

POLITIQUE DE SCI : POLITIQUE DE PROTECTION DES DONNÉES

Domaine d'activité :	Sécurité informatique et protection des données
Propriétaire (nom et fonction) :	Deborah McManamon, déléguée à la protection des données
Approuvé par :	Gareth Packham, directeur de la sécurité informatique et de la protection des données
Date d'approbation :	Octobre 2022
Version :	V5.0
Date de la prochaine révision :	Octobre 2023
Langues (hyperliens compris) :	Anglais
Applicable à :	Tous les employés, travailleurs, bénévoles, stagiaires, et consultants de SCI, et les employés de membres détachés auprès de SCI.

SECTION 1 : OBJECTIF

SCI s'engage à utiliser les données personnelles de manière responsable et à veiller à ce que tout le personnel comprenne et respecte ses responsabilités en vertu de cette politique de protection des données et de la loi, comprenant la législation britannique sur la protection des données et toute législation locale applicable en la matière. SCA prend le RGPD comme norme de base mais, lorsqu'il existe une législation locale qui a des exigences différentes ou plus strictes que celles énoncées dans cette politique, ces exigences locales doivent être respectées.

SCI reconnaît que le traitement correct et licite des données personnelles est une responsabilité essentielle. L'absence de protection adéquate des données personnelles peut entraîner des dommages pour autrui. Elle pourrait également porter atteinte à la réputation du mouvement Save the Children, entraîner une perte de revenus ou des pénalités financières importantes.

La présente politique énonce les principes que SCI applique pour traiter et protéger les données personnelles qui lui sont confiées et définit les obligations du personnel en ce qui concerne les données que nous recueillons et utilisons. Les membres du personnel ont chacun une responsabilité dans la sécurisation et la protection des données personnelles confiées à SCI.

Cette politique est obligatoire pour tout le personnel, qui doit la lire et s'y conformer, ainsi qu'à toutes les procédures et orientations connexes.

Pour toute question concernant cette politique, contactez le délégué à la protection des données de SCI à l'adresse suivante : dpo@savethechildren.org.



SECTION 2 : DÉCLARATIONS DE POLITIQUE GÉNÉRALE

1.	<p>Leadership et surveillance</p> <p>Un élément fondamental de la responsabilité est un leadership et une surveillance solides. Il s'agit notamment de s'assurer que le personnel a des responsabilités claires en matière d'activités liées à la protection des données à un niveau stratégique et opérationnel. Tous les employés et bénévoles sont tenus de respecter cette politique lorsqu'ils traitent des données personnelles.</p> <p>L'équipe de direction de SCI et le conseil d'administration ont une responsabilité stratégique en matière de protection des données. Le comité d'audit et de risque du conseil de fondation reçoit des rapports trimestriels sur les questions et les risques liés à la protection des données. Le comité directeur de la protection des données, présidé par le directeur des opérations et animé par le responsable en chef des risques (CRO), rend compte à l'équipe de direction.</p> <p>SCI est tenu d'avoir un délégué à la protection des données, en raison de la nature des données personnelles que nous recueillons et utilisons. Le rôle du délégué à la protection des données est de fournir des conseils et de surveiller la conformité à cette politique et aux obligations légales de SCI, de donner des conseils sur les évaluations d'impact de la protection des données et d'agir en tant que point de contact pour les personnes concernées et le bureau du commissaire à l'information au Royaume-Uni. Le délégué à la protection des données est le secrétaire du comité directeur de la protection des données.</p> <p>L'équipe de protection des données est assistée par un réseau de points focaux pour la protection des données dans les bureaux nationaux, qui soutiennent la mise en œuvre au niveau local.</p> <p>SCI est enregistré auprès du bureau du commissaire à l'information du Royaume-Uni sous le numéro Z3214775.</p>
2.	<p>Principes de protection des sphères</p> <p>Toute utilisation de données personnelles doit respecter les principes de protection des données, et nous devons être en mesure de prouver que nous le faisons. Les principes sont les suivants :</p> <ul style="list-style-type: none">a) Légalité, équité et transparence : Les données personnelles doivent être traitées de manière légale, équitable et transparente.b) Limitation de l'objectif : Les données personnelles ne doivent être collectées qu'à des fins spécifiques, explicites et légitimes.c) Minimisation des données : Les données personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour



	<p>lesquelles elles sont traitées. Dans la mesure du possible, SCI doit appliquer l'anonymisation ou la pseudonymisation aux données personnelles afin de réduire les risques pour les personnes concernées.</p> <ul style="list-style-type: none"> d) Précision : Les données à caractère personnel doivent être exactes et, si nécessaire, mises à jour, eu égard aux finalités pour lesquelles elles sont traitées e) Limite de stockage : Les données personnelles doivent être conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées. f) Intégrité et confidentialité : Des mesures techniques ou organisationnelles appropriées doivent être mises en place pour assurer la sécurité des données à caractère personnel, y compris la protection contre la destruction accidentelle ou illicite, la perte, l'altération, l'accès non autorisé ou la divulgation. g) Responsabilité : Les responsables du traitement des données doivent être responsables du respect des principes énoncés ci-dessus et être en mesure de le démontrer. Il s'agit notamment d'être responsable des données personnelles traitées en notre nom. <p>Tout le personnel doit respecter ces principes lors de la collecte et de l'utilisation de données personnelles.</p>
3.	<p>Licéité du traitement</p> <p>Chaque fois que des données personnelles sont traitées, elles doivent l'être sur l'une des bases légales suivantes :</p> <ul style="list-style-type: none"> a) La personne concernée a donné son consentement b) Le traitement est nécessaire à l'exécution d'un contrat avec la personne concernée c) Le traitement est nécessaire pour répondre à des obligations légales d) Le traitement est nécessaire pour protéger les intérêts vitaux de la personne concernée e) Le traitement est nécessaire à l'exécution d'une tâche effectuée dans l'intérêt public f) Le traitement est nécessaire à la poursuite des intérêts légitimes de SCI. <p>SCI doit identifier la base légale invoquée pour chaque activité de traitement et la documenter dans nos dossiers</p> <p>Lorsque les données personnelles comprennent des données de « catégorie spéciale » (données personnelles qui nécessitent des mesures de protection renforcées en raison de leur nature sensible et personnelle), nous devons également avoir un motif supplémentaire (tel que défini dans la législation) pour utiliser ces données.</p> <p>Consentement</p> <p>Le consentement ne sera pas toujours la base légale la plus appropriée, mais lorsqu'il est utilisé, nous devons nous assurer qu'il est donné librement, éclairé, spécifique et</p>

	<p>sans ambiguïté. Elle doit être clairement indiquée par une déclaration ou une action positive.</p> <p>Le personnel qui établit des déclarations de consentement ou qui gère des processus reposant sur le consentement doit suivre la Procédure de consentement et se référer au Guide du consentement, qui fournit des informations complémentaires.</p> <p>Enfants</p> <p>SCI reconnaît que les enfants ont besoin d'une protection spécifique en ce qui concerne leurs données personnelles et nous devons nous assurer que le principe d'équité et l'intérêt supérieur de l'enfant sont au cœur de tout traitement des données personnelles des enfants. Le consentement est une base légale possible pour le traitement des données personnelles des enfants, mais SCI reconnaît que parfois l'utilisation d'une base alternative est plus appropriée.</p> <p>Lorsque les données personnelles concernent un enfant de moins de 18 ans, nous devons nous assurer que l'enfant peut comprendre les implications de la collecte et du traitement de ses données personnelles. Si l'enfant n'est pas en mesure de comprendre, il convient d'utiliser une autre base ou de demander le consentement des parents ou du tuteur (à moins que cela ne soit pas dans l'intérêt supérieur de l'enfant).</p>
4.	<p>Transparence</p> <p>La transparence est fondamentalement liée à l'équité et au droit qu'ont les personnes concernées d'être éclairées sur qui nous sommes, comment et pourquoi nous utilisons leurs données personnelles, et avec qui elles sont partagées.</p> <p>SCI s'engage à être clair, ouvert et honnête avec les gens dès le départ. Cela aide les personnes à prendre des décisions éclairées sur l'utilisation de leurs données lorsque cela est approprié, et à exercer leurs droits.</p> <p>Lorsque des données personnelles sont collectées auprès d'enfants, nous devons leur fournir des informations adaptées à leur tranche d'âge afin qu'ils soient en mesure de comprendre ce qu'il adviendra de leurs données personnelles et quels sont leurs droits.</p> <p>Le personnel qui participe à la collecte ou à l'utilisation de données personnelles doit se familiariser avec les informations relatives à la vie privée et savoir comment orienter les personnes vers ces informations.</p> <p>Le personnel chargé de rédiger les informations sur la confidentialité des données ou de veiller à ce qu'elles soient fournies doit s'assurer de bien comprendre tous les éléments du RGPD britannique ou de toute autre législation applicable en se référant au Guide de la transparence et en suivant la Procédure de fourniture d'avis de confidentialité du Cadre de qualité.</p>
5.	<p>Formation et sensibilisation</p>



	<p>Tous les membres du personnel doivent suivre la formation obligatoire sur la protection des données et la sécurité informatique dans les trois mois suivant leur entrée chez SCI. Elle doit être rafraîchie tous les 12 mois, ou plus fréquemment si nécessaire.</p> <p>Le personnel occupant des fonctions spécialisées peut être amené à suivre une formation supplémentaire pour assumer ses responsabilités.</p> <p>Vous trouverez des informations et des conseils supplémentaires sur OneNet ici, et l'équipe de protection des données est disponible pour fournir des conseils et des orientations.</p>
6.	<p>Droits des données individuelles</p> <p>Les personnes concernées (y compris les enfants) ont des droits sur leurs données, y compris le droit de demander une copie de leurs données à SCI, ce que l'on appelle une « demande d'accès » ou SAR.</p> <p>Si vous recevez une demande d'accès ou une autre demande, contactez l'équipe de protection des données par courriel à l'adresse suivante : subjectaccessrequest@savethechildren.org. Vous pouvez également diriger les personnes vers l'avis de confidentialité sur notre site Web, où ils trouveront de plus amples informations. Entre-temps, vous ne devez divulguer aucune information à la personne.</p> <p>Les droits relatifs aux données en vertu de la législation britannique sur la protection des données sont les suivants :</p> <ul style="list-style-type: none"> • Droit d'être informé : Les personnes concernées ont le droit de connaître les activités de protection des données personnelles et de traitement des données de SCI, dont les détails seront contenus dans les avis de confidentialité de SCI. • Droit d'accès : Les personnes concernées peuvent faire ce que l'on appelle une demande d'accès (« SAR ») pour demander une copie de leurs données personnelles. • Droit de rectification : Les personnes concernées ont le droit de demander que toute information incomplète ou inexacte soit corrigée. • Droit à l'effacement (parfois appelé « droit à l'oubli ») Les personnes concernées ont le droit de demander à SCI de supprimer les données les concernant, • Droit de restreindre le traitement : Les personnes concernées peuvent demander que SCI cesse de traiter leurs données dans un but particulier.



	<ul style="list-style-type: none"> • Droit à la portabilité des données : Les personnes concernées peuvent demander à SCI de fournir des copies des données personnelles détenues à leur sujet dans un format communément utilisé et facilement lisible afin de les transférer à une autre organisation (dans des circonstances limitées : consultez l'équipe de protection des données pour plus de détails). • Droit d'opposition : Les personnes concernées ont le droit de s'opposer à l'utilisation de leurs données dans certaines circonstances. Si leurs données sont utilisées à des fins de marketing et qu'ils s'y opposent, le droit est alors absolu et nous devons cesser d'utiliser leurs données personnelles pour leur vendre ou promouvoir des choses, ou pour des collectes de fonds. • Droits en relation avec le traitement automatisé : Les personnes concernées ont le droit de contester les décisions et de demander un réexamen. • Droit de retirer le consentement : Si SCI s'appuie sur le consentement pour traiter ses données personnelles, la personne concernée a le droit de retirer son consentement à tout moment.
7.	<p>Contrats et partage des données</p> <p>Lorsque SCI fait appel à des fournisseurs ou prestataires de services tiers pour traiter les données personnelles en notre nom, nous nous assurons qu'ils ont mis en place les mesures appropriées pour protéger nos données. Cette démarche inclut :</p> <ul style="list-style-type: none"> • Effectuer une évaluation de leurs dispositions en matière de protection des données et de sécurité informatique, le cas échéant • Veiller à ce que les contrats comportent des clauses de protection des données appropriées. <p>Les gestionnaires responsables des décisions d'achat et de la passation des marchés doivent s'assurer qu'ils suivent les procédures convenues et utilisent les modèles de contrat appropriés.</p> <p>Partage des données</p> <p>Pour le partage régulier ou de routine de données à caractère personnel avec d'autres organisations qui ne sont pas couvertes par un contrat, nous devons convenir de la finalité du partage et des responsabilités respectives en ce qui concerne les données – par exemple, répondre aux demandes d'accès. Celles-ci doivent être définies dans un accord de partage des données.</p> <p>Pour les demandes de données personnelles émanant d'autres organisations (y compris les autorités ou les régulateurs) qui ne sont pas couvertes par un contrat ou un accord de partage des données, demandez conseil à l'équipe de protection des données.</p>



8.	<p>Évaluation des risques et de l'impact sur la protection des données</p> <p>L'analyse d'impact sur la protection des données est un processus qui permet d'identifier et de minimiser les risques liés à la protection des données, en particulier lors de la mise en œuvre de nouveaux processus ou systèmes.</p> <p>Elle doit être effectuée lorsqu'il existe un risque élevé pour les personnes et pour certains types de traitement spécifiques – notamment la localisation, la fourniture de services en ligne aux enfants et le traitement de données biométriques ou génétiques. Des informations plus détaillées à ce sujet sont fournies dans la procédure de DPIA et dans les documents d'orientation correspondants.</p> <p>Lorsqu'une DPIA liée à la protection des données et à la sécurité informatique a déjà été réalisée pour un projet ou un programme similaire et qu'elle est jugée applicable au traitement envisagé, une nouvelle évaluation des risques liés à la protection des données peut ne pas être nécessaire – mais les responsables doivent demander conseil à l'équipe de protection des données afin que cela puisse être documenté.</p>
9.	<p>Gestion et sécurité des dossiers</p> <p>Une bonne gestion des dossiers favorise une bonne gouvernance des données et leur protection. La sécurité informatique favorise également une bonne gouvernance des données et constitue en soi une exigence légale en matière de protection des données. Une mauvaise sécurité informatique fait courir des risques à nos systèmes et services et peut causer un préjudice et une détresse réels aux personnes.</p> <p>Tout le personnel doit se conformer à la politique d'utilisation acceptable des technologies de l'information de SCI, qui décrit plus en détail les précautions que le personnel doit prendre pour assurer la sécurité des données, y compris l'utilisation sécurisée du courriel, d'Internet et des dispositifs mobiles.</p> <p>Nous tenons un registre de nos utilisations des données personnelles dans l'ensemble de l'organisation, qui est géré par l'équipe de protection des données.</p>
10.	<p>Conservation des données</p> <p>En principe, les données à caractère personnel ne doivent être conservées qu'aussi longtemps que nécessaire pour la finalité pour laquelle elles ont été recueillies et pour répondre à toute obligation spécifique de conservation des données. Cette période de conservation doit être fixée lors de la première collecte ou utilisation des données, et doit être expliquée aux personnes concernées dans l'avis de confidentialité.</p>



	<p>Les éléments suivants doivent être pris en compte lors de la fixation des périodes de conservation :</p> <ul style="list-style-type: none"> • S'il existe des obligations légales de conserver les données ou les enregistrements pendant une période minimale spécifique. • Si nous avons des obligations contractuelles qui définissent la durée de conservation des documents et la manière dont ils doivent être traités à la fin de la période. • S'il y a un besoin commercial spécifique qui doit être satisfait. <p>Lors de l'examen des données et des enregistrements en vue de leur élimination, les décideurs doivent également se demander si les données ou les enregistrements peuvent avoir une valeur durable pour l'organisation ou pour la société en général, ce qui pourrait justifier leur conservation.</p> <p>Les périodes de conservation des données doivent être incluses dans les contrats ou les accords avec les fournisseurs ou les organisations partenaires qui agissent en notre nom, et les gestionnaires de contrats doivent s'assurer que les instructions de SCI sont suivies et que les données nous sont renvoyées ou supprimées à la fin du contrat, sauf accord contraire.</p> <p>Pour des conseils plus détaillés, référez-vous à la procédure et au calendrier de conservation des dossiers qui définissent les périodes de conservation minimales pour des types de dossiers spécifiques.</p>
--	--

11.	<p>Transferts internationaux de données</p> <p>SCI doit s'assurer que des mesures de protection adéquates sont en place avant le transfert international de données personnelles. Cela inclut les cas où SCI agit en tant que processeur de données au nom des membres de Save the Children.</p> <p>Les nouveaux processus susceptibles d'inclure des transferts internationaux de données personnelles ne doivent pas être lancés sans consultation préalable de l'équipe de protection des données.</p>
12.	<p>Réponse aux violations de données et suivi</p> <p>Une « violation de données à caractère personnel » désigne une violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès accidentel ou illégal à des données à caractère personnel transmises, stockées ou traitées d'une autre manière.</p> <p>Une violation peut résulter de la perte ou du vol des données elles-mêmes, ou de l'équipement ou du dispositif sur lequel elles sont stockées, comme un ordinateur portable ou un téléphone.</p> <p>Les incidents liés aux données sont gérés par l'équipe de sécurité informatique et de protection des données.</p> <p>Les violations de données réelles ou suspectées doivent être signalées à l'aide du système de gestion des incidents DATIX dès que possible et, idéalement, dans les 12 heures. Cela nous permet de prendre rapidement des mesures pour réduire le risque pour les personnes, et de respecter nos obligations de notification aux régulateurs britanniques ou d'autres pays et territoires comme nécessaire.</p>
13.	<p>Violations de la politique</p> <p>Si vous pensez que la présente politique a été violée d'une autre manière, contactez le délégué à la protection des données à l'adresse suivante : dpo@savethechildren.org. Vous pouvez également suivre la politique et les procédures de dénonciation de SCI.</p> <p>Les violation de cette politique peuvent donner lieu à des mesures disciplinaires.</p>

SECTION 3 : DÉFINITIONS

Terme	Définition
<p>Notez que les termes utilisés ou définis dans le RGPD ont été repris dans les législations sur les données d'autres pays et territoires.</p>	
Anonymisation	<p>Tel qu'utilisé dans le RGPD et le RGPD britannique</p> <p>Processus de suppression d'informations ou de caractéristiques dans des données qui permettraient de les utiliser pour identifier les « personnes concernées ». Si les données sont présentées de telle manière que la personne concernée n'est pas ou plus identifiable, la législation sur la protection des données ne s'applique pas.</p> <p>Pour savoir si des données ont été rendues anonymes, nous devons tenir compte de tous les moyens raisonnablement susceptibles d'être utilisés, par nous-mêmes ou par un tiers, pour identifier un individu auquel les informations se rapportent.</p> <p>Processus de suppression d'informations ou de caractéristiques dans des données qui permettraient de les utiliser pour identifier la personne concernée auprès de laquelle elles ont été obtenues. Les données sont présentées de manière à ce que la personne concernée ne soit plus identifiable.</p> <p>Notez qu'il faut tenir compte de la possibilité de ré-identification, ainsi que des risques pour des groupes et des populations découlant de données, même si aucun individu ne peut être identifié.</p>
Disponibilité	<p>Les données sont accessibles et utilisables par ceux qui sont autorisés à y accéder chaque fois que cela est nécessaire. La perte de disponibilité des données, même si elles ne sont pas divulguées ou consultées par d'autres, peut constituer une atteinte à la protection des données.</p>
Données biométriques	<p>Comme défini dans le RGPD et le RGPD britannique</p> <p>Données personnelles résultant d'un traitement technique spécifique relatif aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment l'identification</p>

	<p>unique de cette personne physique, telles que les images faciales ou les données dactyloscopiques*.</p> <p>*empreintes digitales</p>
Données confidentielles	<p>Données qui ne sont pas connues du public et qui sont partagées ou divulguées dans des circonstances qui créent une obligation de confidentialité (par exemple dans le cadre d'un accord de non-divulgaration ou en raison de la relation entre les parties concernées).</p> <p>Notez que le fait de marquer des données ou des documents comme « confidentiels » peut être un indicateur utile de la manière dont ils doivent être traités, mais cela ne protégera pas nécessairement la confidentialité des informations dans toutes les circonstances (par exemple si une personne fait une demande d'accès en vertu du RGPD ou d'une autre législation sur la protection des données).</p>
Consentement	<p>Comme défini dans le RGPD et le RGPD britannique</p> <p>Toute indication librement donnée, spécifique, informée et non ambiguë de la volonté de la personne concernée par laquelle celle-ci, par une déclaration ou par un acte positif clair, manifeste son accord au traitement des données à caractère personnel la concernant.</p>
Données relatives à la santé	<p>Comme défini dans le RGPD et le RGPD britannique</p> <p>Données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la fourniture de soins médicaux, et qui révèlent des informations sur son état de santé.</p>
Responsable du traitement	<p>Comme défini dans le RGPD et le RGPD britannique</p> <p>Personne physique ou morale, autorité publique, service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel.</p>
Processeur de données	<p>Comme défini dans le RGPD et le RGPD britannique</p> <p>Personne physique ou morale, autorité publique, service ou autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.</p>
DATIX	<p>DATIX est un système de gestion de cas et de rapports d'incidents basé sur le cloud. Tous les incidents liés à la fraude, à la sauvegarde de l'enfant, à la sauvegarde des adultes, à la sûreté et à la sécurité, à la médecine, à la sécurité informatique et à la protection des données au sein de SCI doivent être signalés dans DATIX.</p>

Évaluation de l'impact sur la protection des données (DPIA)	<p>Tel qu'utilisé dans le RGPD et le RGPD britannique</p> <p>Processus visant à identifier et à atténuer les risques pour les personnes découlant du traitement de données personnelles, en tenant compte de la nature, de la portée, du contexte et des objectifs du traitement ainsi que des sources de risque.</p>
Délégué à la protection des données	<p>Tel qu'utilisé dans le RGPD et le RGPD britannique</p> <p>Agent nommé pour contrôler le respect des obligations en matière de protection des données, donner des conseils sur l'évaluation de l'impact sur la protection des données et d'autres processus, et servir de point de contact pour les personnes concernées et les autorités de contrôle. L'organisation elle-même reste responsable du respect de la législation sur la protection des données.</p> <p>Le délégué à la protection des données de SCI peut être contacté à l'adresse suivante : dpo@savethechildren.org.</p> <p>La législation de certains autres pays et territoires exige également la désignation d'un délégué à la protection des données ou un rôle similaire.</p>
Système de classement	<p>Comme défini dans le RGPD et le RGPD britannique</p> <p>Tout ensemble structuré de données à caractère personnel accessibles selon des critères spécifiques, qu'il soit centralisé, décentralisé ou dispersé selon des critères fonctionnels ou géographiques.</p>
Données génétiques	<p>Comme défini dans le RGPD et le RGPD britannique</p> <p>Données à caractère personnel, relatives aux caractéristiques génétiques héritées ou acquises d'une personne physique, qui donnent des informations uniques sur la physiologie ou la santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question.</p>
Unité d'informations	<p>Ensemble d'informations qui peut être géré comme une unité unique, avec un contenu et une valeur reconnaissables. Une unité d'informations peut se présenter sous n'importe quel format.</p>
Propriétaire de l'unité d'informations	<p>Propriétaire d'une unité d'informations qui a la responsabilité de veiller à ce qu'elle soit traitée conformément aux politiques de SCI et aux directives et procédures connexes.</p> <p>Ce propriétaire doit être un haut responsable au sein de la direction ou du service concerné.</p>
Sécurité informatique	<p>Selon la définition du ministère américain du Commerce</p>



	<p>Protéger les informations et les systèmes d'information contre tout accès, utilisation, divulgation, perturbation, modification ou destruction non autorisé, afin de garantir :</p> <ul style="list-style-type: none"> • l'intégrité, qui consiste à se prémunir contre la modification ou la destruction inappropriée d'informations, et comprend la garantie de l'authenticité et de la non-répudiation des informations, • la confidentialité, c'est-à-dire le maintien des restrictions autorisées en matière d'accès et de divulgation, y compris des moyens de protéger la vie privée et les informations exclusives, • la disponibilité, qui consiste à garantir un accès rapide et fiable à l'information et son utilisation.
Service de la société de l'information	<p>Telle que définie dans la Directive (UE) 2015/1535 du Parlement européen et du Conseil</p> <p>Tout service normalement fourni contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services.</p>
Organisation internationale	<p>Comme défini dans le RGPD et le RGPD britannique</p> <p>Organisation, avec ses organes subordonnés, régie par le droit international public, ou tout autre organe créé par un accord entre deux ou plusieurs pays ou sur une telle base.</p>
Bureau du commissaire à l'information du Royaume-Uni (<i>Information Commissioner's Office</i> ou ICO)	<p>Le Bureau du commissaire à l'information du Royaume-Uni est l'organisme public britannique indépendant qui régit les droits à l'information dans l'intérêt public.</p> <p>Outre la législation relative à la protection des données (RGPD britannique et loi de 2018 sur la protection des données), elle régleme la législation relative au PECR (communications électroniques), à l'eIDAS (transactions électroniques), au NIS (sécurité des infrastructures nationales), à la réutilisation des informations publiques et aux pouvoirs d'enquête. En Angleterre, au Pays de Galles et en Irlande du Nord, l'ICO régleme également la liberté d'information, l'information sur l'environnement et la législation INSPIRE.</p>
Secret professionnel (Angleterre et Pays de Galles)	<p>Protection contre la divulgation de certaines communications confidentielles (y compris le courrier électronique) :</p> <ul style="list-style-type: none"> • entre les avocats (y compris les juristes d'entreprise) et leurs clients dans le but unique ou principal de donner ou de recevoir des conseils juridiques (<i>Legal Advice Privilege</i>), • entre les avocats (y compris les juristes d'entreprise) ou leurs clients et tout tiers dans le but unique ou principal d'obtenir des conseils ou des informations en rapport avec un litige existant ou raisonnablement

	<p>envisagé (<i>Litigation Privilege</i>).</p> <p>Certaines dispositions de la législation britannique sur la protection des données au Royaume-Uni, notamment le droit d'accès, ne s'appliquent pas aux informations couvertes par le secret professionnel.</p>
<p>Données personnelles</p> <p>(Bien qu'ils soient parfois utilisés de manière interchangeable, les termes « données confidentielles » et « données personnelles » ne sont pas les mêmes)</p>	<p>Comme défini dans le RGPD et le RGPD britannique</p> <p>Toute information relative à une personne physique identifiée ou identifiable (« personne concernée ») ; une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment en se référant à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques de l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne physique.</p>
<p>Atteinte à la protection de données personnelles</p>	<p>Comme défini dans le RGPD et le RGPD britannique</p> <p>Violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès accidentel ou illégal à des données à caractère personnel transmises, stockées ou traitées d'une autre manière.</p>
<p>Traitement</p>	<p>Comme défini dans le RGPD et le RGPD britannique</p> <p>Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ou à des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, de limitation, d'effacement ou de destruction.</p>
<p>Profilage</p>	<p>Comme défini dans le RGPD et le RGPD britannique</p> <p>Toute forme de traitement automatisé de données à caractère personnel consistant à utiliser des données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prévoir des aspects concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les centres d'intérêt, la fiabilité, le comportement, l'emplacement ou les déplacements de cette personne physique.</p>
<p>Pseudonymisation</p>	<p>Comme défini dans le RGPD et le RGPD britannique</p>

	Traitement de données à caractère personnel de telle sorte que ces données ne puissent plus être attribuées à une personne concernée spécifique sans l'utilisation d'informations supplémentaires, à condition que ces informations supplémentaires soient conservées séparément et fassent l'objet de mesures techniques et organisationnelles visant à garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.
Destinataire	<p>Comme défini dans le RGPD et le RGPD britannique</p> <p>Personne physique ou morale, autorité publique, agence ou autre organisme, à qui les données personnelles sont divulguées, qu'il s'agisse d'un tiers ou non. Toutefois, les autorités publiques susceptibles de recevoir des données à caractère personnel dans le cadre d'une enquête particulière conformément au [droit national de l'Union Européenne, d'un de ses États membres, ou du Royaume-Uni] ne sont pas considérées comme des destinataires ; le traitement de ces données par ces autorités publiques doit être conforme aux règles applicables en matière de protection des données selon les finalités du traitement.</p>
Limitation du traitement	<p>Comme défini dans le RGPD et le RGPD britannique</p> <p>Marquage des données personnelles conservées dans le but de limiter leur traitement futur.</p>
Données de catégorie spéciale (parfois appelées « données personnelles sensibles »)	<p>Tel qu'utilisé dans le RGPD et le RGPD britannique</p> <p>Sous-catégorie de données personnelles qui nécessite des mesures de protection renforcées en raison de leur nature sensible et personnelle.</p> <p>Données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, traitement des données génétiques et des données biométriques aux fins d'identifier une personne physique de manière unique, et données concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique.</p> <p>Notez que, dans d'autres pays et territoires, les données personnelles sensibles ou de catégorie spéciale peuvent inclure d'autres facteurs. Ainsi, dans la loi ougandaise de 2019 sur la protection des données et de la vie privée, les données financières sont incluses et, dans la loi kényane de 2019 sur la protection des données, elles comprennent les détails sur la propriété, l'état civil, les détails familiaux, y compris le nom des enfants, des parents, et du ou des conjoints de la personne.</p>
Tiers	Comme défini dans le RGPD et le RGPD britannique

	Personne physique ou morale, autorité publique, service ou organisme autre que la personne concernée, le responsable du traitement, le processeur de données et les personnes qui, sous l'autorité directe du responsable du traitement ou du processeur de données, sont autorisées à traiter les données à caractère personnel.
Registres des activités de traitement	<p>Tel qu'utilisé dans le RGPD et le RGPD britannique</p> <p>Résultat d'une cartographie des données. Documentation formelle conservée par un contrôleur ou processeur de données sur les utilisations des données personnelles dans l'organisation.</p> <p>Les registres des activités de traitement doivent comprendre des informations importantes sur le traitement des données, notamment les catégories de données, le groupe de personnes concernées, la finalité du traitement et les destinataires des données. Ces informations doivent être mises à la disposition des autorités sur demande.</p> <p>Dans certains autres pays et territoires, il existe des obligations similaires de conserver ou de soumettre les détails du traitement aux autorités de contrôle.</p>
Demande d'accès (SAR)	<p>Tel qu'utilisé dans le RGPD et le RGPD britannique</p> <p>Demande par une « personne concernée » d'une copie de ses données personnelles détenues par un contrôleur de données.</p>

SECTION 4 : DOCUMENTS CONNEXES

DOCUMENT	SITE D'EXPLOITATION
SCI_IT_DP_DPIA_Guidance_EN	Cadre de qualité de SCI
SCI_IT_DP_DPIA_Procedure_EN	Cadre de qualité de SCI
SCI_IT_DP_Transparency_Guidance_EN	Cadre de qualité de SCI
SCI_IT_DP_Privacy_Notice_Procedure_EN	Cadre de qualité de SCI
SCI_IT_DP_Consent_Guidance_EN	Cadre de qualité de SCI
SCI_IT_DP_Consent_Procedure_EN	Cadre de qualité de SCI
SCI_IT_DP_Records_Retention_Procedure_EN	Cadre de qualité de SCI
Politique d'utilisation acceptable des technologies de l'information	
Politique de sécurité informatique	

Déclaration de confidentialité de SCI	Site Web de SCI