

OBJET : POLITIQUE ASSOCIATIVE SUR LA PROTECTION DES DONNEES		Date : 02/09/2024
Destinataires : Personnel de RST Adhérents et leurs salariés, IRP des adhérents Affiliés		Version : 001
		ORG DC 013

• Objet et enjeux

.1 Contexte réglementaire

La protection des Données à Caractère Personnel¹ (« DCP ») est une obligation qui s'inscrit dans un cadre juridique profondément renouvelé par le Règlement Général de Protection des Données « RGPD » entré en vigueur le 25 mai 2018. C'est le sens de ce règlement européen qui vient compléter et renforcer les obligations existantes sur le plan national :

- Il conforte la place de l'individu au cœur du système juridique, technique et éthique de la protection des données en Europe et lui offre de **nouveaux droits ou garanties** pour lui permettre de mieux maîtriser le devenir de ses données : meilleure information, extension du consentement, renforcement des droits d'accès, d'opposition, de modification, à l'oubli et création d'un droit à la portabilité pour lui permettre de récupérer ses données sous un format aisément réutilisable, ainsi qu'un droit à la limitation du traitement.
- Il place les entreprises traitant des DCP et leurs sous-traitants dans **une logique de responsabilisation**. Chacune à leur niveau doit protéger les DCP par la mise en place de mesures organisationnelles et techniques adaptées aux risques sur la vie privée des personnes concernées, pour les traitements¹ existants ou nouveaux.
- Il entérine la **nécessité de tracer** les actions et mesures de pilotage et de sécurisation des données personnelles (obligation de tenue d'un registre) et encadre les nouvelles pratiques technologiques (profilage, pseudonymisation).
- Il étend le champ des **échanges avec la CNIL** (obligation de notification de violation de DCP, consultation préalable pour les traitements susceptibles d'engendrer un risque élevé), renforce le contrôle du régulateur et son pouvoir de **sanction** (jusqu'à 4% du chiffre d'affaires. Il autorise en outre les actions de groupe en réparation de dommage.

¹ Cf. définition en annexe 1

.2 Enjeux pour le secteur de la médecine du travail

La protection des données à caractère personnel (DCP) est un droit fondamental et constitue un enjeu stratégique pour assurer la confiance des salariés, des entreprises adhérentes et des partenaires. Cela est également essentiel pour préserver la réputation du service de médecine du travail auprès de ses collaborateurs et de ses financeurs.

A ce titre, l'ensemble des services de RST s'engagent également à se conformer à :

- La loi « Informatique et libertés » du 6 janvier 1978, modifiée notamment par la loi n° 2018- 493 du 20 juin 2018 relative à la protection des données à caractère personnel et l'ordonnance 2018-1125 du 12 Décembre 2018.
- Le décret 2018-687 pris en application de la loi CNIL 3 ainsi que le décret n° 2019-536 du 29 mai 2019 pris en application de la loi « Informatique et libertés » modifiée.
- La Délibération CNIL n° 2018-327 du 11 octobre 2018 listant les traitements de données à caractère personnel pour lesquels une analyse d'impact est forcément requise.

.3 Objectifs

Ce document constitue la politique de protection des DCP de l'Association lorsque ses données font l'objet d'un **traitement**¹, c'est-à-dire de toutes opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de DCP contenues ou appelées à figurer dans un fichier. Le traitement comprend la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Il définit les principes directeurs de la protection des DCP au sein de RST

.4 Périmètre d'application

.4.1 Périmètre d'application juridique et territorial

La politique de protection des DCP s'applique à compter de sa validation la Direction Générale

- À toute personne physique dont les DCP sont traitées ou collectées par RST, y compris les employés, les dirigeants, les responsables légaux des entreprises adhérentes, les salariés et leurs familles et les prestataires externes

.4.2 Données concernées par cette politique

Cette politique s'applique au **traitement** des DCP réalisé par Reims Santé au Travail

.5 Mise à jour

Cette politique de protection des DCP est revue à minima tous les 5 ans.

.6 Articulation de cette politique avec les autres documents internes

Cette politique s'appuie et complète :

- Le Projet Associatif ;
- La Politique de Gestion de crise.

Elle est déclinée opérationnellement par des procédures, chartes ou autre support décrivant les modes opératoires à appliquer.

• Principes fondamentaux de protection des DCP

.1 Traitements des DCP

L'association met en place un dispositif qui permet de s'assurer que les DCP sont :

- Traitées de manière **licite** au sens de la loi², **loyale et transparente** ;
- Collectées pour des finalités **déterminées, explicites et légitimes**, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ;
- **Adéquates, pertinentes et limitées** à ce qui est nécessaire au regard des finalités (minimisation) ;
- **Exactes** et, si nécessaire, **tenues à jour** (exactitude) ;
- **Conservées** sous une forme permettant l'identification des personnes concernées pendant une **durée définie** selon les finalités du traitement et **effacées ou rendues anonymes** au-delà de cette durée ;
- **Sécurisées et protégées** contre l'accès et/ou le traitement non autorisé ou illicite, la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées permettant d'en assurer l'intégrité, la disponibilité et la confidentialité.

.2 Mesures préalables à la mise en œuvre d'un traitement de DCP

.2.1 Licéité des traitements

L'Association met en place les moyens lui permettant de s'assurer que chaque traitement mis en œuvre est licite, conformément aux textes applicables. Un traitement est licite notamment lorsque :

- La personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
- Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie prenante ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci.

Dans les cas où le traitement repose sur le consentement, les entités de l'Association s'assurent de pouvoir démontrer que :

- La personne concernée a donné son consentement au traitement de DCP la concernant ;

² cf. article 6 « Licéité du traitement » du règlement GDPR.

- La personne concernée a le droit de retirer son consentement à tout moment et qu'elle en est informée avant de donner son consentement.

.2.2 Protection des DCP dès la conception

L'Association met en œuvre l'ensemble des actions qui permettent d'intégrer la protection des DCP par défaut (*Privacy by Default*) et dès la conception (*Privacy by Design*) de nouveaux projets, que ces derniers portent sur un processus, une organisation, un produit, un service ou un applicatif ou matériel du Système d'Information. Pour chaque nouveau projet traitant ou impliquant le traitement de données à caractère personnel, l'Association met tout en œuvre pour assurer un niveau de protection approprié.

.2.3 Analyse du risque sur la vie privée

L'Association met en place un processus qui permet d'**analyser l'impact sur la vie privée** de tout nouveau traitement de DCP ou toute modification de traitement susceptible d'engendrer un risque élevé³ pour les droits et libertés des personnes physiques concernées. Cette analyse d'impact comprend des analyses de risques sur la sécurité des systèmes d'information pour les traitements concernés et des analyses de risques des sous-traitants concernés.

.2.4 Registre des traitements

L'Association établit et met régulièrement à jour un registre des traitements de DCP qui, le cas échéant, pourra être présenté à la CNIL sur demande.

.3 Sécurité des DCP

.3.1 Mesures techniques et organisationnelles mises en œuvre

L'Association met en œuvre **par défaut et dès leur conception** les mesures techniques et organisationnelles afin de garantir la sécurité et la confidentialité des DCP contre l'accès et/ou le traitement illégal, la perte, la destruction ou la dégradation non autorisée ou accidentelle de ces données. Les Etablissements et Directions de l'Association intègrent donc la protection des DCP dès la conception des traitements et contrats, et s'assurent que la sécurité des DCP est garantie tout au long des opérations pour lesquelles elles sont collectées, traitées et conservées.

.3.2 Violation de DCP

L'association met en place les processus et les moyens lui permettant de prendre les mesures suivantes :

- S'assurer que ses sous-traitants lui notifient dans « les meilleurs délais » toute violation des DCP après en avoir pris connaissance ;
- Notifier à la CNIL toute violation de sécurité des DCP, dans les 72 heures après en avoir pris connaissance, lorsque cette violation est susceptible d'engendrer un « risque pour les droits et libertés » des personnes concernées ;

³ Cf. définition des risques élevés en annexe 1.

- Informer, le cas échéant, la personne concernée lorsqu'une violation de DCP est susceptible d'engendrer un risque élevé pour ses droits et libertés ;
- Documenter (dans un registre des violations) les violations de DCP, en indiquant les faits, les effets et les mesures prises pour y remédier.

.1 Sous-traitants

L'Association met en place un dispositif de sélection des sous-traitants et partenaires basé sur une analyse de leurs risques, une évaluation de leurs mesures techniques et organisationnelles de protection des DCP et intégrant des critères de respect de la législation sur la protection des DCP.

L'Association encadre ses relations avec ses sous-traitants par des engagements contractuels comprenant :

- L'engagement du sous-traitant à agir pour le compte et sur instruction du responsable de traitement ;
- La définition, l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel, les catégories de personnes concernées, la description des mesures de sécurité mises en place (chiffrement ou autre), et les obligations et les droits de chaque partie ;
- La fourniture des analyses de risques sur la vie privée (*Privacy Impact Assessment* ou PIA), pour les traitements les plus sensibles ;
- L'engagement du sous-traitant à ne recruter un autre sous-traitant qu'après s'être assuré que les garanties et mesures de sécurité appliquées par ce dernier sont conformes aux exigences du RGPD, **et** sous réserve de l'autorisation écrite préalable de l'entité concernée de l'Association ;
- L'engagement du sous-traitant d'assister – dans les 10 jours ouvrés suivant la sollicitation – le responsable du traitement dans le respect de son obligation de répondre aux demandes d'exercice des droits des personnes concernées, tels que décrits au chapitre suivant ;
- L'engagement du sous-traitant à supprimer toutes les DCP ou les renvoyer au responsable du traitement au terme de la prestation de services relatifs au traitement, et de détruire les copies existantes ;
- L'engagement du sous-traitant à notifier l'Association sous 24 heures de toute violation de DCP le concernant ;
- La possibilité pour l'Association de réaliser des contrôles, audits ou inspections des dispositifs de protection des DCP ;
- L'engagement du sous-traitant à ne réaliser de transfert de données hors de France qu'après accord préalable de l'Association
- L'engagement du sous-traitant à prévenir l'Association de tout changement significatif relatif au traitement des DCP.

.2 Droits des personnes concernées

L'Association reconnaît et respecte les droits des personnes concernées. Elle met en œuvre les moyens nécessaires permettant aux personnes concernées d'exercer les droits mentionnés ci-dessous :

- **Droit à l'information préalable** : s'assurent que toute information et communication aux personnes concernées relatives au traitement de DCP sont aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples. Elles s'assurent également que les personnes physiques sont informées, dès la collecte, de l'ensemble des informations requises.
- **Droit d'accès** : répondent sans frais et dans un délai d'un mois maximum aux demandes d'accès des personnes concernées exprimées selon les formalités d'usage.
- **Droit de rectification** : traitent les demandes de rectification des DCP dans un délai d'un mois maximum.

- **Droit d'effacement et droit à l'oubli** : traitent les demandes d'effacement des DCP des personnes concernées dans un délai d'un mois sauf en cas de raison impérieuse nécessaire
- **Droit d'opposition** : traitent les demandes d'opposition des personnes concernées. Ce droit ne s'applique pas dans le domaine des données de santé, mais les demandes doivent être instruites et une information doit être apportée.
- **Droit à la portabilité** : traitent sans frais les demandes de portabilité des DCP et les fournissent à la personne concernée dans un format structuré, couramment utilisé et lisible par machine.
- **Droit à la limitation** : traitent les demandes de limitation de traitement de DCP des personnes concernées en mettant en œuvre les mécanismes permettant de geler le traitement.

.3 Transferts de données et traitements transfrontaliers

L'Association n'autorise les transferts de données que vers d'autres pays de l'Union Européenne.

.4 Traitements présentant des risques particuliers pour les personnes concernées

L'Association met en œuvre des dispositifs et des mesures de sécurité appropriées (notamment le chiffrement en stockage) pour garantir la sécurité (confidentialité, intégrité et disponibilité) des traitements présentant des risques particuliers pour les personnes concernées, notamment les traitements portant sur les données de santé, la cybersurveillance, les objets connectés, les condamnations pénales et les infractions. Par ailleurs, le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont en principe interdits car ce sont des données sensibles. Leur utilisation est donc strictement encadrée par la législation.

.5 Traitements Ressources Humaines

L'Association met en place les processus adéquats pour permettre à ses collaborateurs et candidats au recrutement de bénéficier et, le cas échéant, d'exercer leurs droits lorsqu'ils sont concernés par un traitement de DCP.

L'Association s'assure que les représentants du personnel sont informés et/ou consultés à chaque fois que nécessaire, et notamment lorsque les traitements des données à caractère personnel concernent des collaborateurs.

• Gouvernance de la protection des DCP

.1 Obligations des Etablissements, des partenaires et des sous-traitants

L'Association s'assure du respect du cadre réglementaire et des principes énoncés dans la présente politique :

- Par la mise en place d'une gouvernance reposant sur une filière Protection des DCP et d'un contrôle adapté ;

- Au niveau des sous-traitants – qui incluent les partenaires et délégataires – et de leurs propres sous-traitants : par le moyen d'une sélection rigoureuse, basée sur une analyse de risque, de chaque sous-traitant, par des engagements contractuels et la mise en œuvre de contrôles.

.2 Rôle et responsabilité des entités agissant en qualité de responsable de traitement, responsable de la mise en œuvre et/ou de sous-traitant

Le responsable de traitement est identifié, ainsi que le service chargé de sa mise en œuvre pour chaque traitement mis en œuvre au sein de l'Association ou indirectement (par le biais d'un sous-traitant).

- Une analyse est systématiquement réalisée afin de déterminer qui est « responsable de traitement », « co-responsable du traitement » ou « sous-traitant »⁴ ;
- Le responsable du traitement détermine de manière claire et précise les finalités et les moyens de chacun des traitements de DCP qu'il met en œuvre.

L'Association met en place la filière de protection des DCP telle que décrite au chapitre suivant en nommant les différents acteurs attendus et en leur donnant les moyens et ressources suffisantes pour exercer leurs fonctions en toute indépendance.

Le responsable de traitement est responsable du respect de la présente politique et est en mesure de démontrer qu'elle est respectée, y compris l'efficacité des mesures techniques et organisationnelles mises en œuvre (**principe de responsabilité**).

.3 Rôles et responsabilités des acteurs de la Protection des Données

.3.1 Acteurs

L'Association met en place une organisation articulée autour d'une filière de protection des données animé par le Délégué à la protection des données.

Le processus de protection des DCP fait également intervenir différents acteurs et fonctions de l'Association, et plus particulièrement :

- La fonction Achats ;
- La fonction Qualité ;
- Les responsables de la Sécurité des SI et la fonction Informatique ;
- La fonction Ressources Humaines ;
- La fonction Communication ;
- La fonction Médecin Coordinateur

.3.2 Rôles et responsabilités du Délégué à la Protection des Données (DPO)

Le DPO est le Délégué à la Protection des données de l'Association. Le DPO est doté par l'Association des moyens et ressources, nécessaires pour exercer ses missions en toute indépendance. Il peut être un salarié de l'Association ou exercer ses missions en vertu d'un contrat de prestation externe.

⁴ Voir la définition en Annexe 1

Les missions du DPO au titre du pilotage et de l'animation de la protection des données sont :

- Assurer le management global de la filière de protection des DCP et garantir la cohérence des dispositifs sur le périmètre consolidé de toutes les entités de l'association.
- Alerter la Direction Générale en cas de manquement.
- Effectuer le reporting et le présenter à la Direction Générale
- Définir un plan de contrôle permanent de la protection des DCP à appliquer par chaque Etablissement.
- Définir et mettre en place un plan de formation, de sensibilisation et de communication à destination de l'ensemble des acteurs de la protection des DCP.

Les missions du DPO en tant que Délégué à la protection des données sont :

- Informer et conseiller le responsable de traitement, les sous-traitants et les collaborateurs qui procèdent aux traitements de DCP.
- Vérifier la mise en œuvre de la présente politique.
- Animer et coordonner les travaux relatifs à la protection des DCP dont notamment l'élaboration des analyses de risques sur la vie privée (PIA) et la tenue du registre des traitements.
- Répondre aux réclamations et aux personnes concernées sur leurs demandes d'exercice de leurs droits.
- Alerter sa Direction Générale en cas de manquement ou de non-respect de la présente politique.
- Mettre en œuvre et consolider les dispositifs de suivi et de contrôle permanent de la protection des DCP.
- Etre le point de contact avec la CNIL en cas de notification ou de contrôle.
- S'assurer de la bonne traçabilité des actions réalisées dans le cadre du management de la protection des DCP.
- Veiller aux différentes évolutions réglementaires sur la protection des DCP et s'assurer de la mise en conformité avec la réglementation locale.
- Former, sensibiliser et communiquer auprès de l'ensemble des acteurs de la protection des DCP.

.4 Instances et fonctionnement de la filière protection des DCP

La gouvernance de la protection des DCP repose, au niveau de l'Association, sur le DPO.

.4.1 Réunion de la filière de protection des données

L'ensemble des membres de la filière de protection des données– le DPO et la fonction Informatique et les responsables de la Sécurité des SI se réunissent à *minima* une fois par an afin de :

- Passer en revue l'activité de l'année concernant la protection des DCP ;
- Partager les évolutions réglementaires nationales, européennes et locales. ;
- Échanger sur les solutions techniques, juridiques et organisationnelles de sécurisation des DCP.

.4.2 Arbitrage en cas de désaccord

En cas de désaccord entre le DPO et les métiers, l'arbitrage éventuel sera traité par la voie hiérarchique et, le cas échéant, par le Directeur Général.

.4.3 Articulation avec les autres instances existantes

Le DPO doit assister les différentes instances existantes au sein de l'Association dont les prérogatives sont :

- **D'agrée les nouveaux produits et services**, afin d'y intégrer la protection des DCP dès la conception de nouveaux projets, que ces derniers portent sur un processus, une organisation, un produit, un service ou un actif du Système d'Information ;
- De suivre et reporter **les résultats des différents contrôles et audits** relatifs à la protection des données, d'identifier les risques et mettre en place les contrôles supplémentaires à réaliser ;
- De piloter le processus de **sélection des sous-traitants** afin de s'assurer que :
 - Les critères de protection des données sont pris en compte dès la sélection des sous-traitants, dans les nouveaux contrats de sous-traitance.
 - L'ensemble des analyses de risques sur la vie privée des sous-traitants est bien collecté,
 - Les analyses des risques résiduels sont réalisées et couvertes par des plans d'actions.
- De superviser la mise en œuvre de **dispositifs techniques (SI) de protection des DCP** et d'identifier les plans d'actions transverses permettant la mise en conformité avec le cadre législatif en vigueur.

• Reporting et contrôle

.1 Reporting

Le DPO réalise un reporting à destination de la Direction Générale.

.2 Relation avec les autorités de contrôles de contrôle

L'Association collabore avec les autorités de contrôle compétentes pour toute question relative à la protection des DCP ou bien dans le cadre de leurs procédures d'audit.

L'Association met en place les processus permettant de se conformer et d'appliquer les recommandations de ces autorités conformément au cadre réglementaire et législatif en vigueur.

Le DPO est l'interlocuteur habituel de la CNIL en matière de protection des DCP.

• Déclinaison de la politique

Cette politique se décline dans un référentiel opérationnel comprenant un cadre de procédures opérationnelles et une matrice des rôles et responsabilités.

Annexe 1 : Définitions

Co-responsable de traitement : Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement.

Consentement de la personne concernée : toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des DCP la concernant fassent l'objet d'un traitement.

Donnée à caractère personne, « DCP » : toute information se rapportant à une personne physique identifiée ou identifiable est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Données biométriques : les DCP résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

Données concernant la santé : les DCP relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé, physique ou mentale passé, présent ou futur de cette personne. Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services ou de prestations de soins de santé ; des informations obtenues lors d'un test ou examen médical ; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ; toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne.

Données génétiques : les DCP relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question.

Profilage : toute forme de traitement automatisé de DCP consistant à utiliser ces DCP pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.

Pseudonymisation : le traitement de DCP de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et

organisationnelles afin de garantir que les DCP ne sont pas attribuées à une personne physique identifiée ou identifiable.

Risques élevés et analyse de risque sur la vie privée : lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement doit effectuer, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel :

- L'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
- Le traitement à grande échelle de catégories particulières de données [...] ou de données à caractère personnel relatives à des condamnations pénales et à des infractions [...] ;
- La surveillance systématique à grande échelle d'une zone accessible au public.

Responsable du traitement : 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 ;

Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des DCP pour le compte du responsable du traitement.

Traitement : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de DCP, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Violation de DCP : Il s'agit d'un incident de sécurité ayant des conséquences sur l'intégrité, la disponibilité ou la confidentialité de données à caractère personnel. Cette violation de la sécurité, entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de DCP transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Annexe 2 : Entités concernées par le déploiement ou la déclinaison de cette politique

Liste des Etablissements
Reims Santé au Travail