****

<https://www.porttic.be>

Mesure de sécurité relatives à la protection des données personnelles

Avec le soutien de la Wallonie



**AVERTISSEMENT**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*Le présent modèle de document et clauses-types est rédigé en tant qu’exemple par CAIPS dans le but d’aider à la mise en œuvre du Règlement Général sur la Protection des Données (Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016, ci-après « RGPD »).*

*Les documents et clauses-types dépendent de chaque situation spécifique ; les organismes qui voudraient les utiliser devront se les réapproprier. Les contenus devront donc être modifiés, complétés ou supprimés suivant la situation particulière du centre. Il est également possible d’ajouter toute disposition qui serait jugée utile ou adéquate.*

*En cas de situation complexe (par exemple en cas de transfert de données hors Union européenne), nous recommandons un accompagnement juridique plus poussé. CAIPS ne peut être tenue pour responsable en cas de recours ou de dommage découlant de l’utilisation de ces contenus.*

*CAIPS ne peut garantir l’exhaustivité ou l’exactitude des informations reprises dans ce document.*

Table des matières

[mesures de sécurité relatives à la protection des données à caractère personnel 3](#_Toc34919429)

[1. Dispositions générales en matière de protection des données à caractère personnel 3](#_Toc34919430)

[1.1. Préambule 3](#_Toc34919431)

[1.2. Champ d’application 3](#_Toc34919432)

[1.3. L’analyse des risques 3](#_Toc34919433)

[1.4. Le « traitement » de « données à caractère personnel » 4](#_Toc34919434)

[1.5. L’accès aux informations confidentielles 4](#_Toc34919435)

[1.6. Les consignes générales de sécurité 4](#_Toc34919436)

[1.7. Les objectifs poursuivis par l’Organisme 6](#_Toc34919437)

[1.8. Les coordonnées de contact 7](#_Toc34919438)

[1.9. Modification 7](#_Toc34919439)

[2. Mesures techniques et organisationnelles 7](#_Toc34919440)

[2.1. Identifiants et mots de passe 8](#_Toc34919441)

[2.2. Sécurisation des locaux 8](#_Toc34919442)

[2.3. Utilisation du matériel informatique 9](#_Toc34919443)

[2.4. Transport d’informations confidentielles en dehors des locaux de l’Organisme 11](#_Toc34919444)

[2.5. Protection des dossiers travailleurs 11](#_Toc34919445)

[2.6. Utilisation de la messagerie électronique 11](#_Toc34919446)

[2.7. Utilisation des téléphones 12](#_Toc34919447)

[2.8. Sécurité informatique 12](#_Toc34919448)

[2.9. Archivage sécurisé 18](#_Toc34919449)

[2.10. Encadrement de la maintenance et de la destruction des données 18](#_Toc34919450)

[2.11. Gestion de la sous-traitance 20](#_Toc34919451)

# mesures de sécurité relatives à la protection des données à caractère personnel

**Nom de l’Organisme, ci-après dénommée « l’Organisme »**

*Dernière mise à jour : …*

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## Dispositions générales en matière de protection des données à caractère personnel

### Préambule

L’Organisme accorde une grande importance à la protection adéquate des données à caractère personnel qu’elle traite.

Par le biais de sa Politique de confidentialité, point de départ dont relèvent toutes autres directives, règles ou procédures mises en œuvre en la matière, l’Organisme énonce les principes généraux qu’elle s’est fixée et que doivent respecter ses collaborateurs internes et externes en matière de protection des données à caractère personnel.

Nous vous recommandons de la lire attentivement et de la consulter régulièrement : retrouvez notre Politique de confidentialité sur www…..

L’Organisme y indique que les données à caractère personnel sont traitées de façon strictement confidentielle et que, afin d’empêcher dans la mesure du possible tout accès non autorisé aux données personnelles collectées, l’Organisme a pris des dispositions en matière de sécurité et d’organisation. Celles-ci sont explicitées dans le présent document.

### Champ d’application

Les présentes dispositions générales s’appliquent durant toute la durée de vie des données à caractère personnel au sein de l’Organisme, depuis leur obtention jusqu’à leur suppression définitive.

Elles s’appliquent à toute l’Organisme :

* Tous les collaborateurs internes et externes susceptibles de prendre connaissance de données à caractère personnel dans le cadre de l’exécution de leur travail (travailleurs, apprentis, stagiaires, étudiants, bénévoles, membres de l’assemblée générale, administrateurs, prestataire de services, etc.) ;
* Tous les locaux de l’Organisme ;
* Tous les moyens de l’Organisme et les systèmes de traitement des informations gérés par l’Organisme, de même que, le cas échéant, les systèmes gérés par des parties externes en vue du traitement des informations pour l’Organisme, tels que les bases de données, les informations sur tout support, les réseaux, les centres de données, etc. ;
* Toutes les activités de traitement des données à caractère personnel (voir définitions ci-dessous).

Ces dispositions générales concernent la protection des données confidentielles et participent à garantir le respect des droits des personnes concernées en matière de traitement de leurs données à caractère personnel.

### L’analyse des risques

L’Organisme a veillé à élaborer une analyse des risques, pour chaque catégorie de données à caractère personnel traitée, sur base des éléments suivants :

* L’identification des impacts potentiels sur les droits et libertés des personnes concernées si l’un des événements suivants survient :
  + L’accès illégitime aux données personnelles ;
  + La modification non désirée de données personnelles ;
  + La disparition de données personnelles ;
* L’identification des sources de risques (qui ou quoi pourrait être à l’origine de chaque événement redouté) ;
* L’identification des menaces réalisables (qu’est-ce qui pourrait permettre que chaque événement redouté survienne) ;
* La détermination des mesures existantes ou prévues qui permettent de traiter ces risques ;
* La gravité et la vraisemblance de ces risques.

### Le « traitement » de « données à caractère personnel »

Sont concernées par le présent document toutes les « données à caractère personnel » qui sont mises à disposition de l’Organisme, telles que définies par le Règlement UE 2016/679[[1]](#footnote-1) du Parlement européen et du Conseil du 27 avril 2016, ci-après « RGPD », à savoir : « *toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu’un nom, un numéro d’identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale*».

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

Les catégories de données à caractère personnel traitées par l’Organisme sont reprises dans la Politique de confidentialité.

Chaque activité de traitement de données à caractère personnel est déclinée au Registre des activités de traitement.

### L’accès aux informations confidentielles

Les collaborateurs (internes et externes) de l’Organisme sont susceptibles de prendre connaissance de données à caractère personnel dans l’exercice de leur fonction/mission. Ces informations doivent être considérées, à tout moment, comme confidentielles. Seules les personnes habilitées y ont accès et elles ne pourront être partagées, après vérification, qu’avec des personnes habilitées à prendre connaissance des informations en question.

### Les consignes générales de sécurité

**Tout collaborateur de l’Organisme (interne ou externe)** qui traite des données à caractère personnel dans le cadre de l’exécution de son travail/sa mission, le fait conformément à la Politique de confidentialité de l’Organisme ainsi qu’aux principes et directives suivants :

* Il respecte et, le cas échéant, s’engage à faire respecter par les autres collaborateurs, la Politique de confidentialité de l’Organisme et les présentes dispositions générales ;
* Il ne traite les données à caractère personnel que dans les mesures nécessaires aux finalités pour lesquelles elles ont été obtenues ;
* Il n’utilise jamais les informations confidentielles au détriment de l’Organisme ou à toute autre fin que celle de leur mission ;
* Il respecte les droits des personnes concernant leurs données à caractère personnel ;
* Il ne partage pas les informations confidentielles, volontairement ou involontairement, avec des personnes non autorisées, en ce compris des tiers ;
* Il ne vend en aucun cas à des tiers des données à caractère personnel à sa disposition, pour quelque raison que ce soit ;
* Il ne transfère jamais ces données vers un pays tiers de l’Union européenne ni vers une organisation internationale. Si cela devait s’avérer nécessaire, le responsable du traitement mettra en œuvre les mesures adéquates et nécessaires conformément aux prescriptions en la matière énoncées au Chapitre V du RGPD ;
* Il ne procède jamais à un traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi qu’à un 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. Si cela devait s’avérer nécessaire, le responsable du traitement mettra en œuvre les mesures adéquates et nécessaires en regard des conditions reprises à l’article 9, §2 du RGPD ;
* Il ne procède jamais au traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes. Si cela devait s’avérer nécessaire, l’Organisme mettra en œuvre les mesures adéquates et nécessaires afin que le traitement envisagé se réalise sous le contrôle de l'autorité publique, ou soit autorisé par le droit de l'Union ou par le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées.
* Il n’accède pas aux informations auxquelles il doit raisonnablement savoir ne pas avoir le droit d’accéder, ni ne tente d’accéder, supprimer ou modifier des informations qui ne lui appartiennent pas ;
* Il traite les données avec soin ;
* Il ne masque pas sa véritable identité et n’usurpe jamais l’identité d’autrui ;
* Il applique, dans le cadre de sa mission de traitement, les directives complémentaires en matière de sécurité qui lui sont transmises par l’employeur ;
* Il signale sans délai les infractions dont il a connaissance ;
* Il signale sans délai tout problème de sécurité qu’il constate, violation ou tentative de violation suspectée de son compte réseau et, de manière générale, tout dysfonctionnement ;
* Il coopère et participe positivement à la Politique de confidentialité mise en œuvre par l’Organisme dans le cadre de la protection des données à caractère personnel ;
* Il respecte les principes et règles de déontologie professionnelle ainsi que le secret professionnel qui, le échéant, s’impose à lui.

Ces mesures générales sont complétées par des mesures spécifiques d’ordre technique et organisationnel. Celles-ci sont décrites au point 2 du présent document (« *2. Mesures techniques et organisationnelles* »).

A ces responsabilités qui incombent à tout collaborateur qui traite des données à caractère personnel s’ajoutent, **pour le collaborateur TIC** (Technologies de l’Information et de la Communication – soit la personne responsable de la sécurité informatique), les responsabilités suivantes :

* Il met en œuvre des mesures techniques appropriées afin de protéger les données confidentielles ;
* Il applique des paramètres de sécurité conformément à Politique de confidentialité de l’Organisme et au présent document ;
* Il signale tout problème de sécurité qui survient avant, durant ou après la mise en place de moyens TIC ;
* Il signale les risques en matière de sécurité des applications fournies ;
* Il exécute les tâches de sécurité qui lui incombent ;
* Il endosse un rôle d’expert, dans le cadre duquel il participe à l’identification et à la détermination de mesures de prévention des risques en matière de traitement des données à caractère personnel.

### Les objectifs poursuivis par l’Organisme

L’Organisme, dans son rôle de responsable du traitement de données à caractère personnel, poursuit les objectifs suivants :

* Elle est transparente au sujet des données à caractère personnel qu’elle traite et de la finalité du traitement, tant envers la personne concernée que les autorités de surveillance. La communication menée est honnête, facilement accessible et compréhensible. Le principe de transparence s’applique également lorsque les données à caractère personnel sont échangées.
* Elle traite uniquement les données pertinentes pour l’exécution de ses tâches. Chaque tâche dans le cadre de laquelle des données à caractère personnel sont traitées est licite. Cela signifie notamment que le traitement est réalisé conformément aux finalités légales et statutaires de l’Organisme. Ce point est chaque fois évalué pour toute nouvelle finalité de traitement, le cas échéant, au moyen d’une analyse d’impact relative à la protection des données.
* Elle traite uniquement les données à caractère personnel strictement nécessaires pour l’exécution de ses activités.
* Elle vérifie l’intégrité des données à caractère personnel tout au long du cycle de vie du traitement.
* Elle ne conserve pas les données plus longtemps que nécessaire. La nécessité est vérifiée par rapport aux obligations légales, ainsi qu’aux droits et libertés de la personne concernée.
* Elle évite les violations découlant du traitement des données à caractère personnel. La sécurité des informations, la protection des données dès la conception et les paramètres standard respectueux de la vie privée constituent des outils dans ce cadre. Lorsqu’une violation se produit, celle-ci est rapportée conformément à la réglementation en la matière.
* Elle est capable d’exécuter tous les droits d’une personne concernée. Dans ce cadre, l’Organisme veille aux éventuelles restrictions applicables à ces droits.
* Elle surveille activement que les droits et libertés de la personne concernée soient préservés dans le cadre du traitement des données à caractère personnel pour une finalité bien définie.
* Elle traite les données conformément aux droits et libertés applicables au sein de l’Union européenne et contrôle leur application si des données devaient être échangées en dehors l’Europe. Par conséquent, l’Organisme respecte tous les cadres légaux et normatifs (c’est-à-dire aussi bien les réglementations wallonnes que fédérales et européennes) dans le cadre du traitement des données à caractère personnel et a, pour ce faire, clairement répertorié ses responsabilités et celles des autres à l’égard des données à caractère personnel.
* Elle peut prouver son respect de tous les objectifs du présent document, conformément aux dispositions légales. Ce devoir de responsabilité est suivi en interne, et est exécutable conformément aux principes légaux.

### Les coordonnées de contact

Toute question, remarque, suggestion, ainsi que toute réclamation concernant le traitement de ses propres données à caractère personnel peut être déposée auprès de l’Organisme selon les modalités prévues et aux coordonnées de contact figurant dans la Politique de confidentialité (www……).

### Modification

Les présentes dispositions générales en matière de protection des données à caractère personnel peuvent être adaptées et complétées lorsque des circonstances l’exigent.

Les modifications sont portées à la connaissance des collaborateurs concernés par toute voie de communication interne et externe.

## Mesures techniques et organisationnelles

L’Organisme développe des mesures de sécurité techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques que présente le traitement des données privées. Ces risques résultent notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

Au-delà des dispositions générales en matière de sécurité énoncées au point précédent du présent document (« *1. Dispositions générales en matière de protection des données à caractère personnel*»), l’Organisme élabore des dispositions complémentaires pour certains aspects spécifiques au sein de l’Organisme. Celles-ci décrivent plus en détails quelles mesures sont prises pour atteindre le niveau de sécurité approprié.

### Identifiants et mots de passe

Lors de l’entrée en fonction d’un nouveau travailleur, l’Organisme lui fournit un identifiant et un mot de passe adapté à l’ordinateur mis à disposition. Ceux-ci ne peuvent être modifiés que moyennant accord préalable de la direction et dans le respect des consignes qui lui sont données.

La direction doit à tout moment disposer des identifiants et mots de passe de tous les membres du personnel.

Chaque membre du personnel est personnellement responsable de la bonne utilisation de ses identifiants et mots de passe. Ceci implique que le mot de passe :

* est strictement personnel : il ne doit être confié à personne ;
* est unique : il ne doit pas être utilisé deux fois, chaque compte devant faire l’objet d’un mot de passe différent.
* ne doit être inscrit nulle part (ni sur le sous-main, ni sur un post-it, ni dans un fichier électronique) ;
* ne doit jamais être préenregistré : sur internet, l’option permettant d’enregistrer l’identifiant et le mot de passe ne doit jamais être cochée.

*Comment faire ?*

Sur Internet Explorer, aller dans « Paramètres » - « Paramètres avancés » - « Paramètre de saisie automatique : enregistrer les mots de passe », cliquer sur désactiver.

* doit être modifié régulièrement, selon une périodicité pertinente et raisonnable. En effet, un pirate discret pourrait se contenter d’observer les informations sans laisser de traces.

Il est également conseillé, dans la mesure du possible, de limiter le nombre de tentatives d’accès aux comptes utilisateurs et bloquer temporairement le compte lorsque la limite est atteinte.

Chaque mot de passe doit être constitué en respectant les règles suivantes :

* Mots de passe à éviter : des mots faciles à trouver tels que le nom ou prénom, numéro de téléphone, date de naissance, surnom, nom du compagnon ou de l’animal domestique, film préféré, etc. Un bon mot de passe ne figure pas non plus dans le dictionnaire, un recueil, un fichier ou un listing informatique, etc.
* Mots de passe à privilégier :

Un bon mot de passe doit contenir au moins 8 caractères dont au moins un chiffre, une majuscule et un caractère spécial (ex : @, -, /, +, &, #, etc.).

### Sécurisation des locaux

*Rangement des bureaux*

Chaque membre du personnel est tenu de respecter les directives suivantes :

* Il verrouille son ordinateur lorsqu’il s’absente de son bureau ;

*Comment faire ?*

Pour verrouiller son ordinateur = Ctrl + alt + delete

* Il éteint son ordinateur à la fin de la journée de travail ;
* Il ferme la porte de son bureau lorsqu’il s’absente et lorsqu’il quitte son bureau en fin de journée ;
* Il retire immédiatement de l’imprimante les impressions qui contiennent des données à caractère personnel ;
* Il s’assure que les clés des casiers et armoires ne sont jamais laissées sans surveillance.

Il applique les directives suivantes lorsqu’il quitte son bureau ou son lieu de travail en fin de journée ou pour une absence d’une demi-journée au moins :

* Il retire de son bureau ou son lieu de travail toutes les informations confidentielles et les stocke ou les archive dans une armoire fermée ou un casier. Il en va de même des informations confidentielles sauvegardées sur une clé USB, un disque dur externe ou tout autre support ;
* Il jette dans des corbeilles spécialement prévues à cet effet ou passe par la déchiqueteuse tous les documents qui contiennent des informations confidentielles et qui sont destinés à être jetés.

En cas d’absence prolongée :

* Il autorise l’Organisme, en cas d’absence de plus de 15 jours et/ou d’extrême urgence, à accéder à l’ordinateur et à la messagerie électronique mis à sa disposition si cela s’avère nécessaire pour assurer la continuité du service. Le cas échéant, l’Organisme accède uniquement aux documents et/ou à la boîte de réception dans la mesure nécessaire à la continuité du service, sur le fondement de son intérêt légitime. Tout document ou message comportant la mention expresse ou manifeste de son caractère personnel bénéficiera du droit au respect de la vie privée et du secret des correspondances.

*Protection des locaux*

En vue de sécuriser les données à caractère personnel disponibles dans les locaux de l’Organisme, il est impératif de respecter les directives suivantes :

* Contrôler l’accès des visiteurs : chaque visiteur pénétrant dans les locaux sera accompagné par une personne appartenant à l’Organisme et sera invité à signer une liste d’inscription mentionnant son nom ainsi que son heure d’arrivée et de départ ;
* Distinguer les zones des bâtiments selon les risques et tenir à jour une liste des personnes ou catégories de personnes autorisées à pénétrer dans chaque zone. Seul le personnel dûment habilité est habilité à accéder aux zones à accès restreint ;
* Limiter l’accès à la pièce réservée au serveur informatique et aux back up qu’aux personnes habilitées, avec traçabilité de leurs passages et interventions ;
* Installation d’alarmes anti-intrusion à vérifier périodiquement ;
* Mise en place de détecteurs de fumée ainsi que des moyens de lutte contre les incendies ;
* Protéger les clés permettant l’accès aux locaux et les codes d’alarmes ;
* Le matériel informatique dispose de moyens de protection spécifiques (exemples : système anti-incendie spécifique, surélévation du matériel pour le protéger contre d’éventuelles inondations, redondance d’alimentation électrique et/ou de climatisation,…).

### Utilisation du matériel informatique

Les moyens informatiques et de télécommunication mis à disposition par l’employeur sont les suivants : ordinateur (portable), clé USB, messagerie électronique, ….

*Utilisation du matériel informatique mis à disposition par l’employeur*

Concernant l’utilisation de ce matériel, les membres du personnel doivent respecter les directives suivantes :

* Ne pas conserver des documents ou des données sur le disque dur interne de l’ordinateur mais les enregistrer uniquement sur le serveur qui est régulièrement mis à jour afin de remédier aux risques pour la sécurité. Un back-up du serveur est régulièrement effectué afin de prévenir toute perte de données ;
* Ne pas installer, copier, modifier ou détruire des logiciels sans autorisation ;
* Ne pas modifier les outils informatiques et leur fonctionnement, leur paramétrage ainsi que leur configuration physique ou logicielle sans accord préalable ;
* Ne pas nuire, volontairement ou non, au fonctionnement des outils informatiques et de communication ;
* Ne pas prêter les outils informatiques à une tierce personne ;
* Signaler sans délai à la direction tout problème de sécurité, dysfonctionnement ou suspicion de (tentative de) violation du compte informatique qu’ils constatent.

*Utilisation du matériel professionnel à des fins privés*

Concernant l’utilisation du matériel à des fins personnelles, les membres du personnel doivent respecter les directives suivantes :

* Le matériel mis à disposition par l’employeur est destiné à un usage professionnel. Toute utilisation de celui-ci à des fins privées doit être limitée aux cas strictement nécessaires ;
* Eviter la conservation des documents privés ou des données privées sur ce matériel.

L’utilisation de la messagerie à des fins personnelle est, quant à elle, tolérée pour autant qu’elle n’affecte pas le travail du membre du personnel concerné ni la sécurité du réseau informatique.

Tout message comportant la mention expresse ou manifeste de son caractère personnel bénéficiera du droit au respect de la vie privée et du secret des correspondances. A défaut, le message est présumé professionnel.

De la même façon, l’Organisme s’interdit d’accéder à tout document ou fichier portant une mention claire de son caractère privé.

*Utilisation de matériels privés à des fins professionnels*

En principe, seul le matériel informatique mis à disposition par l’employeur peut être utilisé à des fins professionnelles.

L’utilisation de matériels privés à des fins professionnelles doit être limitée au strict nécessaire et pour autant qu’une sécurité adaptée du matériel soit garantie.

Dans ce cas, le stockage de données sur les appareils privés doit être limité au strict nécessaire et à la durée de conservation nécessaire.

Par exemple, lorsque le travailleur consulte sa messagerie à distance, les fichiers qui seraient copiés sur l’ordinateur utilisé par le travailleur dans ce cadre doivent être effacés dès que possible de l’ordinateur utilisé.

Toute suspicion de (tentative de) violation du compte informatique et tout problème de sécurité doivent être immédiatement signalés à la direction et au délégué à la protection des données.

### Transport d’informations confidentielles en dehors des locaux de l’Organisme

Exemples : sortie d’une clé USB, d’un ordinateur portable, de documents papiers contenant des données à caractère personnel, etc.

Chaque membre du personnel limite au maximum le transport d’informations confidentielles hors des locaux de l’Organisme et exclusivement à ce qui est strictement nécessaire pour l’exécution de son travail.

Conscient en permanence du risque de perte de données dans ce genre de situation, il respecte les directives suivantes :

* Il ne laisse jamais son matériel et des documents contenant des données à caractère personnel sans surveillance en dehors des locaux de l’Organisme ;
* Il fait tout ce qui est en son pouvoir pour prévenir le vol ou la perte de données (ex : oubli d’une clé USB dans les transports en commun, vol d’un ordinateur resté dans son véhicule, etc.) ;
* En cas de vol ou de perte, il informe sans délai la direction et le délégué à la protection des données ;
* En cas de (doute de) piratage sur son matériel, il informe sans délai la direction et le délégué à la protection des données ;
* Il s’assure, s’il utilise un autre réseau de connexion que celui de l’Organisme, qu’il s’agit d’un réseau sécurisé. Si le réseau WIFI ouvert n’est pas sécurisé, il lui est interdit de l’utiliser.

### Protection des dossiers travailleurs

En parallèle des mesures de protection générales développées par ailleurs, les données à caractère personnel des membres du personnel ne sont conservées qu’en version papier, sous clé et sous le contrôle de la personne habilitée à y accéder.

Lorsqu’il est question de traiter des données relatives à la santé d’un travailleur, son consentement écrit est requis sauf si celles-ci sont traitées sous la responsabilité d’un professionnel de la santé soumis au secret professionnel.

### Utilisation de la messagerie électronique

L’utilisation de la messagerie électronique doit se conformer aux règles d’usage définies par la personne responsable de la sécurité informatique et validées par la direction de l’Organisme :

* Volumétrie de la messagerie,
* Taille maximale de l’envoi et de la réception d’un message,
* Nombre limité de destinataires simultanés lors de l’envoi d’un message,
* Gestion de l’archivage et des sauvegardes de messagerie,
* Etc.

Lors d’envoi d’emails groupés, les adresses des différents destinataires doivent être mises en « copie cachée ».

*Comment faire ?*

Le champ « CCI » doit être utilisé.

L’Organisme dispose d’un outil permettant de lutter contre la propagation de messages non désirés (spam). Aussi, afin de ne pas accentuer davantage l’encombrement du réseau lié à ce phénomène, le travailleur est invité à limiter son consentement exprès préalable à recevoir un message de type commercial, newsletter, abonnements ou autres, et de ne s’abonner qu’à un nombre limité de listes de diffusion, notamment si elles ne relèvent pas du cadre strictement professionnel.

Le transfert de messages à caractère professionnel, ainsi que leurs pièces jointes, sur des messageries personnelles est soumis aux mêmes règles que les copies de données sur support externe : il est interdit de communiquer des informations confidentielles sans accord préalable.

### Utilisation des téléphones

L’Organisme met à disposition des membres du personnel, pour l’exercice de leur activité professionnelle, des téléphones fixes.

L’utilisation du téléphone à titre privé est interdite.

Dans le cadre de l’utilisation à titre strictement professionnel, et conformément aux instructions établies par l’ONSS, l’employeur se réserve le droit de vérifier, par le biais des factures de l’opérateur de téléphonie, que le caractère strictement professionnel des appels est respecté.

### Sécurité informatique

*Sécurisation des ordinateurs*

Il s’agit de prévenir les accès frauduleux, l’exécution de virus ou la prise de contrôle à distance (notamment via internet). En effet, les risques d’intrusion dans les systèmes informatiques sont importants et les postes de travail constituent un des principaux points d’entrée.

1. *Système antivirus, antispam, pare-feu et autre protection contre l’extérieur*

*Précautions :*

* Prévoir un mécanisme de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné ;
* Installer un « pare-feu » et limiter l’ouverture des ports de communication à ceux strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail ;
* Utiliser des antivirus régulièrement mis à jour ;
* Prévoir une politique de mise à jour régulière des logiciels ou configurer les logiciels pour que les mises à jour se fassent automatiquement dès que cela est possible ;
* Effectuer une veille de sécurité sur les logiciels et matériels utilisés dans le système d’information de la structure ;
* Favoriser le stockage des données des utilisateurs sur un espace de stockage régulièrement sauvegardé accessible via le réseau de la structure plutôt que sur les postes de travail ;
* Limiter la connexion de supports mobiles (clé USB, disques durs externes, etc.) à l’indispensable ;
* Interdire l’exécution d’application téléchargées ne provenant pas de sources sûres ;
* Effacer les données présentes sur un poste préalablement à sa réaffectation à une autre personne ;
* Diffuser aux membres du personnel la conduite à tenir et la liste des personnes à contacter en cas d’incidents de sécurité ou de survenance d’un évènement inhabituel.

*A éviter :*

* Utiliser des systèmes d’exploitation obsolètes ;
* Donner des droits administrateurs aux personnes n’ayant pas de compétence en sécurité informatique.
* *Option pour les Organismes fonctionnant avec un sous-traitant*

L’Organisme a recours aux compétences techniques et informatiques d’un sous-traitant.

Celui-ci veille à protéger le système informatique de l’Organisme des intrusions externes en veillant à ce que le système réseau et/ou les ordinateurs bénéficient d’une protection optimale et mise à jour, en recourant aux systèmes les plus fiables se trouvant sur le marché.

* *Option pour les Organismes ne fonctionnant pas avec un sous-traitant*

L’Organisme se dote des protections les plus fiables présentes sur le marché. Elle veille à mettre à jour régulièrement ces systèmes de protection en se documentant périodiquement quant aux nouveautés en la matière.

1. *Back up*

* *Option pour les Organismes fonctionnant en réseau*

Un back up de toutes les données se trouvant sur le réseau est régulièrement.

La personne chargée de la sécurité informatique vérifie régulièrement que les back up sont effectués correctement et que le contenu est lisible.

Le back up est sauvegardé à l’extérieur de l’Organisme OU un second back up est sauvegardé, via un sous-traitant, dans un cloud à l’extérieur de l’Organisme.

* *Option pour les Organismes ne fonctionnant pas en réseau*

Un back up est réalisé quotidiennement par le responsable de la sécurité informatique ou une personne déléguée pour chaque ordinateur, fixe ou portable, de l’Organisme.

Chaque travailleur veillera à se conformer aux instructions données par la personne responsable de la sécurité informatique pour que ce back up se réalise à temps et à heure.

Ce back up est sauvegardé en un endroit extérieur à l’Organisme.

1. *Autres mesures*

La connexion de supports mobiles (clé USB, disque dur externe,…) n’est autorisée qu’avec l’accord préalable du responsable de la sécurité informatique. Il en va de même pour l’exécution d’applications téléchargées.

L’Organisme veille à effacer, de façon sécurisée, les données présentes sur un poste de travail préalablement à sa réaffectation à une autre personne.

*Sécurisation du réseau informatique interne*

Il s’agit d’autoriser uniquement les fonctions réseau nécessaires aux traitements mis en place.

*Précautions :*

* Limiter les accès internet en bloquant les services non nécessaires ;
* Gérer les réseaux wifi : le réseau ouvert aux invités doit être séparé du réseau interne.
* Imposer un VPN pour l’accès à distance ;
* Limiter les flux réseau au strict nécessaire en filtrant les flux entrants/sortants sur les équipements (pare-feu, proxy, serveurs, etc.).

*Sécurisation des serveurs*

La sécurité des serveurs doit être une priorité car ils centralisent un grand nombre de données.

Les opérations d’administration des serveurs s’effectuent via un réseau dédié et isolé, accessible après une authentification forte et avec une traçabilité renforcée.

L’Organisme dispose de serveurs dits miroirs et réalisent également des back up journaliers conservés, soit dans un endroit ignifuge et étanche, soit dans un lieu externe au siège sociale de l’Organisme. Le service informatique effectue un suivi régulier de ces back up.

Ces serveurs se trouvent dans un endroit sécurisé.

*Précautions :*

* La sécurisation des serveurs est réservée aux seules personnes habilitées qui disposent d’un accès administrateur ;
* Adopter une politique spécifique de mots de passe pour les administrateurs ;
* Installer les mises à jour critiques sans délai ;
* Effectuer des sauvegardes et les vérifier régulièrement ;
* Disposer de systèmes de détection et prévention d’attaques spécifiques.

*A éviter :*

* Utiliser des services non sécurisés ;
* Utiliser les serveurs hébergeant les bases de données pour d’autres fonctions comme naviguer sur internet, accéder à une messagerie électronique, etc.
* Placer les bases de données sur un serveur directement accessible depuis Internet ;
* Utiliser des comptes partagés entre plusieurs utilisateurs.

*Sécurisation du site internet*

Il s’agit de s’assurer que les bonnes pratiques minimales sont appliquées aux sites web.

*Précautions :*

* Limiter les ports de communication strictement nécessaires au bon fonctionnement des applications installées ;
* Limiter l’accès aux outils et interfaces d’administration aux seuls personnes habilitées ;
* Si des cookies non nécessaires au service sont utilisés, recueillir le consentement de la personne visitant le site internet après information et avant le dépôt du cookie ;
* Limiter le nombre de composants mis en œuvre, en effectuer une veille et les mettre à jour.

*A éviter :*

* Faire transiter des données à caractère personnel dans une URL telles que identifiants ou mots de passe ;
* Utiliser des services non sécurisés ;
* Utiliser les serveurs comme des postes de travail, notamment pour naviguer sur des sites internet, accéder à la messagerie électronique, etc. ;
* Placer les bases de données sur un serveur directement accessible depuis Internet ;
* Utiliser des comptes partagés entre plusieurs utilisateurs.

*Sauvegarde et prévention de la continuité d’activité*

Il est nécessaire d’effectuer des sauvegardes régulières pour limiter l’impact d’une disparition non désirée de données. Des copies de sauvegarde doivent être réalisées et testées régulièrement. Le back up journalier des données du serveur permet une remise en route de l’ensemble des activités de l’Organisme endéans les 24 heures.

Le responsable du service informatique dispose de la procédure à mettre en place en cas de disparition non désirée de données informatiques.

Le responsable de la sécurité informatique ou une personne déléguée teste régulièrement la restauration des sauvegardes et l’application du plan de continuité ou de reprise de l’activité.

*Précautions concernant la sauvegarde des données :*

* Effectuer des sauvegardes fréquentes des données : il peut être opportun de prévoir des sauvegardes « incrémentales » quotidiennes (c’est-à-dire n’enregistrer que les modifications faites par rapport à une précédente sauvegarde) et des sauvegardes complètes à intervalles réguliers ;
* Stocker les sauvegardes sur un site extérieur (si possible dans des coffres ignifugés et étanches) ;
* Protéger les données sauvegardées au même niveau de sécurité que celles stockées sur les serveurs d’exploitation.

*Précautions concernant la reprise et la continuité d’activité :*

* Rédiger un plan de reprise et de continuité d’activité informatique même sommaire, incluant la liste des intervenants ;
* S’assurer que les utilisateurs, prestataires et sous-traitants savent qui alerter en cas d’incident ;
* Tester régulièrement la restauration des sauvegardes et l’application du plan de continuité ou de reprise de l’activité.

*A éviter :*

* Conserver les sauvegardes au même endroit que les machines hébergeant les données. Un sinistre majeur intervenant à cet endroit aurait pour conséquence la perte définitive des données.

*Sécurisation des échanges avec d’autres organismes*

Il s’agit de renforcer la sécurité de toute transmission de données à caractère personnel.

*Précautions :*

* Lors d’envoi de mails groupés, mettre les adresses mail des destinataires en « copie cachée » ;
* Ne pas utiliser d’adresse mail type « gmail » ou autre messagerie grand public ;
* Chiffrer les données avant leur enregistrement sur un support physique à transmettre à un tiers (DVD, clé USB, disque dur externe,….) ;
* Chiffrer les pièces sensibles à transmettre si cette transmission utilise la messagerie électronique ;
* Utiliser un protocole garantissant la confidentialité et l’authentification du serveur destinataire pour les transferts de fichiers, en utilisant les versions les plus récentes des protocoles (exemple : SFTP, HTTPS) ;
* Assurer la confidentialité des secrets (clé de chiffrement, mot de passe,…) en les transmettant via un canal distinct (exemple : envoi du fichier chiffré par courriel et communication du mot de passe par téléphone ou SMS) ;
* Signature électronique lors de l’envoi des données qui garantit l’origine du message.

*A éviter :*

* Transmettre des fichiers contenant des données à caractère personnel en clair via des messageries grand public.

*Encadrement des développements informatiques*

Les structures qui développent des programmes ou des bases de données informatiques doivent intégrer la sécurité et la protection de la vie privée au plus tôt dans leurs projets.

Ainsi, l’intégration de la protection des données à caractère personnel, y compris l’exigence de sécurité des données, doivent être intégrées dès la conception de l’application ou du service informatique. Ces exigences peuvent se traduire par des choix de fonctionnalités (anonymisation à bref délai, minimisation des données), de technologies (chiffrement des communications), etc.

*A éviter :*

* Utiliser des données à caractère personnel réelles pour les phases de développement et de test. Des données fictives doivent être utilisées autant que possible ;
* Développer un programme ou une base de données et puis réfléchir dans un second temps aux mesures de sécurité à mettre en place. Les mesures de sécurité à mettre en place doivent être prises en compte dès la conception.

*Authentification des utilisateurs*

* *Option pour les Organismes fonctionnant en réseau*

Pour s’assurer que chaque utilisateur accède uniquement aux données dont il a besoin, l’Organisme dote chaque travailleur d’un identifiant qui lui est propre et veille à ce qu’il doive s’authentifier avant toute utilisation des moyens informatiques.

Le travailleur chargé de la gestion informatique de l’Organisme et la direction disposent des mots de passe et log in de l’ensemble du personnel. Le stockage des identifiants s’effectue de façon sécurisée.

* *Option pour les Organismes ne fonctionnant pas en réseau*

Chaque ordinateur est indépendant et chaque travailleur dispose de son code d’accès spécifique.

Il y a un ordinateur par poste de travail et celui-ci est dédié à un seul travailleur.

Afin de garantir la continuité du service en cas d’absence d’un travailleur, chaque travailleur communique à la personne responsable de la sécurité informatique ou à la direction ses codes d’accès à chaque modification de ceux-ci. La gestion des ordinateurs et la consultation des fichiers se fait en conformité avec la CCT n° 81 faisant partie intégrante du règlement de travail.

*Gestion des habilitations*

Il s’agit de limiter les accès aux seules données dont un utilisateur a besoin.

* *Option pour les Organismes fonctionnant en réseau*

Chaque travailleur disposant d’un identifiant et d’un mot de passe personnel n’a accès qu’aux seules données strictement nécessaires à l’accomplissement de ses missions.

Les éventuels stagiaires et étudiants effectuant un stage au sein de l’Organisme disposent, si le contenu du stage le justifie, d’un identifiant et mot de passe personnels limités à la durée de leur stage ou contrat.

En cas de suspension du contrat de travail, les identifiants et mots de passe sont bloqués.

En cas de fin du contrat de travail, les identifiants et mots de passe sont désactivés endéans les 24 heures.

Par ailleurs, chaque début d’année civile, une revue annuelle des habilitations est réalisée afin d’identifier et de supprimer les comptes non utilisés et de réaligner les droits accordés sur les fonctions de chaque utilisateur.

* *Option pour les Organismes ne fonctionnant pas en réseau*

Chaque travailleur communique à la personne responsable de la sécurité informatique ses codes d’accès à chaque modification de ceux-ci. La gestion des ordinateurs et la consultation des fichiers se fait en conformité avec la CCT n° 81 faisant partie intégrante du règlement de travail.

En cas d’oubli de ses codes d’accès, le travailleur s’adressera au à la personne responsable de la sécurité informatique ou à la direction. Celui-ci veillera à ce que les codes d’accès répondent aux prescriptions minimales de sécurité informatique.

*Traçage des accès et gestion des incidents*

Il s’agit de mettre en place des procédures pour gérer les incidents afin de pouvoir réagir en cas de violation de données (atteinte à la confidentialité, l’intégrité ou la disponibilité).

* *Option pour les Organismes fonctionnant en réseau*

L’Organisme a mis en place une procédure afin de pouvoir identifier un accès frauduleux, une utilisation abusive de données à caractère personnel ou de déterminer l’origine d’un incident.

Cette procédure consiste en un système d’enregistrement des activités des utilisateurs, des anomalies et des événements liés à la sécurité informatique. Cet enregistrement concerne les accès des utilisateurs en incluant leur identifiant, la date et l’heure de la connexion, la date et l’heure de la déconnexion.

Les utilisateurs sont informés de la mise en place d’un tel système.

Les équipements d’enregistrement et les informations enregistrées sont conservés et protégés par la personne responsable de la sécurité informatique. Celle-ci est la seule à avoir accès à ces données. Elle en gère l’utilisation conformément au RGPD et à la CCT n° 81 du Conseil National du Travail. Le responsable de la sécurité informe le responsable de traitement de toute anomalie ou incident de sécurité informatique.

Ces enregistrements journaliers sont conservés durant une période ne pouvant excéder 6 mois (sauf obligation légale ou risque particulièrement important).

*Administration du système d’information*

A titre préventif, l’Organisme peut mettre en place des systèmes automatiques de filtrage permettant de diminuer les flux d’informations et d’assurer la sécurité et la confidentialité des données. Il peut s’agir du filtrage des sites internet, de l’élimination des courriels non sollicités ou du blocage de certains protocoles (messagerie instantanée…).

La personne responsable de la sécurité informatique au sein de l’Organisme peut opérer sans avertissement les investigations nécessaires à la résolution de dysfonctionnements du système d’information ou de l’une de ses composantes, qui mettent en péril le fonctionnement ou l’intégrité du réseau informatique.

Pour ce faire, le service compétent s’appuie sur des fichiers de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions au système d’information. Ces fichiers comportent les données suivantes : dates, postes de travail et objet de l’événement.

La personne responsable de la sécurité information est la seule à utiliser ces informations qui sont effacées à l’expiration d’un délai de 3 mois.

A des fins de maintenance informatique, elle peut accéder à distance à l’ensemble des postes de travail. Si le travailleur est présent, il en sera prévenu à l’avance.

Dans le cadre de mises à jour et évolutions du système d’information, et lorsqu’aucun utilisateur n’est connecté sur son poste de travail, elle peut être amenée à intervenir sur l’environnement technique des postes de travail. Il s’interdit d’accéder aux contenus.

Elle opère également régulièrement une sauvegarde du système (back-up) afin de prévenir toute perte de données.

### Archivage sécurisé

Il est question d’archiver les données qui ne sont plus utilisées au quotidien mais qui n’ont pas encore atteint leur durée limite de conservation. Ces archives doivent être sécurisées notamment si les données archivées sont des données sensibles ou des données qui pourraient avoir des impacts graves sur les personnes concernées.

*Précautions :*

* Définir un processus de gestion des archives : quelles données doivent être archivées, comment et où elles sont stockées, etc. ;
* Mettre en œuvre des modalités d’accès spécifiques aux données archivées : l’utilisation d’une archive doit intervenir de manière ponctuelle et exceptionnelle selon les modalités déterminées ;
* Choisir un mode opératoire garantissant que l’intégralité d’une archive a été détruite.

*A éviter :*

* Utiliser des supports ne présentant pas une garantie de longévité suffisante (ex : un CD/DVD dépasse rarement 4ou 5 années) ;
* Conserver les données en les notant simplement comme étant archivées : les données archivées ne doivent être accessibles qu’à certaines personnes chargées d’y accéder.
* *Si l’Organisme ne procède pas à un archivage*

A ce jour, aucun archivage n’est réalisé, et ce pour les raisons suivantes :

* Le coût de l’archivage est disproportionné par rapport aux données à caractère personnel récoltées ;
* Les données récoltées sont indispensables tout au long de la relation contractuelle avec les personnes visées et ne peuvent donc être archivées tant que la relation contractuelle perdure ;
* Les données récoltées sont par ailleurs nécessaires dans le cadre d’un contrôle du travail effectué par l’Organisme et/ou des subventions octroyées à l’Organisme et doivent donc rester disponibles tant que la prescription n’est pas atteinte.
* *Si l’Organisme procède à un archivage*

Dans le cadre de la mise en réseau des données, les données à caractère personnel non nécessaires à l’exécution des missions de l’Organisme ne sont plus accessibles au personnel de l’Organisme.

Un archivage est effectué une fois par année civile. Cet archivage est conservé durant 10 ans débutant le 1er janvier de l’année suivant ledit archivage ou un délai plus long si certaines données archivées doivent être conservées en raison d’une action en justice (délai de prescription).

Le serveur sur lequel sont stockées les données archivées bénéficient des mêmes protections et mesures de sécurité informatique que les autres serveurs de l’Organisme.

L’accès aux données archivées ne peut s’effectuer que moyennant l’accord préalable du responsable du service informatique et du responsable du traitement des données.

Les archives sont détruites par une société agréée à cette fin.

### Encadrement de la maintenance et de la destruction des données

Il s’agit de garantir la sécurité des données à tout moment du cycle de vie des matériels et des logiciels.

Les interventions de maintenance confiées à un sous-traitant sont prévues dans le respect d’une clause de sécurité et de confidentialité, sous la responsabilité de la personne responsable de la sécurité informatique de l’Organisme et du responsable de traitement.

La convention avec ce sous-traitant prévoit également la destruction des données auxquelles le sous-traitant a éventuellement eu accès pour sa maintenance de la base de données utilisées par l’Organisme.

Les interventions de maintenance sont transcrites dans un registre ad hoc.

*Précautions :*

* Insérer une clause de sécurité dans les contrats de maintenance effectuée par des prestataires externes ;
* Encadrer par un responsable de l’Organisme les interventions par des tiers ;
* Rédiger et mettre en œuvre une procédure de suppression sécurisée des données ;
* Supprimer de façon sécurisée les données des matériels avant de les jeter, les envoyer en réparation chez un tiers ou en fin de contrat de location.

*A éviter :*

* Installer des applications pour la télémaintenance ayant des vulnérabilités connues ;
* Réutiliser, revendre ou jeter des supports ayant contenu des données à caractère personnel sans que les données n’aient été supprimées de façon sécurisée.

***Exemples de clauses de sécurité et de confidentialité à utiliser en cas de maintenance par un sous-traitant :***

*« Chaque opération de maintenance devra faire l’objet d’un descriptif précisant les dates, la nature des opérations et les noms des intervenants, transmis à* *………, responsable du service informatique, et ……, responsable du traitement des données.*

*En cas de télémaintenance permettant l’accès à distance aux fichiers de l’Organisme, le sous-traitant prendra toutes les dispositions nécessaires afin de permettre à l’Organisme d’identifier la provenance de chaque intervention extérieure. A cette fin, le sous-traitant s’engage à obtenir l’accord préalable de ………, responsable du service informatique, et ……, responsable du traitement des données, avant chaque opération de télémaintenance dont elle prendrait l’initiative.*

*Des registres seront établis sous les responsabilités respectives de l’Organisme et du sous-traitant, mentionnant les date et nature détaillée des interventions de télémaintenance ainsi que le nom de leurs auteurs.*

*Dans le cadre de l’exécution du contrat, le sous-traitant agira uniquement sur les instructions de l’Organisme. A ce titre, le sous-traitant s’engage à ne pas utiliser les données pour son propre compte ou pour celui d’un tiers.*

*Conformément au RGPD, le sous-traitant s’engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment de les protéger contre toute destruction accidentelle ou illicite, perte accidentelle, altération, diffusion ou accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite ou communication à des personnes non autorisées.*

*Le sous-traitant s’engage à prendre toutes précautions conformes aux usages et à l’état de l’art dans le cadre de ses attributions afin de protéger la confidentialité des informations auxquelles il a accès, et en particulier d’empêcher qu’elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.*

*Le sous-traitant s’engage en particulier à :*

* *ne pas utiliser les données auxquelles il peut accéder à des fins autres que celles prévues par ses attributions ;*
* *ne divulguer ces données qu’aux personnes dûment autorisées, en raison de leurs fonctions ;*
* *ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l’exécution de ses fonctions ;*
* *prendre toutes les mesures conformes aux usages et à l’état de l’art dans le cadre de ses attributions afin d’éviter l’utilisation détournée ou frauduleuse de ces données ;*
* *prendre toutes précautions conformes aux usages et à l’état de l’art pour préserver la sécurité physique et logique de ces données ;*
* *s’assurer, dans la limite de ses attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;*
* *en cas de cessation de ses fonctions, restituer intégralement les données, fichiers informatiques et tout support d’information relatif à ces données.*

*Cet engagement de confidentialité, en vigueur pendant toute la durée de la présente convention, demeurera effectif, sans limitation de durée après la cessation de la convention, quelle qu’en soit la cause, dès lors que cet engagement concerne l’utilisation et la communication de données à caractère personnel ».*

### Gestion de la sous-traitance

Il s’agit d’encadrer la sécurité des données avec les sous-traitants.

*Précautions :*

* Faire appel uniquement à des sous-traitants présentant des garanties suffisantes (notamment en termes de connaissances spécialisées, de fiabilité et de ressources). Exiger la communication par le prestataire de sa politique de sécurité des systèmes d’information ;
* Prendre et documenter les moyens permettant d’assurer l’effectivité des garanties offerts par le sous-traitant en matière de protection des données ;
* Prévoir un contrat avec les sous-traitants qui définit notamment l’objet, la durée, la finalité du traitement et les obligations des parties : celui-ci doit contenir en particulier des dispositions fixant leurs obligations en matière de confidentialité des données à caractère personnel, des contraintes minimales en matière d’authentification des utilisateurs, les conditions de restitution et/ou de destruction des données en fin de contrat, les règles de gestion et de notification des incidents.

Fait à , le .

*Signature, NOM, prénom et fonction du/de la responsable*

1. <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR> [↑](#footnote-ref-1)