Charte pour la protection des données dans le cadre du RGPD

Septembre 2019

ÉCOLE DES HAUTES ÉTUDES EN SANTÉ PUBLIQUE

EHESP

Table des matières

PRÉAMBULE

La présente charte a été élaborée en vue de définir les engagements pour la protection des données et préciser la mise en place du Règlement Général de Protection des Données – « RGPD » au sein de l'EHESP.
L'EHESP accorde une importance toute particulière à la protection des données personnelles de ses élèves, étudiants, de son personnel, de ses clients, de ses partenaires, ainsi que des utilisateurs de ses sites internet et de ses applications mobiles.
L'EHESP informe des procédés de collecte des données personnelles, de leur utilisation ainsi que des options dont disposent les personnes concernées. Cette charte fera l'objet de modification par l'EHESP en cas d'évolutions réglementaires et ou d'organisations.
L'EHESP respecte la loi « Informatique & Libertés » n° 78-17 du 6 janvier 1978 modifiée, ainsi que la loi « pour la confiance dans l'économie numérique » n° 2004-575 du 21 juin 2004, ainsi que le Règlement Général sur la Protection des Données, n° 2016/679 du 27 avril 2016.
Ce Règlement Général sur la Protection des Données, n° 2016/679 du 27 avril 2016 est devenu applicable dans l'Union Européenne depuis le 25 mai 2018.
Cette politique concerne l'EHESP (sites rennais et parisien), les applications, les logiciels et services édités et/ou utilisant son interface ou ses fonctionnalités.

ARTICLE 1 – DÉFINITION

Le Règlement Général sur la Protection des Données concerne le traitement et la circulation des données à caractère personnel. Il établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la circulation de ces données.
Il protège les libertés et droits fondamentaux des personnes physiques et en particulier leur droit à la protection des données à caractère personnel.
Les principaux objectifs du RGPD sont d'accroître à la fois la protection des personnes concernées par un traitement de leurs données à caractère personnel et de responsabiliser les acteurs de ce traitement.
L'objectif est également d'harmoniser la norme juridique européenne en matière de protection des données personnelles, afin qu'il n'y ait qu'un seul et même cadre s'appliquant à l'ensemble des États membres.

ARTICLE 2 – NOTION DE DONNÉES PERSONNELLES

Une donnée personnelle est une information qui permet d'identifier une personne physique, directement ou indirectement. Il peut s'agir d'un nom, d'une photographie, d'une adresse IP, d'un numéro de téléphone, d'un identifiant de connexion informatique, d'une adresse postale, d'une empreinte de données biométriques, d'un enregistrement vocal, d'un numéro de sécurité sociale, d'une adresse email, de coordonnées bancaires, etc.

Certaines données sont sensibles, car elles touchent à des informations qui peuvent donner lieu à de la discrimination ou des préjugés : une opinion politique, une sensibilité religieuse, un engagement syndical, une appartenance ethnique, une orientation sexuelle, une situation médicale ou des idées philosophiques. Elles constituent des données sensibles.

Elles bénéficient d'une protection particulière qui interdit toute collecte et utilisation de ces données. Le traitement est possible à titre dérogatoire dans certains cas précis et notamment :

- Si la personne concernée a donné son consentement exprès (écrit, clair et explicite) ;
- Si ces données sont nécessaires dans un but médical ou pour la recherche dans le domaine de la santé ;
- Si leur utilisation est justifiée par l'intérêt public et autorisée par la CNIL ;
- Si elles concernent les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique ou syndicale.

ARTICLE 3 – DONNÉES COLLECTÉES AU SEIN DE L'EHESP

La collecte des données personnelles fait l'objet d'une déclaration inscrite dans le registre tenu par le directeur de l'EHESP, responsable du traitement des données et autorité qualifiée en matière de Sécurité et des Systèmes d'Information. Il doit recenser l'ensemble des traitements mis en œuvre par l'EHESP. Le Délégué à la Protection des Données (DPO) est chargé par le Directeur de la tenue de ce registre. Ce registre a été ouvert le 1er janvier 2018. La désignation du DPO, Philippe MARIN a été enregistrée auprès de la CNIL le 29 mars 2018 avec effet au 25 mai 2018. Le DPO peut être contacté par mail à l'adresse fonctionnelle cil@ehesp.fr .

En pratique, une fiche de registre doit donc être établie pour chacune de ces activités (cf Annexe1).

Par ailleurs, l'EHESP a procédé à une déclaration auprès de la CNIL lui permettant d'assurer le traitement comprenant des données de santé réalisées dans le cadre des recherches. Ces déclarations ont été effectuées pour les 6 méthodologies de référence suivantes (cf. annexe 2).

Le consentement

L'EHESP ne collecte aucune donnée personnelle sans recueillir le consentement exprès et avoir donné au préalable des informations concernant notamment le type de données collectées, le lieu de stockage, leurs finalités, le responsable de leur traitement, et les différents droits que les personnes à l'origine des données sont à même d'exercer sur ces dernières.

Par ailleurs, l'EHESP intègre dans chaque convention, contrat ou engagement, un dispositif précisant la protection des données personnelles recueillies.

Des visites du site internet

L'EHESP peut également être amenée à collecter des informations à l'occasion d'échanges divers, ou auprès de sociétés externes via divers formulaires de collecte de données présentés lors de la navigation (cookies, formulaire d'inscription).

Les données collectées dans le cadre des sites internet de l'EHESP le sont dans le cadre du respect des principes énoncés dans la présente charte, notamment en ce qui concerne la finalité et la durée de conservation de ces données.

ARTICLE 4 – L'OBLIGATION D'INFORMATION ET LE RESPECT DU CONSENTEMENT

À chaque collecte de données, la personne concernée doit être informée du fondement juridique sur lequel le traitement est effectué, de ses droits sur le traitement (limitation, portabilité et recours) et des modalités exactes du traitement de ses données.
Ces informations doivent être visibles et accessibles sur le site internet où les données sont collectées, ou le cas échéant, sur les supports qui permettent la collecte des données, des contrats signés, etc.
La protection des mineurs de moins de 16 ans et des majeurs protégés, est également renforcée. Le consentement du titulaire de l'autorité parentale doit être donné.

ARTICLE 5 – FINALITÉS DES DONNÉES COLLECTÉES

Seules les données nécessaires et pertinentes au regard des finalités poursuivies sont collectées, dans le respect du principe de proportionnalité en fonction du but de la collecte des données concernées.
L'EHESP ne collectera que les données adéquates, pertinentes et strictement nécessaires à la finalité du traitement.

ARTICLE 6 – UTILISATION DES DONNÉES COLLECTÉES

Les données collectées par l'EHESP sont traitées pour les besoins d'exécution de ses différentes activités.

Le traitement des données personnelles est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement…).

Le traitement des données personnelles doit avoir un objectif, une finalité, c'est-à-dire que l'on ne peut pas collecter ou traiter des données personnelles simplement au cas où elles seraient utiles un jour. A chaque traitement des données personnelles doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de votre activité professionnelle.

ARTICLE 7 – SÉCURITÉ DES DONNEES PERSONNELLES

Les données personnelles recueillies par l'EHESP ne sont en aucun cas cédées, louées ou échangées. Toutefois les données personnelles pourront être divulguées en application d'une loi, d'un règlement ou en vertu d'une décision d'une autorité réglementaire ou judiciaire compétente ou encore, si cela s'avère nécessaire, aux fins de préserver les droits et intérêts des personnes.
Tout utilisateur disposant d'un compte est invité à se connecter avec un identifiant fourni par l'EHESP et un mot de passe provisoire à modifier à la 1ère connexion. Ce mot de passe doit impérativement rester secret et il doit limiter l'accès à son ordinateur ou aux appareils mobiles et se déconnecter à la fin de l'utilisation des services.
Les données personnelles étant confidentielles, l'EHESP limite leur accès aux seuls collaborateurs de l'EHESP ou prestataires ayant besoin d'en connaitre dans le cadre de l'exécution du traitement.
Toutes les personnes ayant accès aux données personnelles sont liées par le devoir de confidentialité et s'exposent à des mesures disciplinaires et/ou autres sanctions si elles ne respectent pas ces obligations.
Tout utilisateur est informé du fait que sans des mesures de sécurité adéquates, il court le risque que les données et les mots de passe qu'il utilise pour protéger ses données puissent être divulgués à des tiers non autorisés.
(Exemples : configuration sécurisée d'un navigateur web, mise à jour des programmes anti-virus, logiciel pare-feu, utilisation de logiciels provenant de sources douteuses, etc…).

ARTICLE 8 – DURÉE DE CONSERVATION DES DONNEES PERSONNELLES

Les données personnelles sont stockées et conservées pour la durée nécessaire à la réalisation des finalités visées.
Les données personnelles seront ainsi conservées pour la période pendant laquelle les personnels de l'EHESP utilisent les services support desdites données.
Conformément au RGPD, à l'issue de cette durée de conservation préfixée, les données sont détruites.

ARTICLE 9 – LES DROITS CONCERNÉS

L'EHESP garantit les droits d'accès, de rectification et d'opposition des données personnelles qui existaient déjà avant l'application du RGPD.
L'EHESP garantit également le droit à la limitation du traitement, le droit à l'oubli, le droit à la portabilité et le droit à l'effacement des données personnelles.

L'EHESP entend respecter l'intégralité des droits à l'égard du traitement des données personnelles vis-à-vis des personnels, élèves, étudiants, et tiers :

- le droit d'être informé sur l'utilisation des données personnelles
- le droit d'accéder aux informations personnelles recueillies auprès des personnels, élèves, étudiants, et tiers
- le droit de demander la correction des données personnelles inexactes, incomplètes, équivoques ; périmées pour personnels, élèves, étudiants, et tiers
- la possibilité d'exiger la transférabilité au titre du droit à la portabilité des données personnelles à un autre fournisseur/utilisateur de service ;
- le droit de déposer le cas échéant des plaintes justifiées et dûment motivées auprès de l'autorité nationale en charge de la protection des données personnelles.

ARTICLE 10 – SANCTION EN CAS DE NON-CONFORMITÉ

En cas de manquement aux obligations imposées par le RGPD, les titulaires des données personnelles concernés peuvent se voir infliger une amende pouvant atteindre 20 millions d'euros ou 4% du chiffre d'affaires mondial pour les entités les plus importantes.
La CNIL pourra également émettre des sanctions en cas de violation de la réglementation comme des mises en demeure ou des avertissements.

ARTICLE 11 – INFORMATION DES PERSONNELS, ELEVES, ETUDIANTS, ET TIERS ET PUBLICITÉ

La présente charte, validée par le Comité de Direction dans sa séance du 16 septembre 2019, sera affichée publiquement et communiquée individuellement à chaque personnels, élèves, étudiants, et tiers. Elle sera également disponible sur le site internet de l'EHESP.

ARTICLE 12 – ENTRÉE EN VIGUEUR DE LA CHARTE

La présente charte est applicable dès la date de sa publication.

Fait à *Rennes*, le 30 septembre 2019.

Annexe 1

FICHE DE REGISTRE			
N° FDR	5_	Nom	
Date de création		Date révision	
Responsable du traitement	Laurent Chambaud	Agit en tant que sous-traitant	
Représentant du RT			
Représentant RT du ST			
Responsables conjoints			
DPO ou Référent DCP	Philippe MARIN		
Nom de l'application			
Gestionnaire des droits d'accès			
Traitement hors UE			
SI LE TRAITEMENT EST SOUS TRAITE (Note : une sauvegarde externalisée est un traitement sous-traité)			
Nom du sous-traitant			
Nom de la personne qui gère le contrat			
Le contrat précise la finalité du traitement et la catégorie de données			
Le contrat définit les obligations du sous-traitant au regard des droits des personnes			
FINALITES DU TRAITEMENT (Quel est (sont) l'objectif (s) poursuivi (s) ?)			
Art. 6 Le traitement est licite si au moins une des conditions suivantes est remplie (Choisir le plus approprié)			
CATEGORIE DE PERSONNES CONCERNEES PAR LE TRAITEMENT			
CATEGORIE DE DONNEES			
DCP			
Sensibilité			
Durée de conservation			
CATEGORIE DES DESTINATAIRES DU TRAITEMENT			
GESTION DES 12 DROITS ET PRINCIPES ATTACHES AUX PERSONNES CONCERNEES			
L'information est concise pour l'exercice des droits par la personne concernée (M01)			
La finalité est déterminée, explicite et légitime (M02)			
Les données collectées sont réduites au minimum nécessaire (M03)			
En absence de fondement légal, de contrats, d'intérêts vitaux, obtention du consentement (M04)			
L'intégrité des données est garantie (M05)			
La durée de conservation est justifiée au regard de la finalité et communiquée (M06)			

L'opposition au traitement est exerçable (M07)	
Sur demande de la personne concernée, le traitement peut être limité (M08)	
Sur demande, les données sont rectifiables et/ou effaçables (M09)	
Sur demande, la personne concernée peut accéder à ses données (M10)	
Les données sont portables dans un format acceptable par la personne concernée (M11)	
Transfert hors UE vers un destinataire non conforme RGPD impossible sans l'accord de la personne concernée (M12)	
9 MESURES DE PROTECTION DES DONNEES	
L'accès physique aux locaux contenant des équipements numériques DCP est contrôlé (M13)	
Les actifs numériques traitant de DCP sont protégés contre les malwares et les attaques logiques (M14)	
Les utilisateurs en situation de mobilité sont sensibilisés au vol et à l'écoute et observation passive (M15)	
Les données sont sauvegardées et des tests de restauration effectués (M15)	
Les utilisateurs sont formés aux outils et vigilants dans leurs usages et leurs manipulation (M16)	
Les gestionnaires de droits d'accès aux outils et aux DCP sont formellement identifiés (M17)	
L'extraction et l'export de DCP sont contrôlés (M06)	
Les services en ligne, les échanges ou transferts sur les réseaux sont protégés contre l'interception (M18)	
La gestion des flux de données est cartographiée pour contrôler les transferts ou traitements hors UE(M12)	
PRIVACY IMPACT ASSESSMENT	
Détermination	
Décision	
Commentaire (*hors zone d'impression*) :	

Ce registre doit comporter le nom et les coordonnées pour chaque activité de traitement, la fiche du registre doit comporter au moins les éléments suivants :

- le cas échéant, le nom et les coordonnées du responsable conjoint du traitement mis en œuvre
- les finalités du traitement, l'objectif en vue duquel les données ont été collectées
- les catégories de personnes concernées (client, prospect, employé, etc.)
- les catégories de données personnelles (exemples : identité, situation familiale, économique ou financière, données bancaires, données de connexion, donnés de localisation, etc.)
- les catégories de destinataires auxquels les données personnelles ont été ou seront communiquées, y compris les sous-traitants auxquels vous recourez
- les transferts de données personnelles vers un pays tiers ou à une organisation internationale et, dans certains cas très particuliers, les garanties prévues pour ces transferts
- les délais prévus pour l'effacement des différentes catégories de données personnelles, c'est-à-dire la durée de conservation, ou à défaut les critères permettant de la déterminer
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles que vous mettez en œuvre.

Annexe 2

- MR-001 RECHERCHES DANS LE DOMAINE DE LA SANTÉ AVEC RECUEIL DU CONSENTEMENT Délibération n° 2018-153 du 3 mai 2018
- MR-002 ÉTUDES NON INTERVENTIONNELLES DE PERFORMANCES CONCERNANT LES DISPOSITIFS MÉDICAUX DE DIAGNOSTIC IN VITRO Délibération n° 2015-256 du 16 juillet 2015 portant homologation d'une méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des études non interventionnelles de performances en matière de dispositifs médicaux de diagnostic ...
- MR-003 RECHERCHES DANS LE DOMAINE DE LA SANTÉ SANS RECUEIL DU CONSENTEMENT Délibération n° 2018-154 du 3 mai 2018
- MR-004 RECHERCHES N'IMPLIQUANT PAS LA PERSONNE HUMAINE, ÉTUDES ET ÉVALUATIONS DANS LE DOMAINE DE LA SANTÉ Délibération n° 2018-155 du 3 mai 2018
- MR-005 ÉTUDES NÉCESSITANT L'ACCÈS AUX DONNÉES DU PMSI ET/OU DES RPU PAR LES ÉTABLISSEMENTS DE SANTÉ ET LES FÉDÉRATIONS HOSPITALIÈRES Délibération n° 2018-256 du 7 juin 2018
- MR-006 ÉTUDES NÉCESSITANT L'ACCÈS AUX DONNÉES DU PMSI PAR LES INDUSTRIELS DE SANTÉ Délibération n° 2018-257 du 7 juin 2018 portant homologation d'une méthodologie de référence relative aux traitements de données nécessitant l'accès pour le compte des personnes produisant ou commercialisant des produits mentionnés au II de l'article L. 5311-1 du code de la santé publique aux données.