupe Siaci Saint Honoré diffuse une culture de protection des données auprès de l'ensemble de ses collaborateurs.

Pour cela, il veille à ce que l'ensemble de ses salariés soit sensibilisé et respecte les principes applicables à la protection des données à caractère personnel dans la mise en œuvre de la collecte et du traitement, tant de données à caractère personnel que de données dites « sensibles ».

La formation de l'ensemble des collaborateurs est également organisée tout comme les communications régulières sur l'intranet Groupe sur des sujets relatifs à la protection des données personnelles. La diffusion de newsletters est renforcée sur la période de janvier 2018 à mai 2018 et sera poursuivie dans une logique de diffusion de la culture de la protection des données au sein du Groupe.

En effet, selon la PSSI, la formation et la sensibilisation du personnel à la Sécurité des Systèmes d'Information (ci-après désignée « SSI ») sont une activité prioritaire de SSI et doivent permettre de réduire les risques encourus.

La Direction des Systèmes d'Information et les Ressources Humaines s'assurent que :

- Les documents relatifs à la sécurité ont été diffusés et présentés à l'ensemble du personnel.
- Le personnel a et connaît les moyens d'y accéder en cas de doute ou de question.
- Les formations nécessaires sont disponibles.

5. LES PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

5.1 Collecte

La collecte, le traitement, la conservation et l'enregistrement de données à caractère personnel ne peuvent être effectués au sein du Groupe Siaci Saint Honoré, que dans le cadre des instructions reçues par l'Utilisateur. Cet Utilisateur se doit, dans son activité, de mettre en œuvre notamment les principes fondamentaux décrits ci-dessous.

Tout Utilisateur, dans le cadre de son activité professionnelle et/ou de sa fonction au sein du Groupe Siaci Saint Honoré, doit impérativement, lorsqu'il procède à une collecte de données à caractère personnel, respecter les principes de **loyauté, licéité et de légalité** édictés par la réglementation applicable à la protection des données à caractère personnel.

Pour que la collecte soit loyale, licite et légale, la personne concernée par la collecte et le traitement de ses données doit recevoir une information concise, transparente, compréhensible, facilement accessible et en des termes clairs et simples, de la part de la personne qui recueille de telles données¹⁰.

Dans le cadre d'une **collecte directe**¹¹ (ex : formulaire d'inscription), les informations suivantes doivent être données au moment de la collecte :

- L'identité et coordonnées du responsable de traitement et, le cas échéant, du représentant du responsable de traitement ;
- Les coordonnées du DPO ;
- La / les finalité(s) du traitement ;
- La / les base(s) juridique(s) du traitement (ANNEXE 2). Si le traitement repose sur les intérêts légitimes du responsable du traitement, il est alors nécessaire de préciser quels sont-ils. Dans le cas présent, il sera aussi nécessaire d'informer la personne concernée qu'elle peut retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;
- Le / les destinataire(s) ou catégorie(s) de destinataire(s) des données ;
- L'intention d'effectuer un transfert de données vers un pays tiers ou une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition ;
- La durée de conservation des données ou, lorsque cela n'est pas possible, les critères utilisés pour déterminer cette durée ;
- Les droits d'accès, de rectification ou d'effacement ou de limitation ou d'opposition, et de portabilité ;
- La possibilité d'organiser des directives après sa mort ;
- Le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- Pour chaque données, le caractère obligatoire ou facultatif ainsi que les conséquences éventuelles de la non-fourniture de ces données (si l'exigence de fourniture de données à un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat) ;
- L'existence d'une prise de décision automatisée, y compris un profilage ainsi que des informations concernant la logique sous-jacente et l'importance et les conséquences prévues du traitement sur la personne concernée.

Dans le cadre d'une **collecte indirecte**¹² (ex : achat d'un fichier de prospection), il est nécessaire de fournir l'ensemble des informations précitées ainsi que la source des données. Ces informations doivent être communiquées à la personne concernée :

- Sous un mois maximum, après obtention des données ;
- Au plus tard au moment de la première communication à ladite personne, si les données doivent être utilisées aux fins de communication avec la personne concernée ;
- Au plus tard lorsque les données sont communiquées pour la première fois, si les données doivent être communiquées à un autre destinataire.

5.2 Déclarations des traitements

Le RGPD supprime le régime de déclaration préalable des traitements auprès de la CNIL.

Il appartient au Groupe de mener une analyse d'impact sur la vie privées des personnes concernées afin de mesurer le risque que présente les nouveaux traitements envisagés. Si, à l'issue de l'analyse, le risque est élevé pour la vie privée des personnes concernées, le Groupe doit consulter la CNIL pour une

¹⁰ Art. 12 RGPD et Art. 90 du Décret du 20 octobre 2005.

¹¹ Art. 12 RGPD et Art. 32 Loi « Informatique et Libertés ».

¹² Art. 13 RGPD.

demande d'avis ou d'autorisation (uniquement dans le cas où la prise de mesures techniques et/ou organisationnelles nécessaires ne serait pas suffisante à atténuer le risque initialement mesuré par l'analyse d'impact).

5.3 Etude d'Impact sur la Vie Privée

En l'absence de déclaration préalable, le Groupe Siaci Saint Honoré évalue le niveau de risque que présente un traitement à l'aide des critères énumérés par le G29¹³ :

- **Evaluation ou notation y compris profilage et prédiction** : il s'agit de traitements portant sur le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêts, sa fiabilité ou son comportement, ou sa localisation et ses déplacements
- **Prise de décision automatisée avec effet juridique ou effet similaire significatif** : traitement ayant pour finalité la prise de décisions à l'égard des personnes concernées produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative de façon similaire.
- **Surveillance systématique** : traitement utilisé pour observer, surveiller ou contrôler les personnes concernées.
- **Données sensibles ou données à caractère hautement personnel** : traitements portant sur les catégories de données visées aux articles 9 et 10 du RGPD. Il peut également s'agir de traitements portant sur des données pouvant être considérées comme augmentant le risque possible pour les droits et les libertés des personnes (communications électroniques, coordonnées bancaires, ...)
- **Données traitées à grande échelle** : pour cela il faut prendre en compte plusieurs critères tels sur : le nombre de personnes concernées, volume de données, éventail des différentes données traitées, durée ou permanence de l'activité de traitement, l'étendue géographique de l'activité de traitement.
- **Croisement ou combinaison d'ensembles de données** : issus de deux opérations de traitements par exemple ou effectuées à des fins différentes et/ou par différents responsables de traitement, de manière qui outrepasserait les attentes raisonnables de la personne concernée.
- **Données concernant des personnes vulnérables** : il faut prendre en compte le déséquilibre des pouvoirs existants entre les personnes concernées et le responsable de traitement : enfants, employés, personnes souffrant de maladie mentale, demandeurs d'asile, personnes âgées, patients, etc.
- **Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles** : utilisation combinée, par exemple, de systèmes de reconnaissance des empreintes digitales et de reconnaissance faciale pour améliorer le contrôle des accès physiques.
- **Traitements en eux-mêmes qui empêchent les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat** : il s'agit notamment des traitements qui incluent les opérations visant à autoriser, modifier ou refuser l'accès à un service ou la conclusion d'un contrat.

Le Groupe Siaci Saint Honoré met et mettra en œuvre une Etude d'Impact sur la Vie Privée dès lors que deux critères, a minima, seront remplis. Cependant, le DPO pourra décider qu'une telle étude soit

¹³ Le G29 ou Groupe de travail Article 29 sur la protection des données est un organe consultatif européen indépendant sur la protection des données et de la vie privée. Le G29 va devenir le Comité Européen de Protection des Données à partir du 25 mai 2018 (art. 68 et s. RGPD).

réalisée alors qu'un seul critère n'est rempli et cela pour des raisons telles que, par exemple, la présence d'une chaîne de sous-traitance ou d'un transfert hors UE difficilement encadrés, etc.

5.4 Sécurité des traitements

Comme indiqué dans **la PSSI du Groupe**, la sécurité d'un système d'information est l'état de protection, face aux risques identifiés, résultant de l'ensemble des mesures générales et particulières prises pour assurer : la confidentialité, la disponibilité et l'intégrité des données à caractère personnel.

Le Groupe Siaci Saint Honoré s'engage à traiter les données à caractère personnel de façon à garantir une sécurité appropriée des données, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque¹⁴.

En ce sens, la **PSSI du Groupe** détermine les mesures générales applicables au Système d'Information.

L'ensemble des traitements de données à caractère personnel réalisés au sein du Groupe Siaci Saint Honoré, doit respecter des règles de protection¹⁵ visant leurs :

- Sécurité physique : mesures destinées à limiter, contrôler l'accès aux endroits où sont stockées les données aux seules personnes habilitées ainsi que prévenir et protéger les données à caractère personnel contre les agressions accidentelles ou volontaires telles incendie, dégâts des eaux, etc.
- Sécurité logique : mesures destinées à limiter et contrôler l'accès aux Systèmes d'Information, y compris de télécommunications, aux seules personnes habilitées.

La **PSSI du Groupe** indique que l'utilisation de techniques de chiffrement ou de procédés cryptologiques n'est pas envisagé sans l'aval du ITRM. Ce document détaille également les mesures de sécurité appliquées au Système d'Information Siaci Saint Honoré.

L'utilisateur est d'ailleurs informé de l'existence d'une traçabilité mise en place afin de sécuriser l'activité et les Systèmes d'Information du Groupe. En effet, l'ensemble des bases de données du Groupe Siaci Saint Honoré dispose d'une solution permettant la journalisation et la traçabilité des accès. Cela permet de déterminer quel collaborateur a eu accès à la base de données, les actions réalisées et à quel moment.

La PSSI du Groupe indique que les Directives, d'une part, relative à la Journalisation et analyse des journaux des équipements réseaux et télécoms et d'autre part, relative à l'analyse des logs et journaux systèmes, encadrent la traçabilité des accès aux données.

5.5 Le cas particulier du NIR et des données de santé

Pour les activités de santé, retraite et prévoyance, les articles R115-1 et R115-2 du code de la Sécurité Sociale autorisent le Groupe à collecter et à utiliser le NIR. Toutefois, cette autorisation ne vaut que pour les traitements effectués dans l'exercice des activités d'assurance maladie, maternité, invalidité et assurance vieillesse complémentaire menées par le Groupe.

¹⁴ Art. 32 RGPD et Art. 34 Loi « Informatique et Libertés ».

¹⁵ Art. 24 RGPD et Art. 34 Loi « Informatique et Libertés ».

Le NIR est collecté pour tous les assurés qui bénéficient d'une complémentaire santé pour permettre la mise en place d'un lien automatique entre les différentes Caisses Primaires d'Assurance Maladie (CPAM) de France et les services du Groupe. Le but est de structurer et d'automatiser le circuit des remboursements de santé dans un souci d'efficacité et de rapidité.

Concernant les données de santé, le Groupe s'est organisé de manière à préserver la confidentialité de ces données et à respecter les recommandations des conventions Belorgey et AERAS. L'organisation et les principes applicables en la matière sont disponibles en interne dans un document relatif au secret médical. De plus, l'hébergeur choisi par le Groupe est certifié « Hébergement Données de Santé ».

5.6 Les droits des personnes concernées

Toute personne physique qui figure dans les traitements de données du Groupe dispose de différents droits octroyés par le droit national et le droit de l'Union européenne. Ceux-ci doivent être respectés et leur mise en œuvre doit être effective.

Ainsi, ces personnes physiques disposent d'un **droit d'accès**¹⁶ et d'un **droit de rectification**¹⁷ afin d'obtenir du responsable du traitement : la confirmation que des données la concernant sont ou ne sont pas traitées ou bien la rectification des données personnelles la concernant qui seraient inexactes. Les personnes concernées peuvent également donner des directives relatives à la conservation, à l'effacement et à la communication de leurs données après leur décès. Il s'agit de la **possibilité d'organiser le sort de ses données personnelles après la mort**¹⁸.

Toute personne physique dispose du **droit à l'effacement**¹⁹ qui est le droit d'obtenir l'effacement, dans certaines conditions, de données personnelles la concernant.

Toute personne physique dispose aussi d'un droit à la **limitation**²⁰ et **d'opposition**²¹ au traitement.

Les personnes sont titulaires du **droit à la portabilité**²² qui est le droit pour la personne concernée de recevoir, dans certaines conditions « dans un format structuré, couramment utilisé et lisible par machine »²³, l'intégralité de ses données pour qu'elle puisse les transférer à un autre prestataire.

Enfin, toute personne physique a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le **profilage**²⁴, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

Le responsable de traitement doit répondre à la demande de la personne concernée d'exercer les droits que lui confèrent le RGPD et la Loi « Informatique et Libertés ». Le responsable de traitement doit fournir à la personne concernée les informations dans les meilleurs délais et en tout état de cause dans un **délai d'un (1) mois à compter de la réception de la demande**²⁵. Ce délai peut être porté à deux (2) mois si la demande est complexe. Dans ce dernier cas, il sera essentiel de démontrer la complexité de la demande.

¹⁶ Art. 15 RGPD et Art. 40 Loi « Informatique et Libertés ».

¹⁷ Art. 16 RGPD et Art. 40 Loi « Informatique et Libertés ».

¹⁸ Art. 32, I, 6° Loi « Informatique et Libertés ».

¹⁹ Art. 17, 1 RGPD et Art. 40 Loi « Informatique et Libertés ».

²⁰ Art. 18,1 RGPD.

²¹ Art. 21 RGPD et 28 Loi « Informatique et Libertés ».

²² Art. 20,1 RGPD ; Art. 48 Loi du 16 octobre 2016 et Art. L 224-42-1 et s. C.Conso.

²³ **Art. 20 RGPD.**

²⁴ Art. 22 RGPD.

²⁵ Art. 12,3° RGPD. La Loi « Informatique et Liberté » prévoyait un délai de deux (2) mois pour répondre.

Le Groupe a mis en place une **Procédure de gestion des demandes d'exercice des droits des personnes concernées** ainsi qu'un **Mode opératoire** dédié. La Procédure de gestion des données personnelles, quant à elle, décrit en détail les conditions générales applicables dès réception de toute demande et les conditions spécifiques applicables à un type déterminé de demande. Le Mode opératoire a vocation à déterminer rapidement comment mettre en œuvre concrètement la demande de la personne concernée dans les délais légaux.

L'ensemble de ces documents est disponible en interne auprès du DPO du Groupe et l'ensemble des salariés y a accès via l'intranet personnel. Une diffusion régulière est également réalisée.

Le DPO tient et met à jour régulièrement un tableau des demandes permettant d'historiser les demandes d'exercice des droits des personnes et les réponses qui y sont apportées.

L'ensemble des demandes réalisées par les personnes concernées doit impérativement être transmis au DPO du Groupe et traitée par ce dernier et de ses collaborateurs. Pour permettre cela, le DPO est joignable par mail (à l'adresse suivante : dpo@s2hgroup.com). Un formulaire de transmission des demandes d'exercice des droits par les personnes concernées (ANNEXE 3 et ANNEXE 4) est mis à disposition des opérationnels pour faciliter la transmission des demandes. Ce formulaire, une fois transmis au DPO, permettra d'adapter sa réponse à la personne concernée.

5.7 Transferts de données à caractère personnel

Le Groupe Siaci Saint Honoré réalise son activité sur deux types de zones géographiques :

- Sur le territoire de l'Union européenne ;
- En dehors du territoire de l'Union européenne.

Le transfert, l'importation ou l'exportation de données à caractère personnel, en dehors des traitements gérés dans le SI Groupe, ne peuvent être réalisés que dans le cadre d'une instruction préalable, expresse et écrite du supérieur hiérarchique de l'utilisateur et en conformité avec les déclarations ou autorisations et l'information des personnes concernées décidés par le Groupe.

Un transfert de données à caractère personnel²⁶ est possible à condition que :

- Le pays vers lequel le transfert a lieu assure un **niveau de protection adéquat** reconnu par la Commission Européenne par le biais d'une décision d'adéquation²⁷ ;
- Le responsable de traitement a prévu des **garanties appropriées** et les personnes concernées informées du transfert, disposent de droits opposables et de voies de droit effectives²⁸. Les garanties appropriées peuvent être, entre autres, la mise en place de règles d'entreprises contraignantes²⁹ (ou B.C.R.), des clauses types adoptées par la Commission Européenne, les clauses types adoptées par une autorité de contrôle et approuvées par la Commission Européenne ou encore un mécanisme de certification approuvé. Avec autorisation de la CNIL, il est également possible de mettre en place des clauses contractuelles entre le responsable de traitement ou le sous-traitant et le responsable de traitement, le sous-traitant ou le destinataire des données.

Le Groupe Siaci Saint Honoré accorde une vigilance importante à l'ensemble de ses transferts de données à caractère personnel en dehors de l'Union européenne.

La **PSSI** indique que les échanges des informations sont encadrés par les Directives relatives à l'envoi de supports informatiques et aux échanges d'informations par messagerie électronique.

²⁶ Art. 44, 45, 46, 47 et s. RGPD.

²⁷ Art. 45 RGPD.

²⁸ Art. 46 RGPD.

²⁹ Art. 47 RGPD.

Les demandes d'autorisation nécessaires ont été réalisées auprès de la CNIL et sont disponibles auprès du DPO du Groupe.

5.8 Sous-traitance

Le RGPD apporte une vigilance particulière concernant le recours à la sous-traitance.

Le Groupe Siaci Saint Honoré, dans le cadre de contrats conclus avec des sous-traitants³⁰ amenés à traiter des données à caractère personnel pour son compte (ou d'une entité du Groupe), veille à ce que soit précisé dans le contrat :

- Que le sous-traitant est informé du fait que ces données et fichiers sont soumis au respect de la législation applicable à la protection des données et relève de la vie privée et du secret professionnel ;
- Et qu'il s'engage à mettre en place toutes les procédures ou mesures nécessaires pour en assurer la sécurité et la confidentialité.

Le Groupe veille à ce que le sous-traitant présente des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité et l'ensemble des contrats de sous-traitance, contient une clause relative à la protection des données personnelles déterminant la responsabilité de chacun des acteurs.

Selon **la PSSI du Groupe**, une convention de service est établie entre Siaci Saint Honoré et ses hébergeurs. Cette convention précise les engagements de l'exploitation vis-à-vis des besoins et exigences exprimés par la maîtrise d'ouvrage lors de la mise en production. Elle décrit donc le niveau de secours, la sécurité physique et logique, les tâches d'exploitation prévues et les plages d'astreinte, la disponibilité requise et les mesures conservatoires.

5.9 Contrôle

Outre les contrôles de conformité qui peuvent être menés en interne, la CNIL peut avoir accès, de 6 heures à 21 heures, pour l'exercice de ses missions, aux lieux et locaux servant à la mise en œuvre des traitements de données à caractère personnel³¹.

Elle peut demander la communication de tous les documents nécessaires à l'accomplissement de sa mission, quel qu'en soit le support, en prendre copie, accéder aux programmes informatiques et aux données.

Toutefois, seul un médecin peut requérir la communication de données de santé.

Le Groupe Siaci Saint Honoré s'engage, en cas de contrôle de la CNIL, à coopérer avec cette dernière.

5.10 Protection des données dès la conception des projets et au plus haut niveau de protection³²

Afin de pouvoir assurer la conformité du Groupe Siaci Saint Honoré en matière de protection des données, le DPO doit impérativement être consulté dès l'initialisation de tout projet impliquant des traitements de données à caractère personnel.

Il convient donc pour tout utilisateur, en charge d'un nouveau projet entrant dans ce périmètre, de consulter le DPO. Pour cela, le Groupe a mis en place un formulaire « Nouveau Projet » (en ANNEXE 1) permettant aux équipes en charges des nouveaux projets de faire prendre connaissance au DPO du projet en question pour que ce dernier puisse les conseiller.

³⁰ Art. 4, 8° RGPD : le sous-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* ».

³¹ Art. 11-2° - f et 44 de la Loi « Informatique et Libertés ».

³² Art. 25 RGPD.

5.11 Gestion des violations de données

En cas d'incident de sécurité, Siaci Saint Honoré a mis en place une Procédure de gestion des incidents de sécurité permettant de détecter, d'évaluer et de répondre à une violation de données par exemple.

Selon la **PSSI du Groupe**, la procédure de gestion des incidents permet de réagir à bon escient et de transmettre l'information. Le système de gestion des incidents mis en place, compte :

- Des systèmes de détection des incidents ;
- Des processus de *reporting* et de traitement après la découverte d'un incident jusqu'à la gestion de crise ;
- Une consolidation d'une base d'information ;
- Un système de suivi et un tableau de bord.

Le Groupe a également mis en place un Plan de Continuité de Service en cas d'indisponibilité critique de tout équipement. Ces solutions sont décrites dans les documents intitulés « Plan de Continuité d'Activité » ou « Plan de Reprise d'Activité » et incluent les règles de déclenchement, les actions à mener, les priorités, les acteurs à mobiliser et leurs coordonnées.

5.12 Le sort des données après réalisation de la prestation

En tant que responsable de traitement, le Groupe Siaci Saint Honoré met en œuvre la suppression des données de manière régulière et selon les exigences légales.

En tant que sous-traitant, le Groupe Siaci Saint Honoré s'engage à ne traiter les données que sur instruction documentée du Client. Selon le choix de ce dernier, le Groupe s'engage également à supprimer toutes les données ou à les renvoyer au Client au terme de la prestation de services relatifs au traitement ainsi qu'à détruire les copies existantes.

6. EXAMENS DE CONFORMITE PERIODIQUES

Le Groupe Siaci Saint Honoré est amené à réaliser deux types d'audits :

- En interne dans le cadre du plan d'audit interne pluriannuel. La fonction audit interne du Groupe Siaci Saint Honoré est une activité indépendante et objective qui donne à l'organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte des conseils pour les améliorer et contribue à créer de la valeur ajoutée. La fonction audit interne aide le Groupe Siaci Saint Honoré à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de gouvernance, de management des risques et de contrôle, en faisant des propositions pour renforcer leur efficacité. La mise en œuvre de l'audit interne est décrite dans la **Charte d'audit interne S2H Groupe 2017**.
- Chez les sous-traitants dans le cadre de leurs relations contractuelles afin de vérifier que les principes applicables à la protection des données à caractère personnel sont bien respectés.

Le Groupe met à la disposition du Client toutes les informations nécessaires pour démontrer le respect des obligations prévues par la législation applicable à la protection des données à caractère personnel. Le Groupe Siaci Saint Honoré s'engage également à permettre la réalisation d'audits par le Client ou un autre auditeur qu'il a mandaté, et contribuer à ces audits dans les conditions suivantes : un (1) audit par année calendaire dont la demande aura été exposée minimum quinze (15) jours avant la date de réalisation de l'audit.

Concernant les audits des systèmes d'information, la **PSSI du Groupe** indique qu'ils sont planifiés et approuvés de façon à minimiser les risques de perturbation des processus professionnels. L'accès aux outils d'audit des systèmes est protégé afin d'empêcher toute compromission ou toute utilisation abusive éventuelle.

ANNEXE 1

FORMULAIRE « NOUVEAU PROJET »

1. Informations générales relatives au nouveau projet

- *Titre* : _____
- *Date du nouveau projet* : _____
- *Personne en charge* : _____
- *Service / Département* : _____
- *Date de transmission du DPO* : _____

2. Informations spécifiques relatives au nouveau projet :

- *Date souhaitée de mise en production* : _____/_____/_____
- ***Types de données personnelles concernées*** :
 - Etat-civil identité (nom, prénom, mail, image) : _____
 - Vie personnelle (habitudes de vie, situation familiale) : _____
 - Vie professionnelle (CV, scolarité, formation) : _____
 - Informations d'ordre économique et financier (revenus, situation fiscale) : _____
 - Données de connexion, cookies (adresse IP, logs) : _____
 - Données de localisation (déplacements, données GPS) : _____
 - Autres : _____
- ***Présence de données sensibles ?***
 - Non
 - NIR = Numéro de sécurité sociale
 - Données de santé : _____
 - Données concernant la vie sexuelle ou l'orientation sexuelle : _____
 - Données relatives aux condamnations pénales : _____
 - Données biométriques aux fins d'identifier une personne physique de manière unique : _____
 - Données génétiques : _____
 - Données révélant l'appartenance syndicale : _____
 - Données révélant les convictions religieuses ou philosophiques : _____

Données révélant les opinions politiques : _____

Données révélant l'origine raciale ou ethnique : _____

- **Type de collecte :**

Directement auprès de la personne concernée

Indirectement (utilisation d'une autre BDD, achat d'un fichier, ...) : _____

- **Type de personnes concernées :**

Salariés

Usagers

Visiteurs

Adhérents

Clients (actuels)

Prospects (potentiels futurs clients)

Autres : _____

- **Utilisation d'une technologie particulière :**

Dispositif sans contact (RFID) : _____

Mécanisme d'anonymisation : _____

Mécanisme de pseudonymisation : _____

Carte à puce : _____

Géolocalisation : _____

Vidéoprotection : _____

Nanotechnologies : _____

Profilage : _____

Autre : _____

- **Durée de conservation prévue :**

1 mois

2 mois

3 mois

Pendant la durée de la relation contractuelle

Illimitée

Autre : _____

- **Une suppression définitive est-elle possible à l'issue de ce délai ?**

Oui : _____

Non : _____

- **Un processus d'archivage ou de suppression automatique est-il prévu ?**

• Oui : _____

• Non : _____

- **Destinataire(s) des données :**

Autre Département / Service de S2H Groupe : _____

Prestataire / Fournisseur : _____

Filiale / Autre entité du Groupe : _____

Personnes concernées par le traitement : _____

Autre : _____

- **Sécurité du traitement :**

Accès physique au traitement est protégé

Procédé d'authentification des utilisateurs mis en œuvre

Journalisation des connexions

Traitement réalisé sur un réseau interne dédié (non relié à internet)

Autre : _____

- **Transferts de données hors UE :**

Oui :

o Vers quel pays ? _____

o Le transfert est-il sécurisé ? Si oui, comment ? _____

Non

- **Droit des personnes concernées :**

- *Les personnes seront-elles informées du traitement ?*

Oui. Comment ? _____

Non

- *Pourront-elles donner leur consentement ?*

Oui. Comment ? _____

Non. Pourquoi ? _____

- *La mise en œuvre des droits des personnes concernées est-elle prévue (accès, rectification, portabilité, suppression, ...) ?*

Oui. Comment ? _____

Non : _____

3. **Acteurs de consultation :**

DRC _____ le ___/___/___

DJ : _____ le ___/___/___

DSI : _____ le ___/___/___

DG : _____ le ___/___/___

ANNEXE 2

LES DIFFERENTES BASES JURIDIQUES D'UN TRAITEMENT DE DONNEES A CARACTERE PERSONNEL

L'article 6, 1 du RGPD définit les différentes bases légales qui permettent au responsable de traitement de mettre en œuvre un traitement de données à caractère personnel de manière licite :

1. Le **consentement** spécifique et éclairé de la personne concernée par le traitement ;
2. Le traitement est nécessaire à l'**exécution d'un contrat** auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci (ex : données nécessaires pour réaliser un contrat d'assurance) ;
3. Le traitement est nécessaire au **respect d'une obligation légale** à laquelle le responsable de traitement est soumis (exemple : obligations de lutte contre le blanchiment et le financement du terrorisme) ;
4. Le traitement est nécessaire à la **sauvegarde des intérêts vitaux** de la personne concernée ou d'une autre personne physique (ex : la santé de la personne concernée ou d'une autre personne est en jeu) ;
5. Le traitement est nécessaire à l'**exécution d'une mission d'intérêt public** ou relevant de l'autorité publique dont est investi le responsable du traitement ;
6. Le traitement est nécessaire aux fins d'**intérêts légitimes** poursuivis par le responsable du traitement ou par un tiers (étude de proportionnalité des intérêts du responsable de traitement et de la personne concernée).

ANNEXE 3

**FORMULAIRE DE TRANSMISSION D'UNE DEMANDE D'EXERCICE DES
DROITS PAR UNE PERSONNE CONCERNEE (INTERNE)**

Informations sur la personne ayant reçu la demande :

- Demande reçue le : ____/____/_____, à ____H____
- Demande reçue par :
- Entité :
- Service :

Informations sur la personne concernée :

- Nom :
- Prénom :
- Adresse postale :
- Téléphone :
- Adresse mail :
- Autre information mentionnée :

Informations sur la demande :

- **Type de demande** (cochez la demande exercée par la personne – possibilité qu'il y ait plusieurs choix – et indiquer si la personne concernée a précisé sa demande)
 - Demande d'accès :
 - Demande de rectification :
 - Demande de suppression / effacement :
 - Demande de portabilité :
 - Demande de limitation du traitement :
 - Demande d'opposition au traitement :
 - Demande d'organisation de directives après le décès :
- **Transmission de la demande au DPO S2H Groupe le :** ____/____/_____, à ____H____

Nom et signature de la personne ayant reçu la demande

ANNEXE 4

**FORMULAIRE DE TRANSMISSION D'UNE DEMANDE D'EXERCICE DES
DROITS PAR UNE PERSONNE CONCERNEE AU RESPONSABLE DE TRAITEMENT : Société X (EXTERNE)**

Informations sur la personne ayant reçu la demande :

- Demande reçue le : ____/____/_____, à ____H____
- Demande reçue par :
- Entreprise : **Société X**
- Service :
- Qualité (prestataire de service, fournisseur, développeur, hébergeur, ...) :
- Responsable de traitement :

Informations sur la personne concernée :

- Nom :
- Prénom :
- Adresse postale :
- Téléphone :
- Adresse mail :
- Autre information mentionnée :

Informations sur la demande :

- **Type de demande** (cochez la demande exercée par la personne – possibilité qu'il y ait plusieurs choix – et indiquer si la personne concernée a précisé sa demande)
 - Demande d'accès :
 - Demande de rectification :
 - Demande de suppression / effacement :
 - Demande de portabilité :
 - Demande de limitation du traitement :
 - Demande d'opposition au traitement :
 - Demande d'organisation de directives après le décès :
- **Transmission de la demande au DPO S2H Groupe le :** ____/____/_____, à ____H____

Nom et signature de la personne ayant reçu la demande