



Alexis Astruc^{1,2,3}, Adeline Jouannin^{4,5,6}, Erik Lootvoet¹, Timothée Bonnet⁷, Frederic Chevallier^{1,8}

- 1.. Université Sorbonne Paris Nord, Département universitaire de Médecine générale, DUMG, F-93000 Bobigny
- 2.. Centre de santé Ellasanté, F-75008, Paris
3. Maison de santé Orly Santé, F-94310, Orly
4. Département de médecine générale, Université de Rennes, F-35000 Rennes.
5. Centre d'investigation clinique de Rennes (CIC Inserm 1414), Université de Rennes, CHU Rennes, Inserm, F-35000 Rennes.
- 6.. Centre de recherche des Cordeliers (UMRS1138), INSERM, Sorbonne Université, USPC, Université Paris-Descartes, Université Paris-Diderot, équipe ETREs, F-75006 Paris.
7. Université Sorbonne Paris Nord, Service des archives, F-93430 Villetaneuse
8. MUSSP, 14 rue de la république, 95120 Ermont

alexis.astruc@yahoo.fr
exercer 2021 ; 172:178-84.

Les données à caractère personnel : quelles formalités réglementaires pour les travaux de recherche en médecine générale ?

Personal data: what are the regulatory requirements for research work in general medicine?

Annexe 4 - Exemple de page d'inscription au registre des traitements

Date de création de la fiche	
Date de dernière mise à jour de la fiche	
Nom du responsable conjoint du traitement (dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)	
Nom du logiciel ou de l'application (si pertinent)	

OBJECTIFS POURSUIVIS

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.

CATÉGORIES DE PERSONNES CONCERNÉES

Listez les différents types de personnes dont vous collectez ou utilisez les données.

Exemples : salariés, usagers, clients, prospects, bénéficiaires, etc.

CATÉGORIES DE DONNÉES COLLECTÉES

Cochez et listez les différentes données traitées

- État-civil, identité, données d'identification, images (ex. nom, prénom, adresse, photographie, date et lieu de naissance, etc.)
- Vie personnelle (ex. habitudes de vie, situation familiale, etc.)
- Vie professionnelle (ex. CV, situation professionnelle, scolarité, formation, distinctions, diplômes, etc.)
- Informations d'ordre économique et financier (ex. revenus, situation financière, données bancaires, etc.)
- Données de connexion (ex.

adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)

- Données de localisation (ex. déplacements, données GPS, GSM, ...)
- Internet (ex. cookies, traceurs, données de navigation, mesures d'audience, ...)
- Autres catégories de données (précisez) :

DES DONNÉES SENSIBLES SONT-ELLES TRAITÉES ?

La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions poli-

tiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).

Oui Non

Si oui, lesquelles ? :

DURÉES DE CONSERVATION DES CATÉGORIES DE DONNÉES

Combien de temps conservez-vous ces informations ?

... Jours,
... Mois,
... Ans,
... Autre durée :

Si vous ne pouvez pas indiquer une durée chiffrée, précisez les critères utilisés pour déterminer le délai d'effacement (par exemple, 3 ans à compter de la fin de la relation contractuelle).

Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre.

CATÉGORIES DE DESTINATAIRES DES DONNÉES

Destinataires internes
(Exemples : entité ou service, catégories de personnes habilitées, direction informatique, etc.)

Organismes externes
(Exemples : filiales, partenaires, etc.)

Sous-traitants
(Exemples : hébergeurs, prestataires et maintenance informatiques, etc.)

TRANSFERTS DES DONNÉES HORS UE

Des données personnelles sont-elles transmises hors de l'Union européenne ?

Oui Non

Si oui, vers quel(s) pays :

Dans des situations particulières (transfert vers un pays tiers non couvert par une décision d'adéquation de la Commission européenne, et sans les garanties mentionnées aux articles 46 et 47 du RGPD), des garanties spécifiques devront être prévues et documentées dans le registre (article 49 du RGPD). Consultez le site de la CNIL.

MESURES DE SÉCURITÉ

Cochez et décrivez les mesures de sécurité organisationnelles et techniques prévues

pour préserver la confidentialité des données.

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.

Contrôle d'accès des utilisateurs

Décrivez les mesures :

Mesures de traçabilité

Précisez la nature des traces (exemple : journalisation des accès des utilisateurs), les données enregistrées (exemple : identifiant, date et heure de connexion, etc.) et leur durée de conservation :

Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Décrivez les mesures :

Sauvegarde des données

Décrivez les modalités :

Chiffrement des données

Décrivez les mesures (exemple : site accessible en https, utilisation de TLS, etc.) :

Contrôle des sous-traitants

Décrivez les modalités :

Autres mesures :