

# POLITIQUE DE PROTECTION DES DONNÉES PERSONNELLES

À L'USAGE DES CLIENTS DE TERANGA SOFTWARE

Version 1.2 – 24/05/2018

## Table des matières

<b>Introduction</b>	<b>3</b>
<b>La gouvernance des données personnelles par TERANGA Software</b>	<b>3</b>
<b>Vos obligations en qualité de responsable de traitement des données collectées dans les applications de TERANGA Software</b>	<b>4</b>
<b>Les obligations de TERANGA Software en qualité de sous-traitant de vos traitements de données</b>	<b>6</b>

## 1. Introduction

L'intégration croissante des technologies dans le secteur de la gestion des maisons de retraite et de structures handicap s'accompagne de nouveaux enjeux tels que la conformité réglementaire, l'évolution des systèmes et des compétences ainsi que la sécurité et la confidentialité des données.

TERANGA Software s'impose aujourd'hui comme un acteur majeur de confiance pour les EHPAD et s'est engagé dans une politique de respect et de maintien de normes élevées en matière de déontologie et notamment de protection des données à caractère personnel.

Dans le cadre de notre mission de développement des applications NETSoins, NETFactu, NETContact, NETFamille, TERANGA Software met à disposition de ses clients des solutions opérant des traitements de données à caractère personnel.

Soucieux de construire avec nos clients des relations de confiance durables basées sur le respect mutuel et le partage de valeurs sociales responsables, TERANGA Software a mis en place les moyens techniques et organisationnels nécessaires afin d'être en conformité avec le règlement européen général de protection des données (ci-après « RGPD ») et de proposer à ses clients les garanties nécessaires en termes de protection des données en sa qualité de sous-traitant des traitements.

En effet, le responsable de traitement conformément aux dispositions du RGPD a l'obligation de faire uniquement appel à des sous-traitants présentant des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits de la personne concernée.

La présente politique a ainsi pour objet de présenter les engagements pris par TERANGA Software en matière de protection des données à caractère personnel en sa qualité de sous-traitant des données à caractère personnel mais aussi de rappeler à ses clients les principales nouvelles obligations à sa charge en qualité de responsable de traitement

TERANGA Software se tient disponible à l'adresse suivante pour apporter toute précision nécessaire concernant sa politique de protection des données à caractère personnel.

## 2. La gouvernance des données personnelles par TERANGA Software

La présente politique regroupe les règles, procédures et pratiques développées par TERANGA Software permettant de prendre en compte les exigences légales et réglementaires relatives à l'usage et la protection de ces données au titre de sa qualité de sous-traitant des données à caractère personnel pour ses clients, responsables de traitement.

Ainsi, TERANGA Software a mis en place une organisation interne destinée à gérer les différentes problématiques posées par la protection des données personnelles.

Dans ce cadre, TERANGA Software a créé à compter de 2018 un Comité de gouvernance chargé d'examiner les questions intéressant les questions sur les données à caractère personnel et d'assurer le respect de la politique générale de protection des données.

Par ailleurs, TERANGA Software a également désigné un délégué à la protection des données.

Le délégué à la protection des données de TERANGA Software a notamment pour mission de veiller au respect de la réglementation en matière de protection des données et coopérer avec la Commission Nationale Informatique et Libertés (CNIL) sur les questions relatives aux traitements.

Il est l'interlocuteur de la CNIL et de toutes les personnes concernées par une collecte ou un traitement de données à caractère personnel.

Le délégué à la protection des données personnelles de TERANGA Software peut être contacté par toute personne intéressée à l'adresse postale suivante :

RGPD TERANGA Software  
21, rue Viète  
75017 PARIS

ou

[rgpd@TERANGA-software.com](mailto:rgpd@TERANGA-software.com)

La politique de gouvernance mise en place par TERANGA Software repose sur le respect de principes directeurs applicables ) à la sous-traitance du traitement des données à caractère personnel pour le compte de ses clients, responsables de traitement.

### **3. Vos obligations en qualité de responsable de traitement des données collectées dans les applications de TERANGA Software**

Dans le cadre de vos relations contractuelles avec TERANGA Software, vous agissez en tant que responsable de traitement des données à caractère personnel. À ce titre, le RGPD vous impose les obligations suivantes :

- une utilisation légitime et proportionnée des données collectées de vos résidents/usagers/patients/personnes de l'entourage ;
- une utilisation des données compatible avec leur finalité ;
- les données personnelles collectées par votre établissement doivent être strictement nécessaires à l'objectif poursuivi par la collecte de données ;
- la collecte des données doit être loyale et transparente vis-à-vis des personnes concernées ;
- aucune collecte ne doit être effectuée à l'insu des personnes concernées et sans qu'elles en soient informées ;
- le recueil du consentement clair et explicite des personnes concernées par le traitement de leurs données personnelles est obligatoire que ce soit au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale. *A ce titre, dans nos applications nous avons ajouté à chaque formulaire de création d'utilisateur un rappel visuel sur les précautions à prendre en vertu du respect du cadre légal RGPD ;*

- le traitement des données de soin et de santé que votre établissement effectue doit être nécessaire et respecter les obligations légales en matière de protection de données de santé (tenir une documentation interne, désigner un DPO, assurer le respect du droit des personnes, réaliser une analyse d'impact ...);
- mise en place d'une politique d'habilitation stricte pour les personnes autorisées au sein de votre établissement. *(Dans nos applications cela fait référence à la gestion des identifiants/mots de passe, dates de début et fin de contrat, profil d'accès en cohérence avec la catégorie professionnelle de l'intervenant).*
- les données peuvent être transférées dans l'Union européenne ou dans un pays présentant les garanties suffisantes au regard du RGPD *(Ce que TERANGA Software confirme en tant qu'éditeur de logiciels hébergés);*
- respect de la limitation de la durée de conservation des données conformément aux finalités du traitement considéré et en accord avec la législation applicable notamment concernant les durées de prescription légale;
- respect du droit d'accès à l'information de la personne concernée : en cas de demande vous devez donner un accès aux données d'un résident/usager/patient *(Ce que vous pouvez faire via l'impression et la remise d'un dossier de liaison dans NETSoins par exemple, veuillez à cocher les bonnes options);*
- respect du droit de rectification de la personne concernée : un résident/usager/patient peut demander à faire modifier certaines données ou s'opposer à la collecte de certaines données le concernant de son vivant ou après sa mort;
- respect du droit à l'effacement de la personne concernée : la personne concernée a la possibilité d'obtenir de votre établissement l'effacement de données personnelles le concernant lorsque l'un des motifs suivants s'applique :
  - o Les données personnelles ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière;
  - o Le demandeur retire le consentement sur lequel est fondé le traitement; le demandeur s'oppose au traitement des données personnelles le concernant lorsqu'il n'existe pas de motif légal audit traitement;
  - o Le traitement des données personnelles n'est pas conforme aux dispositions de la législation et de la réglementation applicable.

Néanmoins, l'exercice de ce droit à l'effacement ne sera pas effectif pour certaines exceptions légales. *Dans la pratique, dans nos applications, vous devez archiver les dossiers des résidents/usager/patient mais la loi exige la conservation des données médicales pendant 20 ans après son dernier passage dans votre établissement ou 10 ans après son décès (Art R. 1112-7 du Code de la santé publique).*

- respect du droit à la portabilité des données : toute personne concernée disposera d'un droit à la portabilité sur ses données personnelles collectées par le responsable de traitement dans le cadre des finalités de ses services. *Dans la pratique, dans nos applications, vous pouvez fournir à la personne un export excel de ses données, pour cela allez dans Paramètres/Outils/Interface/Nouveau/Exporter/NETSoins résident (usuel);*
- respect du droit d'opposition de la personne concernée : la personne concernée a le droit de s'opposer, pour des raisons tenant à sa situation particulière, à un traitement de données personnelles le concernant. En cas d'exercice d'un tel droit d'opposition, votre établissement pourra cesser le traitement sauf lorsqu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et droits et les libertés de la personne concernée ou pour la constatation, l'exercice ou la défense d'un droit en justice;

- respect du droit à la limitation du traitement par la personne concernée: la personne concernée a la possibilité de demander la limitation du traitement de ses données personnelles ;
- respect du droit de recours de la personne concernée : la personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle, par exemple la CNIL sur le territoire français et ce sans préjudice de tout autre recours administratif ou juridictionnel. La personne peut effectuer ce recours auprès de l'autorité de contrôle de l'Etat membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise ;
- respect des directives post mortem de la personne concernée : la personne concernée a la possibilité de définir des directives relatives à la conservation, à l'effacement et à la communication de ses données personnelles après son décès. Si tel est le cas, votre établissement, au décès de la personne, respectera les directives enregistrées auprès d'elle.

#### **4. Les obligations de TERANGA Software en qualité de sous-traitant de vos traitements de données**

TERANGA Software a adopté des politiques et processus internes et met en œuvre des mesures qui respectent les principes de protection des données personnelles dès la conception de ses logiciels.

Ainsi, lors de l'élaboration et la conception de ses applications, TERANGA Software prend en compte le droit à la protection des données personnelles.

À ce titre, TERANGA Software procède à la pseudonymisation des données personnelles dès que cela est possible ou nécessaire.

Par ailleurs, dans le cadre de ses activités, TERANGA Software a choisi des hébergeurs de données de santé agréés, situés sur le territoire français.

En qualité de sous-traitant, TERANGA Software prend les engagements suivants en qualité de sous-traitant des traitements afin d'être en conformité avec les dispositions du RGPD :

- traitement des données à caractère personnel uniquement sur instruction documentée du responsable de traitement y compris en ce qui concerne le transfert des données à caractère personnel vers un pays tiers ou une organisation internationale à moins qu'il n'y soit obligé en vertu d'une obligation légale auquel cas le responsable de traitement en sera informé au préalable par TERANGA Software ;
- engagement de confidentialité imposé contractuellement aux personnes autorisées à traiter les données par TERANGA Software ;
- respect de toutes les mesures requises en vertu de l'article 32 du RGPD c'est-à-dire prendre toutes les mesures nécessaires à la sécurité des données à caractère personnel traitées. À ce titre, TERANGA Software s'engage à prendre les mesures de sécurité physiques, techniques et organisationnelles nécessaires contre tout accès, modification, déformation, divulgation, destruction ou accès non autorisés des données personnelles qu'elle détient pour le compte de ses clients ;

- aider le responsable de traitement à s'acquitter des demandes de personnes pour l'exercice de leurs droits (opposition, rectification, effacement) en s'engageant à transmettre par mail dans les meilleurs délais au responsable de traitement toute demande ;
- supprimer ou renvoyer toutes les données à caractère personnel du responsable de traitement comme TERANGA Software s'y engage contractuellement ;
- mettre à la disposition du responsable de traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues et pour permettre la réalisation d'audits notamment en mettant à disposition à première demande du responsable de traitement le registre des traitements que TERANGA Software effectue pour lui. Par ailleurs, les applications de TERANGA Software sont régulièrement soumises à des audits afin de vérifier la bonne application opérationnelle des règles relatives à la sécurité des données ;
- le respect des obligations mises à la charge du sous-traitant dans le cadre d'un recrutement d'un autre sous-traitant telles que décrites contractuellement. À ce titre, TERANGA Software choisit ses sous-traitants et prestataires avec soin et leur impose :
  - Un niveau de protection des données personnelles équivalent aux siens ;
  - Une utilisation des données personnelles ou des informations uniquement pour assurer la gestion des services qu'ils doivent fournir ;
  - Un respect strict de la législation et de la réglementation applicable en matière de confidentialité, de secret bancaire, et de données personnelles ;
  - La mise en œuvre de toutes les mesures adéquates pour assurer la protection des données personnelles qu'ils peuvent être amenés à traiter ;
  - La définition des mesures techniques, organisationnelles nécessaires pour assurer la sécurité.