Bird & Bird

New French CNIL standard on health vigilance activities (e.g. pharmacovigilance, materiovigilance, etc.)

Unofficial English translation

French	English
Délibération n° 2019-057 du 9 mai 2019 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre à des fins de gestion des vigilances sanitaires	*Deliberation No. 2019-057 of May 9, 2019 adopting a standard relating to the processing of personal data implemented for health vigilance management purposes*
1. A qui s'adresse ce référentiel? Ce référentiel encadre exclusivement les traitements de données à caractère personnel : - constitués pour gérer les vigilances sanitaires ; - et mis en œuvre par des fabricants, entreprises, exploitants, organismes responsables de la mise sur le marché d'un médicament, d'un dispositif ou d'un produit et dénommés, ci-après, responsables de traitement. Par application des dispositions du 1° de l'article 65 de la loi du 6 janvier 1978 modifiée, les traitements de données à caractère personnel mis en œuvre par les professionnels de santé et les systèmes ou services de soins de santé (p. ex. : établissements de santé, maisons de santé, centres de santé, agences sanitaires, etc.) ne sont pas concernés par ce référentiel.	**1. Who is this standard for?** This standard exclusively governs the processing of personal data: - set up to manage health vigilance; and - implemented by manufacturers, companies, operators, bodies responsible for the placing on the market of a medicine, device or product, and hereinafter referred to as controllers. In accordance with the provisions of article 65, paragraph 1, of the Act of 6 January 1978 amended [French Data Protection Act], the processing of personal data by health care professionals and health care systems or services (e. g. health establishments, healthcare homes, health centres, health agencies, etc.) are not covered by this standard.
2. Portée du référentiel Ce référentiel précise le cadre juridique, issu du règlement général sur la protection des données (RGPD) et des dispositions nationales, applicable aux traitements de données à caractère personnel constitués dans le cadre des vigilances sanitaires. Il couvre le périmètre des vigilances sanitaires mentionnées dans l'arrêté du 27 février 2017 fixant la liste des catégories d'événements sanitaires indésirables pour lesquels la déclaration ou le signalement peut s'effectuer au moyen du portail de signalement des événements sanitaires indésirables.	**2. Scope of the standard** This standard specifies the legal framework, based on the General Data Protection Regulation (GDPR) and national provisions applicable to the processing of personal data in the context of health vigilance. It covers the scope of health vigilance mentioned in the arrêté of 27 February 2017 establishing the list of categories of adverse health events for which the notification or reporting can be done through the portal for reporting adverse health events.

Les responsables de traitement qui adressent à la CNIL une déclaration de conformité, pour les traitements de données à caractère personnel répondant aux exigences fixées par le présent référentiel, via le formulaire de déclaration de conformité à remplir sur le site internet de la CNIL, sont autorisés à les mettre en œuvre.

Tout traitement de données à caractère personnel qui excède le cadre ou les exigences définis par le présent référentiel doit en revanche faire l'objet d'une demande d'autorisation spécifique conformément aux dispositions de l'article 66-III de la loi du 6 janvier 1978 modifiée.

Les responsables de traitement doivent mettre en œuvre toutes les mesures appropriées (techniques et organisationnelles) afin de garantir la protection des données personnelles traitées, à la fois dès la conception du traitement et par défaut. Ils doivent, en outre, démontrer cette conformité tout au long de la vie des traitements. Les traitements mis en œuvre dans le cadre du référentiel doivent également être inscrits dans le registre des activités de traitement prévu à l'article 30 du RGPD (voir les modèles de registres sur le site cnil.fr).

Les principes dégagés par la CNIL, dans ce référentiel, constituent une aide à la réalisation de l'analyse d'impact à la protection des données que les responsables de traitement concernés doivent mener. Les responsables de traitement pourront ainsi définir les mesures leur permettant d'assurer la proportionnalité et la nécessité de leurs traitements (points 3 à 7 du référentiel), de garantir les droits des personnes (points 8 et 9 du référentiel) et la maîtrise de leurs risques (points 10 à 12 du référentiel).

Data controllers who send the CNIL a declaration of conformity for the processing of personal data meeting the requirements set by this standard, using the declaration form to be filled on the CNIL's website, are authorised to perform the processing of personal data.

Any processing of personal data that goes beyond the framework or requirements set out in this standard must, however, be the subject of a specific authorisation request in accordance with the provisions of Article 66-III of the Act of 6 January 1978 amended [French Data Protection Act].

Data controllers must put in place all appropriate measures (technical and organisational) to ensure the protection of the personal data they process, both at the design stage of processing and by default. They must also demonstrate compliance throughout the lifetime of the processing. The processing carried out within the framework of this standard must also be entered in the record of processing activities provided for in Article 30 of the GDPR (see the templates for records on the CNIL's website cnil.fr).

The principles identified by the CNIL in this standard constitute an aid to the completion of a data protection impact assessment that data controllers must carry out. Data controllers will thus be able to define measures to ensure the proportionality and necessity of their processing (points 3 to 7 of the standard), guarantee the rights of individuals (points 8 and 9 of the standard) and control their risks (points 10 to 12 of the standard).

3. Objectif(s) poursuivi(s) par le traitement (FINALITÉS)

Un traitement mis en œuvre aux fins de gestion des vigilances sanitaires a pour finalité de permettre la prévention, la surveillance, l'évaluation, la gestion des événements sanitaires indésirables mis en place par le responsable de traitement.

Le traitement vise à permettre :

- la collecte, l'enregistrement, l'analyse, le suivi, la documentation, la transmission et la conservation des données relatives à l'ensemble des événements sanitaires indésirables ;

- la gestion des contacts, par le responsable de traitement, avec la personne lui ayant notifié l'événement sanitaire indésirable (membre d'une association agréée, professionnel de santé, membre d'une autorité sanitaire, patient, etc.) ou le professionnel de santé pouvant être interrogé pour obtenir, dans le respect du secret médical, des précisions sur l'événement sanitaire indésirable signalé (professionnel suivant la personne victime de l'événement sanitaire indésirable, etc.).

Les informations recueillies pour ces finalités ne pourront pas être réutilisées pour poursuivre une autre finalité que celle prévue dans le cadre du présent référentiel.

3. Purpose(s) of the processing (PURPOSES)

The purpose of a processing implemented to manage health vigilance is to enable the prevention, monitoring, evaluation and management of adverse health events set up by the controller.

The processing is to allow:

- the collection, recording, analysis, monitoring, documentation, transmission and storage of data relating to all adverse health events;

- the management of the contacts by the controller with the person who reported the adverse health event (member of an approved association, health professional, member of a health authority, patient, etc.) or the health professional who may be interviewed to obtain, in compliance with medical secrecy, details of the reported adverse health event (professional taking care of the person who suffered the adverse health event, etc.).

The information collected for these purposes cannot be reused for any purpose other than that provided for in the framework of this standard.

4. Base(s) légale(s) du traitement

Dans le cadre des vigilances sanitaires entrant dans le champ du présent référentiel, le respect des obligations légales imposées au responsable de traitement par les dispositifs de vigilance sanitaire prévus notamment par le code de la santé publique est retenu comme base légale du traitement de données à caractère personnel constitué.

La collecte de données de santé dans le cadre des vigilances sanitaires est nécessaire pour des motifs d'intérêt public ; elle a notamment pour objectif de garantir le respect de normes élevées de qualité et de sécurité des soins de santé et des médicaments, des dispositifs ou des produits conformément aux dispositions de l'article 9 du RGPD et de l'article 66 de la loi du 6 janvier 1978 modifiée.

4. Legal basis for the processing

In the context of health vigilance falling within the scope of this standard, compliance with the legal obligations imposed on the controller by health vigilance regulations provided for in particular by the Public Health Code is considered as the legal basis for the processing of personal data.

The collection of health data in the context of health vigilance is necessary for reasons of public interest; in particular it aims to ensure compliance with high standards of quality and safety of health care and medicinal products, devices or products, in accordance with the provisions of Article 9 of the GDPR and Article 66 of the Act of 6 January 1978 amended [the French Data Protection Act].

5. Données personnelles concernées

Seules des données pertinentes au regard de l'objectif du traitement, à savoir la gestion des vigilances sanitaires, peuvent être collectées et traitées.

A ce titre, le responsable de traitement peut collecter et traiter, en fonction de l'objectif poursuivi par le traitement et des situations :

a) Les données relatives à la personne exposée strictement nécessaires à l'appréciation de l'événement sanitaire indésirable :

- données permettant d'identifier indirectement la personne exposée à l'événement sanitaire indésirable (informations signalétiques telles que l'âge, l'année ou la date de naissance, le sexe, le poids, la taille) ou numéro d'identification de la personne (code alphanumérique, code alphabétique d'identification tel que prévu par les formulaires existant) permettant de garantir le respect de sa vie privée, à l'exclusion du numéro d'inscription au répertoire national d'identification des personnes physiques et de l'identifiant national de santé;

- données relatives à l'identification du produit concerné par le signalement de l'événement sanitaire indésirable : type de médicament, de dispositif ou de produit utilisé, numéro de série, etc.;

- données de santé, notamment : traitements administrés, résultats d'examens, nature du ou des effets indésirables, antécédents personnels ou familiaux, maladies ou événements associés, facteurs de risques, informations relatives au mode de prescription et d'utilisation des médicaments et à la conduite thérapeutique du prescripteur ou des professionnels de santé intervenant dans la prise en charge de la maladie ou de l'événement sanitaire indésirable.

En complément de ces données, le responsable de traitement peut également collecter et traiter d'autres données sous réserve qu'elles soient strictement nécessaires à l'appréciation de l'événement sanitaire indésirable (vie professionnelle, consommation de tabac, alcool, drogue, habitudes de vie et comportements).

5. Personal data concerned

Only data relevant to the purpose of the processing, namely the management of health vigilance, can be collected and processed.

In this respect, the controller may collect and process, depending on the purpose of the processing and the situations:

a) Data relating to the affected person, strictly necessary for the assessment of the adverse health event:

- data allowing for the indirect identification of the person exposed to the adverse health event (identifying information such as age, year or date of birth, sex, weight, height) or the person's identification number (alphanumeric code, alphabetical identification code as provided for in the existing forms) to ensure the respect of the person's privacy, excluding the registration number in the national register of natural persons and the national health identifier;

- data relating to the identification of the product concerned by the adverse health event report: type of medicinal product, device or product used, serial number, etc.;

- health data, including: administered treatments, test results, nature of the adverse effect(s), personal or family history, associated diseases or events, risk factors, information on how medicinal products are prescribed and used and on the therapeutic conduct of the prescriber or of the health professionals involved in the management of the disease or adverse health event.

In addition to this data, the controller may also collect and process other data under the condition that such data be strictly necessary for the assessment of the adverse health event (professional life, tobacco consumption, alcohol, drugs, lifestyle and behaviour).

Des données relatives à l'origine ethnique peuvent être collectées par le responsable de traitement lorsqu'un document de présentation des caractéristiques du médicament, du dispositif ou du produit validé par une autorité compétente (p. ex. : résumé des caractéristiques du produit pour les médicaments, résumé des caractéristiques du dispositif médical, etc.) fait état, en s'appuyant sur des travaux scientifiques, de la circonstance que l'origine ethnique des personnes peut avoir une incidence sur son efficacité ou sa sécurité.	Data relating to ethnic origin can be collected by the controller when a document presenting the characteristics of the medicinal product, device or product validated by a competent authority (e.g. summary of product characteristics for medicinal products, summary of medical device characteristics, etc.) indicates, on the basis of scientific work, that the ethnic origin of the persons may have an impact on its effectiveness or safety.
b) Les coordonnées de la personne ayant procédé à la notification de l'événement sanitaire indésirable ou de tout professionnel de santé susceptible d'apporter des précisions (nom, prénom, coordonnées postales, électroniques, téléphoniques, le cas échéant spécialité du professionnel de santé). Selon les situations, la personne ayant procédé à la notification peut être : le membre d'une autorité sanitaire, un professionnel de santé, la personne exposée à l'événement sanitaire indésirable ou son entourage, le(s) titulaire(s) de l'autorité parentale, l'ayant droit en cas de décès, une association de patients agréée, etc.	**b)** The contact details of the person who reported the adverse health event or of any health care professional likely to provide details (surname, first name, postal and electronic address, telephone number and, where applicable, speciality of the health care professional). Depending on the situation, the person who made the report may be: a member of a health authority, a health care professional, the person affected by the adverse health event or their relatives, the legal guardian(s), the beneficiary in the event of death, an approved patient association, etc.
La notification de l'événement sanitaire indésirable, qui serait réalisée directement par la personne exposée, a pour effet de lever le secret de son identité, et doit être limitée à ce que le responsable de traitement a besoin de connaître pour satisfaire à ses obligations en matière de vigilances sanitaires et pour une durée strictement limitée à ce qui est nécessaire pour répondre auxdites obligations.	The reporting of the adverse health event that would be made directly by the affected person, has the effect of lifting the secrecy regarding his or her identity, and must be limited to what the controller needs to know in order to comply with its obligations regarding health vigilance and for a period of time strictly limited to what is necessary to comply with those obligations.
6. Destinataires des données	**6. Data recipients**
Seuls les employés habilités du responsable de traitement doivent pouvoir, sous la responsabilité de ce dernier, accéder aux données à caractère personnel traitées, dans la limite de leurs attributions respectives et pour ce qui les concerne, notamment:	Only authorised employees of the controller, acting under the responsibility of the latter, can have access to the processed personal data, within the limits of their respective assignments and in particular:
- le responsable de la vigilance, ainsi que ses collaborateurs et agents intervenant dans le processus de gestion des vigilances sanitaires ;	- the person in charge of vigilance, as well as their collaborators and agents involved in the process of managing health vigilance;
- les personnels du service des audits, de manière ponctuelle et motivée, pour vérifier le respect des exigences réglementaires ;	- audit department staff, on an occasional and reasoned basis, to verify compliance with regulatory requirements;
- les personnels habilités en charge de la gestion des réclamations, en fonction des dossiers qu'elles ont à traiter.	- the authorised staff in charge of managing complaints, depending on the cases they have to deal with.
Peuvent également être destinataires des données nécessaires à l'exercice de leurs missions, exclusivement dans le cadre de leur activité de vigilance :	May also be recipients of the data necessary for the performance of their missions, exclusively as part of their vigilance activity:
- les sous-traitants intervenant pour le compte et sous la responsabilité de l'organisme, dans la limite de leurs fonctions et dans les conditions définies par le contrat de sous-traitance. En cas de recours à un sous-traitant, le contrat qui lie le responsable de traitement au sous-traitant doit faire mention des obligations qui lui incombent en matière de protection des données (article 28 du RGPD). Le guide du sous-traitant édité	- processors acting on behalf of and under the responsibility of the organisation, within the limits of their functions and under the conditions defined by the data processing agreement. In the event a processor is engaged, the contract between the controller and the processor must mention their data protection obligations (Article 28 of the GDPR).

par la CNIL précise ses obligations et les clauses à intégrer dans les contrats; - les autres sociétés du groupe auquel l'organisme appartient qui participent à l'exploitation ou à la commercialisation du médicament, du dispositif ou du produit mis en cause ; - les tiers dont un médicament, un dispositif ou un produit pourrait être mis en cause, à l'exception des données directement identifiantes de la personne exposée à l'événement sanitaire indésirable qui aurait notifié l'événement ; - les professionnels de santé participant au suivi du patient et les professionnels de santé ou autres professionnels pouvant apporter un complément ; - les organismes notifiés en charge de l'évaluation d'un médicament, d'un dispositif ou d'un produit, à l'exception des données directement identifiants de la personne exposée à l'événement sanitaire indésirable qui aurait notifié l'événement ; - les organismes publics nationaux (p. ex. : agences régionales de santé, agences sanitaires, etc.) ou étrangers en charge des vigilances dans le cadre de l'exercice de leurs missions telles que définies par les textes, les autorités ou agences sanitaires nationales étrangères et les autorités ou agences sanitaires internationales (p. ex. : Agence européenne des médicaments), à l'exception des données directement identifiantes de la personne exposée à l'effet indésirable qui aurait notifié l'événement.	The Processor's Guide published by the CNIL specifies the processor's obligations and the clauses to be included in the contracts; - other companies in the group to which the organisation belongs which are involved in the exploitation or marketing of the medicinal product, device or product in question; - third parties whose medicinal product, device or product could be implicated, with the exception of directly identifying data of the person affected by the adverse health event who reported the event; - health care professionals involved in patient follow-up and health professionals or other professionals who can provide additional information; - the notified bodies in charge of the evaluation of a medicinal product, device or product, with the exception of directly identifying data of the person exposed to the adverse health event who reported the event; - national (e.g. regional health agencies, health agencies, etc.) or foreign public bodies in charge of vigilance in the exercise of their tasks as defined by law, foreign national health authorities or agencies and international health authorities or agencies (e.g. European Medicines Agency), with the exception of directly identifiable data of the person exposed to the adverse reaction who reported the event.
7. Durées de conservation Les données collectées et traitées pour gérer les vigilances sanitaires ne peuvent être conservées de façon indéfinie. Une durée de conservation précise doit être préalablement fixée en fonction de la finalité du traitement. Au regard des finalités du traitement, les données sont conservées en base active pendant la durée d'utilisation courante des données. Elles sont ensuite conservées en archivage intermédiaire pendant la durée légale ou réglementaire applicable à chaque vigilance sanitaire. En l'absence de durée légale ou réglementaire, les données ne peuvent être conservées au-delà d'une période de soixante-dix ans à compter de la date du retrait du marché du médicament, du dispositif ou du produit. A l'expiration de ces délais, les données sont supprimées ou archivées sous une forme anonymisée. La conservation et l'archivage des données doivent être réalisés dans des conditions de sécurité conformes aux dispositions de l'article 32 du RGPD.	**7. Retention periods** Data collected and processed to manage health vigilance cannot be stored indefinitely. A specific storage period must be fixed in advance, depending on the purpose of the processing. With regard to the purposes of the processing, the data are kept in an active database for the duration of the current use of the data. They are then kept in intermediate storage for the legal or regulatory period applicable to each health vigilance. In the absence of a legal or regulatory period, the data may not be stored for more than 70 years from the date on which the medicinal product, device or product is withdrawn from the market. At the end of these periods, the data must be deleted or archived in an anonymized form. The storage and archiving of data must be carried out under security conditions compliant with the provisions of Article 32 of the GDPR.

8. Information des personnes

Un traitement de données à caractère personnel doit être mis en œuvre en toute transparence vis-à-vis des personnes concernées (personnes exposées à l'événement sanitaire indésirable, personne ayant notifié l'événement sanitaire indésirable et professionnel de santé ayant suivi la personne concernée par l'événement). Le responsable de traitement prend les mesures appropriées pour fournir à la personne concernée une information concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples.

Dès le stade de la collecte, les personnes concernées par le traitement doivent être individuellement informées des modalités de traitement de leurs données dans les conditions prévues par les articles 13, le cas échéant, 14 du RGPD, 69 et 70 de la loi Informatique et libertés.

En cas de notification de l'événement sanitaire indésirable par la personne qui y est exposée, une information particulière doit lui être fournie préalablement, afin de l'informer que le secret de son identité ne sera pas préservé.

Le support d'information est libre (oral ou écrit).

Si la personne concernée en fait la demande, elle peut obtenir la mise à disposition d'un support d'information écrit.

En cas de notification de l'événement sanitaire indésirable par une personne autre que celle qui y est exposée, l'information est réalisée par le notificateur sur la base des éléments d'information écrits remis par le responsable de traitement au notificateur.

Le responsable de traitement doit à tout moment justifier que l'information des personnes concernées a été délivrée, à charge pour le responsable de traitement de recueillir auprès du notificateur la preuve de cette délivrance.

Les personnes concernées doivent par ailleurs être informées de la manière d'exercer leurs droits.

8. Information of the subjects

Processing of personal data must be done in a transparent way vis-a-vis the data subjects (persons exposed to the adverse health event, persons who reported the adverse health event and health care professionals taking care of the person concerned by the event). The controller shall take appropriate measures to provide the data subject with concise, transparent, comprehensible and easily accessible information in clear and simple terms.

Starting from the collection stage, the data subjects must be individually informed of the characteristics of the processing of their data in accordance with Articles 13, and where applicable articles 14 of the GDPR, 69 and 70 of the [French] Data Protection Act].

In the event of a notification of the adverse health event by the person exposed to it, specific and prior information must be provided, in order to inform that person that the secrecy regarding their identity will not be preserved.

The information can be provided in any medium (oral or written).

At the data subject's request, the information shall be provided in writing.

In the event of notification of the adverse health event by a person other than the person exposed to it, the information shall be provided by the notifying person on the basis of the written information provided by the controller to the notifying person.

The controller must at all times prove that the data subjects have been provided with the information, and it is up to the controller to obtain proof of this provision from the notifying person.

Data subjects must also be informed about how to exercise their rights.

9. Droits des personnes

Les personnes concernées par le traitement (personnes exposées à l'événement sanitaire indésirable, personne ayant notifié l'événement sanitaire indésirable et professionnel de santé ayant suivi la personne concernée par l'événement) disposent des droits suivants, qu'elles exercent dans les conditions prévues par le RGPD :

- droit d'accès;

- droit de rectification;

- droit à la limitation du traitement (par exemple, lorsque la personne conteste l'exactitude de ses données, elle peut demander au responsable de traitement le gel temporaire de ses données le temps que celui-ci procède aux vérifications nécessaires).

9. Rights of subjects

The persons concerned by the processing (persons exposed to the adverse health event, person who reported the adverse health event and health care professional who provided care to the person concerned by the event) have the following rights, which they can exercise under the conditions laid down in the GDPR:

- right of access;

- right of rectification ;

- right to restriction of processing (for example, when the accuracy of the data is contested by the data subject, they may ask the controller to temporarily "freeze" their data during the time the controller carries out the necessary checks).

Dans la mesure où le traitement est fondé sur le respect d'une obligation légale, les personnes concernées par la collecte des données ne disposent ni du droit d'opposition, ni du droit à l'effacement des données, ni du droit à la portabilité des données. Les personnes concernées en sont informées préalablement.

Where the processing is based on compliance with a legal obligation, the data subjects do not have the right to object, the right to erase data or the right to data portability. The data subjects must be informed about it in advance.

10. Sécurité

De manière générale, le responsable du traitement doit prendre toutes les précautions utiles au regard des risques présentés par son traitement pour préserver la sécurité des données à caractère personnel et, notamment au moment de leur collecte, durant leur transmission et leur conservation, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

En particulier, dans le contexte spécifique du présent référentiel, soit le responsable de traitement adopte les mesures suivantes, soit il justifie de leur équivalence ou du fait de ne pas avoir besoin ou pouvoir y recourir.

Catégories	Mesures
Former les utilisateurs	Informer et sensibiliser les personnes manipulant les données
	Rédiger une charte informatique et lui donner une force contraignante
Authentifier les utilisateurs	Définir un identifiant (login) unique à chaque utilisateur
	Utiliser un moyen d'authentification forte, appuyé sur un annuaire vérifié
	Adopter une politique de mot de passe utilisateur conforme aux recommandations de la CNIL
	Obliger l'utilisateur à changer son mot de passe après réinitialisation
	Limiter le nombre de tentatives d'accès à un compte
Gérer les habilitations	Définir des profils d'habilitation
	Supprimer les permissions d'accès obsolètes
	Réaliser une revue annuelle des habilitations
Tracer les accès et gérer les incidents	Prévoir un système de journalisation

10. Security

In general, the controller must take all appropriate measures with regard to the risks presented by the processing, to safeguard the security of personal data and, in particular at the time of collection, during their transmission and storage, to prevent them from being distorted, damaged or accessed by unauthorised third parties.

In particular, in the specific context of this standard, the controller must either adopt the following measures, or justify that the measures adopted are equivalent or that it does not need or cannot use them.

Categories	Measures
Training users	Inform and raise awareness among data handlers
	Write an IT policy and give it binding force
Authenticate users	Define a unique identifier for each user
	Use a strong authentication method, based on a verified directory
	Adopt a user password policy in accordance with the recommendations of the CNIL
	Force the user to change their password after reset
	Limit the number of attempts to access an account
Manage authorisations	Set up authorisation profiles
	Remove obsolete access permissions
	Carry out an annual review of authorisations
Log access and manage incidents	Set up a log system
	Inform users that a log system has been

	Informer les utilisateurs de la mise en place du système de journalisation
	Protéger les équipements de journalisation et les informations journalisées
	Prévoir les procédures pour les notifications de violation de données à caractère personnel
Sécuriser les postes de travail	Prévoir une procédure de verrouillage automatique de session
	Utiliser des antivirus régulièrement mis à jour
	Installer un « pare-feu » (firewall) logiciel
	Recueillir l'accord de l'utilisateur avant toute intervention à distance sur son poste
Sécuriser l'informatique mobile	Prévoir des moyens de chiffrement des équipements mobiles
	Faire des sauvegardes ou des synchronisations régulières des données
	Exiger un secret pour le déverrouillage des ordiphones
Protéger le réseau informatique interne	Limiter les flux réseau au strict nécessaire
	Sécuriser les accès distants des appareils informatiques nomades par VPN
	Mettre en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-F
Sécuriser les serveurs	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées
	Installer sans délai les mises à jour critiques
	Assurer une disponibilité des données
Sécuriser les sites web	Utiliser le protocole TLS et vérifier sa mise en œuvre
	Vérifier qu'aucun mot de passe ou identifiant ne passe dans les URL

	implemented
	Protect log equipment and logged information
	Set up procedures to notify personal data breaches
Secure workstations	Set up an automatic session locking procedure
	Use regularly updated antivirus software
	Install a firewall software
	Obtain the user's agreement before any remote intervention on their workstation
Securing mobile equipment	Provide means for encrypting mobile equipment
	Regularly carry out backups or synchronizations of data
	Require a secret answer for unlocking smartphones
Protect the internal network	Limit network flows to what is strictly necessary
	Secure remote access to mobile computing devices via VPN
	Implement WPA2 or WPA2-PSK protocol for Wi-Fi networks
Securing the servers	Limit access to administration tools and interfaces to authorized persons only
	Install critical updates without delay
	Ensure data availability
Securing websites	Use the TLS protocol and check its implementation
	Check that no passwords or IDs are used in URLs

	Contrôler que les entrées des utilisateurs correspondent à ce qui est attendu
	Mettre un bandeau de consentement pour les traceurs (cookies) non nécessaires au service
Sauvegarder et prévoir la continuité d'activité	Effectuer des sauvegardes fréquentes des données, que celles-ci soient sous forme papier ou électronique.
	Stocker les supports de sauvegarde dans un endroit sûr
	Prévoir des moyens de sécurité pour le convoyage des sauvegardes
	Prévoir et tester régulièrement la continuité d'activité
Archiver de manière sécurisée	Mettre en œuvre des modalités d'accès spécifiques aux données archivées
	Détruire les archives obsolètes de manière sécurisée
Encadrer la maintenance et la destruction des données	Enregistrer les interventions de maintenance dans une main courante
	Encadrer par un responsable de l'organisme les interventions par des tiers
	Effacer les données de tout matériel avant sa mise au rebut
Gérer la sous-traitance	Prévoir une clause spécifique dans les contrats des sous-traitants
	Prévoir les conditions de restitution et de destruction des données
	S'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)
	Prévoir une clause spécifique dans les contrats des sous-traitants
Sécuriser les échanges avec d'autres organismes	Envoyer les données de façon chiffrée (soit en chiffrant directement les données ou en utilisant un tunnel chiffré)

	Check that what the user inputs corresponds to what is expected
	Provide a consent banner for trackers (cookies) not required for the service
Backup and forecast business continuity	Perform frequent backups of data, whether in paper or electronic form.
	Store backup media in a safe place
	Provide security processes for the transport of backups
	Plan and test business continuity on a regular basis
Secure archiving	Implement specific access procedures for archived data
	Securely destroy obsolete archives
Supervise the maintenance and destruction of data	Record maintenance interventions in a log
	A person from the organisation should supervise third party interventions
	Delete data from any material before it is discarded
Managing processors	Provide a specific clause for data processing agreements
	Set out the conditions for the return and destruction of data
	Ensure the effectiveness of the provided guarantees (security audits, visits, etc.)
	Provide for a specific clause in contracts with processors
Secure exchanges with other organizations	Send the data in encrypted form (either by directly encrypting the data or by using an encrypted transfer protocol)

	S'assurer qu'il s'agit du bon destinataire
	Transmettre le secret lors d'un envoi distinct et via un canal différent
Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées que ce soit aux fichiers papiers ou aux matériels informatiques, notamment aux serveurs.
	Installer des alarmes anti-intrusion et les vérifier périodiquement
Encadrer les développements informatiques	Proposer des paramètres respectueux de la vie privée aux utilisateurs finaux
	Éviter les zones de commentaires ou les encadrer strictement
	Tester sur des données fictives ou anonymisées
Utiliser des fonctions cryptographiques	Utiliser des algorithmes, des logiciels et des bibliothèques reconnues
	Conserver les secrets et les clés cryptographiques de manière sécurisée

Pour ce faire, le responsable de traitement pourra utilement se référer au Guide de la sécurité des données personnelles publié par la CNIL.

Toute violation de données devra être notifiée à la CNIL dans les conditions prévues à l'article 33 du RGPD.

Il est demandé, qu'en cas de recours à un prestataire extérieur pour le stockage et la conservation des données de santé à caractère personnel par le responsable de traitement, ce prestataire soit un hébergeur de données de santé agréé ou certifié.

Par exception, lorsque le responsable de traitement n'est pas établi en France, le responsable de traitement doit démontrer que le prestataire auquel il recourt présente des garanties de sécurité équivalentes.

Le recours aux services d'un sous-traitant devra s'effectuer dans les conditions prévues à l'article 28 du RGPD.

	Ensure that it is the right recipient
	Transmit the key separately and using a different channel of communication
Protect the premises	Restrict access to premises with locked doors regardless of whether the premises contain paper files or computer equipment, in particular to servers.
	Install intruder alarms and check them periodically
Supervise IT developments	Provide privacy-friendly settings to end users
	Avoid free text/comment areas or frame them strictly
	Test on fictitious or anonymized data
Use encryption functions	Use renowned algorithms, software and libraries
	Keep passwords and encryption keys securely

To do this, the controller may refer to the Guide on personal data security published by the CNIL.

Any personal data breach must be notified to the CNIL under the conditions provided for in Article 33 of the GDPR.

It is requested that, if the controller relies on an external service provider for the storage and retention of personal health data, this service provider be an approved or certified health data hosting provider.

By way of exception, where the controller is not established in France, the controller must demonstrate that the service provider he is using offers equivalent security guarantees.

Using a processor must be done under the conditions provided for in Article 28 of the GDPR.

11. Transfert de données hors de l'Union européenne

Les données indirectement identifiantes des personnes exposées à un événement sanitaire indésirable et les données directement identifiantes des personnes ayant notifié l'événement sanitaire indésirable peuvent faire l'objet d'un transfert hors de l'Union européenne si les conditions suivantes sont réunies :

- les dispositions de l'article 6 relatives aux destinataires des données sont respectées ;

- le transfert de données est strictement nécessaire à la mise en œuvre du dispositif de vigilance.

Le transfert peut être effectué dans le cadre de la déclaration de conformité au présent référentiel lorsque l'une des conditions suivantes est remplie :

- le transfert s'effectue à destination d'un pays ou d'une organisation internationale reconnu par la Commission européenne comme assurant un niveau de protection adéquat, conformément à l'article 45 du RGPD (décision d'adéquation) ;

- le transfert s'effectue moyennant des garanties appropriées, listées à l'article 46, paragraphe 2, du RGPD (notamment : clauses contractuelles types approuvées par la Commission européenne, règles d'entreprise contraignantes, code de conduite, mécanisme de certification) ;

- en l'absence d'une décision d'adéquation ou de garanties appropriées, le transfert peut être fondé sur l'une des exceptions prévues par l'article 49 du RGPD lorsqu'un tel transfert n'est pas répétitif, massif ou structuré.

Le responsable de traitement doit avoir préalablement informé les personnes concernées du transfert de leurs données à caractère personnel vers des pays tiers à l'Union européenne, de l'existence ou de l'absence d'une décision d'adéquation ou de garantie appropriée et des moyens d'en obtenir une copie conformément à l'article 13, paragraphe 1, point f, du RGPD.

11. Data transfer outside the European Union

Indirectly identifying data of persons affected by an adverse health event and directly identifying data of persons who have reported the adverse health event may be transferred outside the European Union if the following conditions are met:

- the provisions of Article 6 relating to the recipients of the data are respected;

- the transfer of data is strictly necessary for the implementation of the vigilance system.

The transfer may be made as part of the declaration of conformity to this standard when one of the following conditions is met:

- the transfer is made to a country or international organisation recognised by the European Commission as providing an adequate level of protection, in accordance with Article 45 of the GDPR (adequacy decision);

- the transfer is carried out with appropriate safeguards, listed in Article 46(2) of the GDPR (in particular: standard contractual clauses approved by the European Commission, binding corporate rules, code of conduct, certification mechanism);

- in the absence of a decision on adequacy or appropriate safeguards, the transfer may be based on one of the exceptions provided for in Article 49 of the GDPR where such a transfer is not repetitive, large scale or structured.

The controller must have previously informed the data subjects of the transfer of their personal data to third countries outside of the European Union, of the existence or absence of an adequacy decision or appropriate safeguards and of the means of obtaining a copy thereof in accordance with Article 13(1)(f) of the GDPR.

12. Analyse d'impact sur la protection des données (AIPD)

Conformément à l'article 35 du RGPD, le responsable de traitement doit réaliser une analyse d'impact sur la protection des données.

Pour réaliser son analyse d'impact, le responsable de traitement pourra se reporter :

- aux principes contenus dans ce référentiel ;

- aux outils méthodologiques proposés par la CNIL sur son site web.

12. Data Protection Impact Assessment (DPIA)

In accordance with Article 35 of the GDPR, the controller must carry out a data protection impact assessment.

To carry out the impact assessment, the controller may refer to:

- the principles contained in this standard;

- the methodological tools proposed by the CNIL on its website.

Le cas échéant, le délégué à la protection des données (DPO) devra être consulté. Conformément à l'article 36 du RGPD, le responsable de traitement doit consulter la CNIL préalablement à la mise en œuvre du traitement si, à l'issue de l'analyse d'impact, il ne parvient pas à identifier des mesures suffisantes pour réduire les risques à un niveau acceptable (risque résiduel restant trop élevé).	Where applicable, the Data Protection Officer (DPO) shall be consulted. In accordance with Article 36 of the GDPR, the controller must consult the CNIL before carrying out the processing if, following the impact assessment, he is unable to identify sufficient measures to reduce the risks to an acceptable level (i.e. if the residual risk remains too high).

Get in touch

Ariane Mole
Partner

Tel: +33142686304
ariane.mole@twobirds.com

Dora Talvard
Associate

Tel: +33142686398
dora.talvard@twobirds.com

twobirds.com

Abu Dhabi & Amsterdam & Beijing & Berlin & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & San Francisco & Shanghai & Singapore & Stockholm & Sydney & Warsaw

The information given in this document concerning technical legal or professional subject matter is for guidance only and does not constitute legal or professional advice. Always consult a suitably qualified lawyer on any specific legal problem or matter. Bird & Bird assumes no responsibility for such information contained in this document and disclaims all liability in respect of such information.

This document is confidential. Bird & Bird is, unless otherwise stated, the owner of copyright of this document and its contents. No part of this document may be published, distributed, extracted, re-utilised, or reproduced in any material form.

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority. Its registered office and principal place of business is at 12 New Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.