HES - POLITIQUE D'ÉVALUATION DE L'IMPACT DE LA PROTECTION DES DONNÉES

1. Introduction

Voici la Politique de HES International B.V. (« **HES** ») d'évaluation de l'impact de la protection des données, ou « **Politique DPIA** » (*data protection impact assessment policy*). Au sens de la présente Politique DPIA, Données personnelles désigne toute information liée à une personne vivante identifiable. Cette définition est très large et englobe presque toutes les informations (du nom de la personne à son numéro de téléphone portable) dans la mesure où elles sont liées à un individu vivant pouvant être identifié. De plus, Traitement signifie collecte, stockage, analyse, utilisation, divulgation, archivage, effacement ou toute autre action affectant les Données personnelles.

2. Qu'est-ce que l'évaluation de l'impact de la protection des données ?

La loi, dans certaines circonstances, oblige HES (en tant que Responsable de traitement) à procéder à une évaluation (une « **DPIA** ») de l'impact et des risques potentiels que son Sous-traitant envisagé peut avoir ou faire peser sur les personnes concernées, en particulier lorsqu'il procède à un traitement potentiellement très risqué, ou en vrac, de Données personnelles. Les responsables du traitement doivent : (i) décrire le traitement, (ii) expliquer le cas échéant les raisons de ce traitement, (iii) évaluer la nécessité et la proportionnalité de ce traitement, avec pour les personnes concernées les risques résultant du traitement de leurs Données personnelles.

Une DPIA doit identifier efficacement, puis résoudre tout domaine de préoccupation à un stade précoce, et toujours avant le début du traitement.

L'utilisation systématique et prescrite de la DPIA chez HES dans son ensemble fait partie intégrante de son programme de conformité en démontrant que HES a soigneusement et convenablement envisagé tout risque réel ou potentiel présenté par son traitement.

Une DPIA est un outil essentiel, tant pour garantir la conformité au RGPD que pour faire la démonstration de cette conformité. Le cadre de la DPIA est un élément important de la conformité au « principe de responsabilité » plus général imposé par le RGPD.

3. Quand une DPIA est-elle requise ?

Vous (en tant que chef de projet ou délégué du chef de projet) devez conduire une DPIA : (i) lorsqu'un nouveau système informatique ou autre dispositif (qu'il soit de nature technique ou autre) impliquant le traitement de Données personnelles (un « **Système de traitement** ») doit être mis en œuvre au sein ou au nom de HES, ou (ii) lorsqu'une modification significative doit être apportée à un Système de traitement existant.

Il convient de faire particulièrement attention lorsque le Système de traitement peut déboucher sur un risque élevé pour la vie privée des personnes concernées visées. Par exemple, lorsque le Système de traitement :

- surveille systématiquement les individus ;
- traite des Données personnelles à grande échelle ;
- utilise des solutions techniques nouvelles ou novatrices ;
- manipule des Données hautement personnelles ou sensibles ; ou
- implique l'engagement d'un nouveau fournisseur.

4. Que dois-je faire ?

Vous devez :

- veiller à ce qu'il soit tenu compte des exigences de la présente Politique DPIA et des droits à la vie privée des personnes concernées dans la sélection, la conception et la mise en œuvre du Système de traitement modifié ou nouveau, et en particulier :

  (a) conserver les Données personnelles à traiter par le Système de traitement au niveau minimum requis pour satisfaire aux exigences professionnelles de HES ; et

  (b) lorsque des Données personnelles doivent être traitées et s'il est raisonnablement faisable et cohérent de le faire pour HES, conserver les Données permettant l'identification des personnes concernées séparément des autres éléments de ces Données personnelles traitées et les protéger efficacement, afin que les personnes concernées ne soient identifiables que si cela est nécessaire pour la réalisation des objectifs commerciaux de HES ; et

- considérer les exigences de la présente Politique DPIA et de la Politique de confidentialité de HES pour le traitement des Données personnelles par HES dans ce Système de traitement et ses implications pour la vie privée des personnes concernées. Vous devez vous assurer qu'à la suite de la mise en œuvre ou du changement, le Système de

traitement sera conforme aux principes exposés dans la présente Politique DPIA et dans le politique de HES en matière de vie privée à tous les égards et que cette mise en œuvre ne se traduira pas par des risques élevés qu'il ne serait pas possible de limiter pour les personnes concernées.

5. Une DPIA doit-elle être conduite ?

Ayant considéré les implications de la présente Politique DPIA et de la Politique de confidentialité de HES pour le traitement des Données personnelles par HES dans ce Système de traitement et ses implications pour la vie privée des personnes concernées, vous devrez décider de la nécessité de conduire une DPIA.

Si vous n'êtes pas certain de l'applicabilité des principes de la présente Politique DPIA ou de la Politique de confidentialité de HES ou si vous pensez que la mise en œuvre du Système de traitement nouveau ou modifié peut entraîner des risques pour la vie privée des personnes concernées visées, vous devez envoyer au Compliance Officer local des explications suffisamment détaillées sur le Système de traitement nouveau ou modifié, accompagnées d'un résumé de votre évaluation ou demande et de votre raisonnement en remplissant la Partie C de l'Annexe 1 (un « **Avis initial** »).

À réception de cet Avis initial, le Compliance Officer local déterminera si une DPIA est requise et vous informera de sa décision. Si le Compliance Officer local décide qu'une DPIA est nécessaire, vous devrez suivre ses instructions, y compris remplir le Formulaire DPIA ci-joint dans la Partie D de l'Annexe 1 pour examen par le Compliance Officer local (Le « **Formulaire DPIA** »).

Un nouveau Système de traitement ne doit pas être mis en œuvre au sein ou au nom de HES et aucun changement ne doit être effectué sur un Système de traitement existant, si l'évaluation visée aux sections 4 et 5 n'a pas été conduite et :

- soit (i) vous avez pris en considération les principes de la présente Politique DPIA et de la Politique de confidentialité de HES en matière de vie privée et pensez qu'ils seront entièrement respectés et (ii) vous ne pensez pas que la mise en œuvre du Système de traitement nouveau ou modifié entraînera des risques élevés pour la vie privée des personnes concernées visées ; soit
- vous avez envoyé au Compliance Officer local un Avis initial et il vous a répondu qu'une DPIA complète n'était pas requise ; ou
- vous avez conduit une DPIA complète sur instruction du Compliance Officer local et ce dernier vous a confirmé que le Système de traitement nouveau ou modifié pouvait être mis en œuvre.

6. Vos obligations découlant de la présente politique

Nous souscrivons à nos obligations en matière de protection de Données et confidentialité et les prenons très au sérieux. Dans le cadre de vos devoirs envers nous, nous vous demandons de faire

de même. Ne pas s'acquitter de ces devoirs et/ou ne pas respecter la présente Politique peut constituer une infraction disciplinaire et se traduire par un licenciement.

7. Questions

Pour toute question relative à la présente Politique ou en cas de doute au sujet de ses exigences, n'hésitez pas à contacter le Chief Compliance Officer (compliance@hesinternational.eu).

ANNEXE 1

Modèle de Formulaire d'évaluation de l'impact sur la confidentialité des données

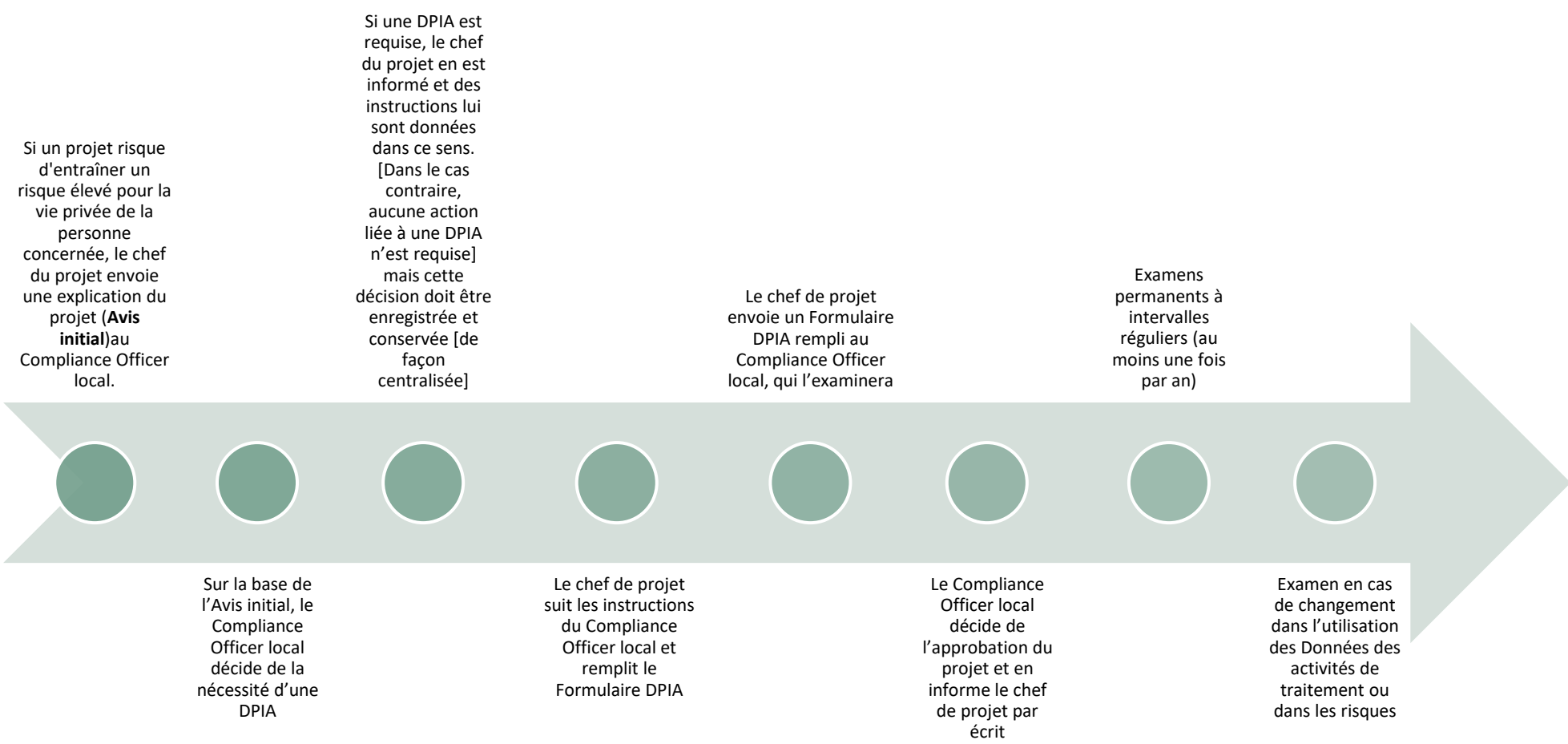
Partie A : Introduction

Les définitions des termes utilisés dans cette Annexe 1 se trouvent dans la Partie E (*Glossaire*) ci-jointe.

La Partie B propose un diagramme récapitulatif du processus de DPIA. La Partie C pose plusieurs questions préliminaires visant à établir la nature du projet et la nécessité d'une DPIA (« L'**Avis initial** »). La Partie D est le Formulaire DPIA, qui contient une série de questions sur le projet proposé et l'utilisation qu'il entend faire des informations personnelles (le « **Formulaire DPIA** »).

Avertissement : Le Formulaire DPIA ne prévoit pas la situation dans laquelle le responsable de traitement doit consulter l'Autorité de surveillance de la protection des données. Cela doit être dirigé par le **Service juridique**.

Partie B : Aperçu du Processus DPIA



Partie C : Questions préliminaires pour déterminer si une DPIA est nécessaire ; dans l'affirmative, modalités d'exécution de l'évaluation (« Avis initial »)

Informations générales sur le projet

Question	Réponse
[*Entité HES concernée*] demandant/entreprenant le projet.	
Coordonnées du chef de projet.	Nom : Fonction : Téléphone : Courriel :
Votre projet impliquera-t-il le traitement de Données personnelles – dans la négative, aucune autre action n'est requise. Veuillez envoyer ce Formulaire au Compliance Officer local pour examen et approbation.	
Veuillez fournir le plus possible de détails sur la façon dont votre projet impliquera le traitement de Données personnelles.	
HES traitera-t-elle des Donnés personnelles en tant que responsable de traitement ou en tant que Sous-traitant ? Expliquez pourquoi dans chaque cas.	
Quel est le but du projet ?	
Quels sont les avantages pour HES ?	

Quels sont les avantages potentiels pour les autres Parties (y compris les clients de HES et les individus affectés, dans la mesure où ils s'appliquent) ?	
Existe-t-il des documents revêtant de l'importance pour le projet, comme une proposition de projet, pouvant avoir une utilité aux fins de la présente DPIA – par exemple, expliquant comment les Données personnelles seront utilisées ? Si tel est le cas, veuillez joindre la liste au présent Formulaire.	
À quelle date le projet sera-t-il mis en œuvre ?	

Le projet et les Données personnelles

Question	Oui/Non	Risque pour la vie privée
Le projet impliquera-t-il la collecte de Données personnelles sur des individus ?		Faible à moyen
Le projet exigera-t-il des individus qu'ils fournissent des informations sur leur personne dans le cadre des prestations de service de traitement ou cela sera-t-il volontaire ?		Moyen
Comment les individus seront-ils notifiés/informés ?		Moyen

Les Données personnelles seront-elles divulguées ou stockées au sein de l'organisation de HES, ou de Tiers, d'une façon inédite ?		Moyen
Les Données personnelles seront-elles utilisées à des fins nouvelles ou différentes ?		Faible à moyen
Le projet implique-t-il l'utilisation de nouvelles technologies ?		Moyen à élevé
Le projet débouchera-t-il sur la prise de décisions ou de mesures à l'encontre d'individus pouvant avoir un impact significatif sur leur personne (en établissant par exemple leur profil) ?		Élevé
Le projet impliquera-t-il un quelconque processus de décision automatisé ou le profilage d'individus ?		Élevé
Le projet impliquera-t-il le traitement à grande échelle de Données personnelles ?		Moyen à élevé
Le projet impliquera-t-il le traitement à grande échelle d'une catégorie spéciale de Données ou de Données sur des condamnations pénales ou des infractions ?		Élevé

Y aura-t-il un traitement transfrontalier ?		Élevé

Résumé

Question	O/N
Sur la base des informations et réponses qui précèdent, est-il possible de conclure que le traitement des Données personnelles est susceptible d'entraîner des risques élevés pour les personnes concernées ou de constituer une activité de traitement risquée ?	
Si la réponse à la question précédente est non, veuillez donner les raisons détaillées de cette conclusion et retourner ce Formulaire au Compliance Officer local pour approbation.	
Si la réponse est oui, veuillez passer à la section suivante.	

Partie D : Formulaire d'évaluation de l'impact sur la confidentialité des données (« Formulaire DPIA »)

#	Question	Réponse
Les Données personnelles		
1.	Quelles Données personnelles seront-elles collectées ? (Veuillez encercler l'option O/N correspondante)	Nom : O / N Adresse : O / N Date de naissance : O / N Origine raciale ou ethnique : O / N État civil : O / N Informations sur la famille et les relations : O / N Religion : O / N Informations sur la santé : O / N Orientation sexuelle : O / N Opinions politiques : O / N Informations génétiques : O / N Informations sur les condamnations pénales : O / N Informations sur les caractéristiques physiques (hauteur, poids, etc.) : O / N Carte de crédit / numéro de compte bancaire : O / N Informations sur la propriété (véhicules, maisons, appartements, biens personnels) : O / N Historique de crédit : O / N Informations sur les réseaux sociaux : O / N Autre (veuillez préciser) : O / N
2.	Comment les Données sont-elles collectées ?	

#	Question	Réponse
3.	Quelle est l'activité de traitement ?	
4.	Ce traitement est-il nécessaire ou l'activité pourrait-elle être conduite de façon différente ?	
5.	Le projet pourrait-il encore être entrepris avec des chances de succès sans la collecte de l'ensemble ou d'une partie de ces Données personnelles ?	
6.	Quelles personnes peuvent-elles faire l'objet de la collecte / du traitement de Données personnelle ? (Veuillez encercler l'option O/N correspondante)	Collaborateurs : O / N Non-collaborateurs : O / N S'il ne s'agit pas de collaborateurs, spécifiez de qui il s'agit (clients, fournisseurs, autres Tiers, etc.) :
7.	Dans quel but spécifique les Données personnelles seront-elles traitées (par exemple pour l'exploitation d'un nouveau portail sur les avantages sociaux des collaborateurs) ? Donnez le plus possible de détails sur les raisons du traitement de l'information.	
8.	Combien de temps les Données personnelles seront-elles stockées ?	
La base légale		
9.	Les Données personnelles seront-elles traitées sur la base du consentement de la personne concernée ? Si oui, comment ce consentement est-il obtenu ?	
10.	Les Données personnelles seront-elles traitées dans le cadre de l'exécution	

#	Question	Réponse
	d'un contrat avec les personnes concernées visées ?	
11.	Les Données personnelles seront-elles traitées sur la base d'un intérêt professionnel légitime de HES (par exemple l'administration interne des ressources humaines) ?	
12.	Les Données personnelles seront-elles traitées sur le base d'une autre justification juridique (voir la Partie F pour une liste des justifications licites) ?	
Les flux d'information		
13.	Après la collecte des Données personnelles des personnes concernées, où ces données sont-elles stockées ?	
14.	Qui aura accès aux Données personnelles ?	
15.	Des rapports seront-ils générés exigeant l'utilisation et la divulgation de Données personnelles ?	
16.	Les Données personnelles seront-elles transférées à une quelconque entité étrangère à HES ? Si oui, à quelles entités et dans quels buts ?	
17.	Les Donnés personnelles seront-elles transférées à l'étranger ou accessibles pour de quelconques personnes résidant hors de l'Espace économique européen ?	

#	Question	Réponse
18.	Une cartographie des Données personnelles a-t-elle été entreprise ?	
19.	Si la réponse à la question (18) est « Oui », veuillez fournir une carte des Données personnelles illustrant les flux de Données personnelles impliquées dans ce projet. (Indication du type de Données, entités entre lesquelles elles sont partagées, localisation de ces entités et lieux où sont stockées les Données)	
20.	Combien de temps les Données personnelles seront-elles stockées ?	
Exigences de consultation		
21.	Qui consulterez-vous en interne sur les risques de confidentialité et de sécurité associés au projet ?	
22.	Avez-vous demandé conseil au Compliance Officer local, au Chief Compliance Officer ou au Service juridique ?	
23.	Des syndicats ou autres organisations de travailleurs doivent-ils être consultés (là où les Données des ressources humaines/collaborateurs sont impliquées) ?	

#	Question	Réponse
24.	En cas de transfert au-delà des frontières, l'approbation d'une autre juridiction doit-elle être détaillée ?	
25.	Si les réponses aux questions (23) ou (24) précédentes sont « Oui », avez-vous entrepris une consultation adéquate des parties impliquées ? Veuillez confirmer ici et détailler cette consultation, en indiquant avec qui et les dates.	
Identification des risques		
26.	Sur la base des questions qui précèdent, quels problèmes spécifiques de confidentialité avez-vous le cas échéant identifiés ? Par exemple, risque de voir une personne non autorisée accéder aux Données personnelles, par exemple : • risque de compromettre la sécurité des Données • risque de voir les individus s'opposer au traitement s'ils sont informés • risque de compromettre le maintien de l'exactitude des Données • risque que les Données personnelles soient conservées plus longtemps que nécessaire	
27.	Quel préjudice spécifique de tels risques causerait aux individus (par exemple risque de vol des Données personnelles, résultant de l'exposition des individus à la fraude et au vol d'identité) ?	

#	Question	Réponse
28.	Existe-t-il un risque spécifique de conformité ?	
29.	Existe-t-il un risque organisationnel plus général (par exemple lourdes amendes à la suite de la violation, suivies d'une couverture médiatique négative) ?	
Mesures pour sauvegarder, sécuriser et protéger les Données personnelles		
30.	À l'égard de chacun des risques identifiés ci-dessus, quelles mesures seront-elles mises en place pour sécuriser et protéger les Données personnelles (par exemple cryptage, authentification multifacteur) ?	
31.	À l'égard de chacun des risques identifiés ci-dessus, comment faciliterons-nous l'exercice des droits des personnes concernées (par exemple le droit d'accès) ?	
32.	Comment les informations appropriées seront-elles communiquées aux personnes concernées sur le projet et au besoin sur les risques y étant associés ?	
33.	Ces actions élimineront-elles la totalité du risque ou ne feront-elles que le réduire ?	

#	Question	Réponse
34.	Tenant compte des risques identifiés et des solutions proposés pour les réduire, l'impact final sur les droits à la vie privée des personnes concernées est-il considéré comme étant acceptable à la lumière des buts et des bénéfices du projet ?	
Incorporer les résultats et les mesures pour éliminer/réduire les risques identifiés		
35.	Comment ces résultats seront-ils incorporés dans le projet ?	
36.	Qui sera responsable de garantir l'intégration correcte des résultats ?	
37.	Sous quel délai ?	
38.	Quel est le processus pour les personnes concernées désireuses de discuter de leurs préoccupations en matière de vie privée en rapport avec le projet ?	

Résumé

Question	O/N
Les risques identifiés ont-ils été éliminés, réduits ou acceptés ?	
Dans la négative, le traitement ne doit pas commencer avant d'avoir fait remonter la DPIA à [•] et d'avoir ou mettre en place des mesures appropriées.	

Aval et approbation/rejet	
Chef de projet	
Nom	
Titre de la fonction	
Signature	
Date	
Représentant de l'équipe conformité (le cas échéant)	
Nom	
Titre de la fonction	
Signature	
Date	

Détermination du Compliance Officer local	
Nom	
Date	
Réponse	
Explication (le cas échéant)	

Signature	

Partie E

Glossaire

Terme	Définition
RGPD :	Le Règlement général sur la protection des données, entré en vigueur le 25 mai 2018. Le RGPD ne s'applique qu'aux Données personnelles – il n'inclut pas les Données personnelles liées aux entreprises et autres personnes non vivantes.
Responsable de traitement :	L'entreprise qui décide des buts et moyens du Traitement des Données personnelles.
Sous-traitant :	L'entreprise qui traite les Données personnelles au nom du Responsable de traitement.
Compliance Officer local	La personne au sein de l'entité de HES qui est responsable des évaluations de l'impact sur la confidentialité des Données.
Données personnelles :	Toutes les informations liées à des individus identifiables. Exemples de Données personnelles :
	A. Nom (tel que nom complet, nom de jeune fille, ou nom d'emprunt).
	B. Numéro d'identification personnelle (tel que numéro de sécurité sociale, de passeport, de permis de conduire, de compte bancaire ou de carte de crédit).
	C. Adresse (adresse physique ou courriel).
	D. Information sur un actif (tel que protocole Internet (IP) ou adresse de contrôle d'accès au support (MAC)).
	E. Numéros de téléphone (y compris de portables).
	F. Caractéristiques personnelles, y compris photo (par exemple du visage), rayons X, empreintes digitales ou autre image biométrique/modèle de Données personnelles (par exemple scan de la rétine, signature vocale, géométrie faciale).
	G. Information identifiant les possessions personnelles (telles que numéro d'immatriculation de véhicule et informations liées).

	H. Informations sur les individus étant ou pouvant être liées à un des éléments qui précèdent ; (par exemple date et/ou lieu de naissance, race, religion, activités, indicateurs géographiques, informations sur l'emploi, informations médicales, éducationnelles ou financières).
	I. Informations apparemment insignifiantes, telles que l'envoi d'un courriel par un individu à un moment particulier, ou le fait qu'un individu soit un client ou un collaborateur de HES (ou d'une autre organisation).
	J. Opinions sur un individu (telles que des opinions exprimées dans une lettre de référence ou d'appréciation).
Traitement :	Presque toutes les opérations conduites en relation avec les Données personnelles, dont :
	A. Collecte, stockage et enregistrement ;
	B. Organisation et structuration ;
	C. Adaptation et modification ;
	D. Extraction, consultation et utilisation ;
	E. Divulgation et dissémination ;
	F. Synchronisation et combinaison ; et
	G. Restriction, effacement et destruction.

Partie F

Liste des justifications légales du Traitement

- **L'individu auquel les données personnelles se rapportent a autorisé le Traitement.**
  - Cette autorisation doit être exprimée, documentée et librement donnée. Un individu doit également pouvoir retirer son autorisation. Pour plus de renseignements sur l'autorisation, veuillez consulter la Politique de confidentialité de HES.
- **Le traitement est nécessaire :**
  - en relation avec un contrat signé par l'individu ; ou
  - parce que l'individu a demandé à ce que quelque chose soit fait afin de conclure un contrat.
- **Le Traitement est nécessaire en raison d'une obligation légale applicable à votre personne (à l'exception d'une obligation contractuelle).**
  - Par exemple, les données doivent être conservées afin de satisfaire à des exigences légales, à des obligations de présentation d'informations financières où aux lois anti-fraude et anti-corruption.
- **Le Traitement est nécessaire pour protéger les « intérêts vitaux » des individus.**
  - Cette condition ne s'applique qu'en cas de vie ou de mort, par exemple lorsque le dossier médical d'un individu est communiqué à un hôpital qui le traite à la suite d'un grave accident de la route.
- **Le Traitement est conforme à la condition « d'intérêt légitime ».**
  - Les intérêts légitimes constituent le fondement juridique le plus flexible pour le Traitement mais il ne faut pas considérer que ce sera toujours le fondement le plus approprié.
  - Ils sont susceptibles d'être les plus appropriés lorsque vous utilisez les données des personnes d'une façon qu'elles peuvent considérer comme étant raisonnable et ayant un impact minimal sur leur vie privée ou lorsqu'il existe une justification impérieuse pour le traitement.
  - Trois éléments sont à la base des intérêts légitimes. Il est utile de les penser sous forme de test en trois parties. Vous devez : (i) identifier un intérêt légitime ; (ii) montrer que le traitement est nécessaire pour défendre cet intérêt ; et (iii) le comparer aux intérêts, libertés et droits individuels.
  - Les intérêts légitimes peuvent être vos propres intérêts ou les intérêts de Tiers. Il peut s'agir d'intérêts commerciaux, d'intérêts individuels ou d'avantages plus importants pour la société. Le Traitement doit être nécessaire. Si vous pouvez raisonnablement atteindre le même résultat d'une autre façon moins intrusive, les intérêts légitimes ne seront pas applicables.