

		Convention générale à la protection des données personnelles	Comité de confidentialité et de sécurité des systèmes informatiques
COSI-DSQ-024	0.10		Date d'application : 12/06/2018

Le présent document a été communiqué au Conseil d'Entreprise le 12 juin 2018 -

A travers le présent document, les **Cliniques universitaires Saint-Luc (CUSL)** entendent vous fournir des informations claires et précises concernant le traitement de vos données personnelles, le fondement juridique de ce traitement, vos droits et la procédure à mettre en œuvre en cas de violation des données afin de conserver votre confiance et vous fournir l'assurance que la protection et la gestion de vos données se fera de manière adéquate et responsable dans le respect des dispositions légales¹.

Art. 1 : Principes généraux et justification

Le Règlement Général sur la Protection des Données (RGPD) impose des règles et conditions strictes aux employeurs dans le cadre du traitement des données à caractère personnel de leurs travailleurs/collaborateurs, et ce afin de protéger la vie privée de ceux-ci et de faire un usage responsable de ces données.

À travers la présente convention vie privée, l'employeur entend fournir au travailleur/collaborateur des informations claires et précises concernant le traitement de ses données à caractère personnel.

L'employeur est contraint de traiter des données à caractère personnel du travailleur/collaborateur aux fins de l'exécution et du respect du contrat de travail (ou convention) conclu entre l'employeur et le travailleur/collaborateur.

L'employeur a besoin de certaines informations pour pouvoir calculer le salaire du travailleur/collaborateur et lui accorder des avantages, par exemple, ainsi que pour pouvoir mener une politique du personnel efficace dans l'intérêt du travailleur/collaborateur (évaluations, formations, gestion d'annuaire, etc.).

En outre, le traitement de données à caractère personnel du travailleur/collaborateur est indispensable au bon fonctionnement de l'institution (planification du travail, sécurité du matériel, contacts avec les patients, avec les fournisseurs, etc.).

Dès lors, le traitement des données à caractère personnel du travailleur/collaborateur par l'employeur s'avère à la fois légitime et nécessaire (art. 6 du RGPD) :

- aux fins de l'exécution du contrat de travail conclu entre l'employeur et le travailleur/collaborateur ;
- pour satisfaire à des obligations légales imposées à l'employeur dans le cadre de la relation de travail ;
- en vue du bon fonctionnement de l'institution.

Pour toutes ces raisons, des données à caractère personnel doivent nécessairement être fournies à l'employeur par le travailleur/collaborateur. Dans le cas contraire, l'employeur ne pourra calculer correctement le salaire du travailleur/collaborateur, assurer sa bonne intégration au sein du fonctionnement de l'institution, etc.

¹ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD) entrant en vigueur le 25 mai 2018.

Art. 2 : Finalité du traitement des données à caractère personnel des travailleurs/collaborateurs

L'employeur est contraint de traiter des données à caractère personnel aux fins suivantes :

- Administration des données du personnel

Finalité	- Gestion du dossier du membre du personnel - Sélection et recrutement - Application de la législation sociale - Remise de documents - Calcul du salaire des travailleurs/collaborateurs, - gestion des incapacités et congés - Organisation et planification de formations - source de l'octroi de certains accès (e-mail professionnel, logiciels, locaux ...)
Personnes concernées	Membres du personnel au service de l'employeur ou assimilé
Données	<u>Données d'identification personnelles :</u> - nom, titre, adresse privée, numéro de téléphone (fixe et GSM), numéro de registre national - données d'identification attribuées par l'employeur (numéro de matricule), - date d'entrée en service et de sortie ; - modifications éventuelles d'affectation, de fonction et de durée contractuelle - horaire théorique, heures prestées, absences et motifs des absences - photos (non actif au 18/05/2018) <u>Données d'identification de tiers : (contacts / famille)</u> - nom, titre, adresse privée, numéro de téléphone (fixe et GSM) ; <u>Données d'identification financières :</u> - numéro de compte bancaire, dettes connues dans le cadre d'une saisie ou cession sur salaire ; - salaire : paiements et retenues : rémunération de base, éléments fixes (comme une prime due dans le cadre d'une CCT) et variables (par exemple les sursalaires pour prestations particulières ou encore les forfaits pour permanence à domicile) remboursement prévu de dépenses, avantages, prélèvements sociaux (cotisations ONSS) et fiscaux (précompte professionnel), méthodes de paiement, date des modifications de barème ; - détails concernant les assurances souscrites par l'employeur pour les travailleurs/collaborateurs : type d'assurance, risques couverts, montants assurés, période de couverture, date d'échéance, paiements, options, bénéficiaires. <u>Caractéristiques personnelles :</u> - âge, sexe, date de naissance et lieu de naissance, état civil, nationalité ; - composition du ménage, enfants à charge ; - statut d'immigration : détails du visa, permis de travail, conditions particulières liées au droit de séjour ; - pas de données judiciaires ni liées à l'affiliation éventuelle à un syndicat <u>Études et formation :</u> - curriculum académique : historique des établissements scolaires fréquentés, nature des cours suivis, diplômes visés et obtenus ; - qualifications professionnelles : brevets et formations professionnelles, agréments,... - expérience professionnelle : intérêts professionnels, intérêts de recherche, intérêts académiques, sujets de spécialisation ou de mémoire ... ; - publications : livres, articles, rapports, matériel audiovisuel publié ; <u>Loisirs, intérêts et affiliations</u> informations reçues dans le cadre de la sélection et du recrutement. <u>Carrière :</u> fonctions et expériences antérieures auprès d'autres employeurs, périodes sans emploi. <u>Actifs détenus par le personnel :</u> Badge, clés (de bureau, vestiaire,...), tenues de travail, outils informatiques (PC, imprimantes, digipass ...), GSM de service ou de société, voiture de société,

	lecteur radioprotection, matériels et outils, autres objets détenus par le travailleur/collaborateur. <u>Recrutement :</u> date, méthode, source de recrutement, résultat de tests, note du recruteur (par exemple à l'occasion d'un entretien individuel). <u>Fin de l'emploi :</u> date du départ, raison du départ, préavis donné, conditions de fin de l'emploi.
Destinataires	- Membres du personnel RH de l'employeur en charge de l'administration du personnel - Membres du personnel de l'employeur en charge de matière RH associée (personnel hiérarchique, Assistants de gestion, personnel gérant le suivi statistique, personnel assurant l'octroi d'accès (locaux, vestiaires, clé, informatique,...),...) - Entreprises privées en vertu d'une obligation légale de l'employeur, p.ex.: banques et huissiers dans le cadre de dossiers de saisie - Compagnies d'assurances, mutuelles, médecine du travail ... - Services publics : Office national des Vacances annuelles, ONSS, SPF finance, SPF santé publique, Fonds social des hôpitaux privés, ONEM, Fonds des maladies professionnelles, AWIPH ...
Durée de conservation	5 ans après la sortie des CUSL 30 ans dernier acte pour les médecins
Transfert de données vers des pays tiers	Oui – fiche de paie – datacenter en Hollande (hébergeur Equinix)

- Évaluation du personnel

Finalité	- Évaluations et suivi du personnel. - Entretiens de fonctionnement et d'évaluation - Augmentation salariale le cas échéant (avancements barémiques prévus par les statuts du personnel PATO) - nomination agent définitif (cfr statuts du personnel PATO) - Prévision de formations - Planification de formations - Planification de la carrière - Motivation du licenciement
Personnes concernées	Membres du personnel au service de l'employeur
Données	- Organisation du travail : responsabilités actuelles, projets. - Absences et motifs. - Performances du travailleur/collaborateur. - Mesures disciplinaires. - Salaire et évolution salariale. - Déroulement de la carrière. - Évaluations précédentes et entretiens intermédiaires. - Évaluation des performances, possibilités. - Formation à la fonction : détails des besoins de formation propres à la fonction et de la formation reçue, qualifications obtenues et compétences acquises. - Pas de données médicales, sensibles ou judiciaires.
Destinataires	- Employeur et conseillers RH professionnels de l'employeur - Supérieurs directs.
Durée de conservation	5 ans après la fin du contrat de travail 30 ans dernier acte pour les médecins
Transfert de données vers des pays tiers	Non

- Planification du travail

Finalité	- Planification des tâches. - Suivi des tâches. - Mobilisation efficace des collègues et planification des activités avec les patients. - Gestion de la charge de travail.
Personnes concernées	Membres du personnel au service de l'employeur ou personnes travaillant pour l'employeur.
Données	- Système de suivi et de traçabilité installé. - Organisation du travail : responsabilités actuelles, projets, heures prestées.
Destinataires	- Employeur et conseillers RH professionnels de l'employeur. - Supérieurs directs - planificateurs au sein des services - collègues de service (en cas d'affichage du planning au sein du service)
Durée de conservation	5 ans après année concernée
Transfert de données vers des pays tiers	Non

- Contrôle d'accès et surveillance

Finalité	1. Sécurité de l'institution et des collaborateurs de l'institution 2. Protection des biens et du système d'information de l'institution. 3. Refus de l'accès aux personnes non autorisées. 4. Accès aux applications, aux locaux, aux parkings,...
Personnes concernées	Membres du personnel au service de l'employeur ou personnes travaillant pour l'employeur.
Données	- identité, coordonnées, fonctions - Vidéosurveillance (liste des caméras transmise au Conseil d'entreprise). - Relevé des actions d'accès (journaux/logs) - Badge - plaque d'immatriculation
Destinataires	- Employeur et conseillers professionnels de l'employeur, y compris service de gestion des accès, service de gardiennage, centre de contrôle, personnel informatique, supérieurs directs...
Durée de conservation	temps nécessaire au traitement des données
Transfert de données vers des pays tiers	Non

- communication interne (*)

Finalité	Diffusion d'informations concernant l'Institution
Personnes concernées	Tout collaborateur disposant d'une adresse mail professionnelle CuSL
Données	<u>Données d'identification personnelles</u> : Identité + Adresse mail
Destinataires	service communication, personnel RH, direction médicale
Durée de conservation	(dépendant de l'activation du compte utilisateur)
Transfert de données vers des pays tiers	Non

(*) Saint-Luc express, agmed, mails aux listes de distribution,...

- outils collaboratifs

Finalité	Gestion de service – agenda - documents messagerie électronique Annuaire téléphonique, liste de gardes
Personnes concernées	Tout collaborateur disposant d'un compte utilisateur et/ou adresse mail CUSL
Données	<u>Données d'identification personnelles</u> : Identité + Adresse mail + compte utilisateur
Destinataires	Le collaborateur + personne déléguée ou mandatée Utilisateurs techniques : Le personnel informatique La cellule de gestion des messageries (UCL) Le sous-traitant pour les solutions externalisées (« dans le cloud ») (Microsoft)
Durée de conservation	1 an fin de contrat

Informations complémentaires	plateforme exchange/outlook, sharepoint, oneDrive, répertoire personnel (Y :), serveur de fichier central
Transfert de données vers des pays tiers	Pour le cloud microsoft (sites en Hollande et en Irlande)

- outils qualité, d'alertes ou de suivi d'interventions

Finalité	Gestion d'intervention, de maintenance et de disponibilité des services
Personnes concernées	Collaborateur
Données	Compte utilisateur + identité dans les échanges et/ou zone texte
Destinataires	Personnel habilité au suivi des incidents
Durée de conservation	En fonction des besoins (30 ans pour alerte environnement zone médicale, pharmacie,...)
Transfert de données vers des pays tiers	Non

(*) exemple de solutions : intervention helpdesk/service. technique, suivi variable d'environnement (t°, tx humidité,...), suivi des événements indésirables ...

- Médecine du travail

Finalité	Suivi légal médecine du travail
Personnes concernées	Tout collaborateur
Données	<u>Données d'identification personnelles</u> : Identité + coordonnées + Adresse mail + Données de santé (dossier médecine du travail et accès au dossier tenu par les CUSL)
Destinataires	Personnel du prestataire de service (CESI), personnel RH pour le suivi administratif
Durée de conservation	(sous la responsabilité du prestataire)
Transfert de données vers des pays tiers	Non

- leasing

Finalité	Gestion des contrats individuels relatifs au leasing
Personnes concernées	Tout collaborateur bénéficiant de ce service
Données	<u>Données d'identification personnelles</u> : Identité + coordonnée (adresse, mail) + plaque d'immatriculation
Destinataires	Personnel de la société prestataire de service, personnel RH, personnel du service de gestion des accès, personnel du service achats et services financiers
Durée de conservation	(dépendant du prestataire de service)
Transfert de données vers des pays tiers	Non

- suivi des formations

Finalité	Gestion des formations
Personnes concernées	Tout collaborateur bénéficiant d'une formation auprès d'un prestataire de service
Données	<u>Données d'identification personnelles</u> : Identité + coordonnée (mail) + fonction + relevé des formations et compétences (option)
Destinataires	Personnel de la société prestataire de service, personnel RH, personnel hiérarchique
Durée de conservation	(dépendant du prestataire de service)
Transfert de données vers des pays tiers	Non

Toutes ces données sont traitées dans le respect des principes de base généraux tels que les principes de finalité et de proportionnalité.

Art. 3 : Responsable du traitement, sous-traitant et délégué à la protection des données

- **Le responsable du traitement** détermine la finalité et les moyens du traitement des données à caractère personnel (*obligation*) = l'employeur

En tant que responsable du traitement, l'employeur s'engage, en application des articles 24 et 25 du RGPD, à prendre des mesures techniques et organisationnelles appropriées afin de garantir l'application et le respect du RGPD. Il s'engage également à mettre en œuvre une politique appropriée en matière de protection des données.

- **Le sous-traitant** est celui qui traite les données à caractère personnel pour le compte du responsable du traitement (*obligation*). Ci-après les principaux sous-traitants :

= Le Département Information et Système des Cliniques universitaires Saint-Luc.

= La Société Popay, assurant le support de la solution HR-Access

= La Société SopraRH, fournisseur de la solution HR-Access

= La Société EasyPay, assurant le transfert des fichiers légaux (Dimona, Dmfa, ONSS,...)

= La Société Talensoft, assurant l'hébergement et la fourniture des services de la plateforme web de gestion du recrutement

= La Société Equinix, assurant l'hébergement et la fourniture des services de la plateforme web de gestion des fiche de paie.

= La société Assusoft, fournisseur de la solution Assusoft

= la société Decis, fournisseur de la solution staffplanner

= la société Joos assurant l'impression, la mise sous enveloppe et l'envoi par la poste des fiches de paie, fiches fiscales et comptes individuels du personnel qui a exprimé son souhait de recevoir ces documents sous format papier

- Le délégué à la protection des données

Désignation d'un délégué à la protection des données : personnel affecté au service sécurité de l'information (rgpd-saintluc@uclouvain.be)

Le délégué à la protection des données est chargé d'informer, de conseiller et de contrôler le respect du RGPD en général. Il coopère avec l'Autorité de Contrôle nationale et agit de manière indépendante. Il assiste et conseille le responsable du traitement.

Le travailleur/collaborateur peut prendre contact à l'adresse rgpd-saintluc@uclouvain.be pour toute question concernant le traitement de ses données à caractère personnel et l'exercice des droits que lui confère le RGPD.

Art. 4 : Droit à l'information

4.1. À travers cette convention vie privée, l'employeur entend fournir au travailleur/collaborateur des informations correctes et exhaustives concernant le traitement de ses données à caractère personnel, le fondement juridique de ce traitement, ses droits, les personnes à contacter.

En marge des raisons légitimant le traitement de certaines données à caractère personnel du travailleur/collaborateur par l'employeur (voir article 1) et sans préjudice de l'article 6, entre autres, du RGPD, en acceptant de collaborer avec l'Institution, le collaborateur fait un acte positif, équivalent à un consentement tacite. Il reconnaît la nécessité de procéder dans le cadre de sa collaboration avec l'employeur aux traitements par l'employeur des données à caractère personnel telles que décrites dans la présente convention vie privée.

4.2. Catégories particulières de données à caractère personnel et consentement explicite

Le traitement de données à caractère personnel révélant 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 santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits, à moins que le

travailleur/collaborateur ne donne son consentement explicite au traitement de ces données pour une finalité spécifique.

Le travailleur/collaborateur donne à l'employeur son consentement explicite, univoque et éclairé en vue du traitement des catégories particulières de données à caractère personnel telles que décrites dans la présente convention vie privé. Le travailleur/collaborateur a le droit de retirer son consentement à tout moment, sur simple demande écrite adressée à l'employeur. L'employeur met alors immédiatement un terme au traitement de ces données à caractère personnel.

Art. 5 : Droits du travailleur/collaborateur

Le responsable du traitement est tenu de prendre les mesures techniques et organisationnelles appropriées afin de garantir la sécurité du traitement des données à caractère personnel du travailleur/collaborateur (art. 32 du RGPD).

5.1. Droit d'accès (art. 15 du RGPD)

Le travailleur/collaborateur a le droit d'accéder aux données à caractère personnel enregistrées. Si le travailleur/collaborateur exerce son droit d'accès et demande des informations complémentaires, le responsable du traitement est tenu de lui fournir une copie des données à caractère personnel traitées. Si le travailleur/collaborateur demande des copies supplémentaires, le responsable du traitement peut exiger le paiement de frais raisonnables, basés sur les coûts administratifs.

5.2. Droit de rectification (art. 16 du RGPD)

S'il constate que des données à caractère personnel sont inexactes, le travailleur/collaborateur a le droit de demander leur rectification immédiate au responsable du traitement.

S'il constate que des données à caractère personnel sont incomplètes, il a également le droit de demander à ce qu'elles soient complétées.

Le responsable du traitement apporte les modifications nécessaires et fournit au travailleur/collaborateur concerné une déclaration complémentaire.

5.3. Droit à l'effacement (« droit à l'oubli ») (art. 17 du RGPD)

Le travailleur/collaborateur a le droit de demander l'effacement de ses données à caractère personnel dans les cas suivants, entre autres :

5. Données à caractère personnel n'étant plus nécessaires au regard des finalités pour lesquelles elles avaient été collectées ou traitées ;
6. Le travailleur/collaborateur s'oppose au traitement ;
7. Les données à caractère personnel ont fait l'objet d'un traitement illicite ;

5.4. Droit à la limitation du traitement (art. 18 du RGPD)

Le travailleur/collaborateur a le droit d'obtenir la limitation du traitement dans les cas suivants, entre autres :

8. L'exactitude des données est contestée par le travailleur/collaborateur et le responsable du traitement a besoin de temps pour vérifier l'exactitude des données à caractère personnel ;
9. Le traitement est illicite et le travailleur/collaborateur ne demande pas l'effacement de ses données à caractère personnel mais une limitation de leur utilisation ;
10. Le responsable du traitement n'a plus besoin des données à caractère personnel mais celles-ci sont encore nécessaires au travailleur/collaborateur pour la constatation, l'exercice ou la défense de droits en justice ;
11. Le travailleur/collaborateur s'est opposé au traitement.

Le responsable du traitement notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées toute rectification (4.2) ou tout effacement (4.3) de données à caractère personnel, ou toute limitation du traitement (4.4), à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. Si le travailleur/collaborateur en fait la demande, le responsable du traitement est tenu de lui fournir des informations sur ces destinataires.

5.5. Droit à la portabilité des données (art. 20 du RGPD)

Le travailleur/collaborateur a le droit de recevoir les données à caractère personnel le concernant traitées par le responsable du traitement dans un format structuré, couramment utilisé et lisible par machine.

Il a également le droit de transmettre ces données à un autre responsable du traitement. Et ce, aux conditions énoncées à l'article 20 du RGPD.

Le travailleur/collaborateur a le droit de demander au responsable du traitement que ces données soient transmises directement à l'autre responsable du traitement lorsque cela est techniquement possible.

Dans tous les cas, le droit à l'effacement des données reste d'application.

5.6. Droit d'opposition (art. 21 et 22 du RGPD)

Le travailleur/collaborateur a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, au traitement de ses données à caractère personnel.

Le responsable du traitement cesse immédiatement le traitement des données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés du travailleur/collaborateur concerné, ou pour la constatation, l'exercice ou la défense de droits en justice.

5.7. Droit d'introduire une réclamation (art. 77 du RGPD)

Le travailleur/collaborateur a le droit d'introduire à tout moment une réclamation auprès de l'Autorité de Contrôle nationale s'il estime que le traitement de ses données à caractère personnel constitue une violation du RGPD.

Si le travailleur/collaborateur introduit une demande dans le cadre des points 4.1 à 4.7 inclus, le responsable du traitement est tenu de fournir les informations demandées dans un délai d'un mois à compter de la réception de la demande. Au besoin, ce délai peut être prolongé de 2 mois compte tenu de la complexité et du nombre de demandes. Le responsable du traitement doit alors informer le travailleur/collaborateur de cette prolongation dans un délai d'un mois à compter de la réception de la demande.

Si le travailleur/collaborateur présente sa demande sous une forme électronique, le responsable du traitement fournit également les informations par voie électronique, à moins que le travailleur/collaborateur ne demande qu'il en soit autrement. (Art. 12 du RGPD)

Art. 6 : Procédure en cas de violation

Il est toujours possible que des données à caractère personnel traitées dans le cadre de la relation de travail tombent dans de mauvaises mains à la suite d'une erreur humaine, d'une erreur informatique, etc. (p.ex. : perte ou vol d'un ordinateur portable/d'une clé USB contenant des données à caractère personnel par un travailleur/collaborateur).

Toute personne constatant une violation, une fuite ou perte de données à caractère personnel doit en avvertir l'employeur (ainsi que le délégué à la protection des données) le plus rapidement possible, en fournissant un maximum d'informations (faits, circonstances, etc.).

L'employeur fait le nécessaire pour notifier la violation en question à l'Autorité de Contrôle dans les 72 heures après en avoir pris connaissance, à moins que la violation ne présente pas un risque élevé pour les droits et libertés du travailleur/collaborateur (art. 32-34 du RGPD).

Lorsque la violation présente un risque élevé pour les droits et libertés du travailleur/collaborateur, l'employeur en informe immédiatement le travailleur/collaborateur concerné. L'employeur informe le travailleur/collaborateur concernant les faits et les mesures prises.