# Logiciel ACT Enterprise de Vanderbilt

# Règlement général de l'UE sur la protection des données – Guide de conformité

## Table des matières


Résumé ..... 2
Présentation ..... 2
Que sont les données à caractère personnel ? ..... 2
Qu'est-ce qui constitue un traitement de données ? ..... 3
Agissez-vous en qualité de responsable du traitement ou de sous-traitant ? ..... 3
Qu'est-ce qu'un consentement et devez-vous en tenir compte ? ..... 4
Qu'est-ce qu'un contrat de traitement de données et devez-vous en tenir compte ? ..... 4
Connaître votre rôle et vos responsabilités ..... 4
ACT Enterprise et RGPD ..... 5

## Résumé

Les solutions et produits Vanderbilt permettent à leurs utilisateurs de gérer et de traiter des données à caractère personnel de sorte à répondre aux exigences du RGPD. Le présent guide a pour objectif d'aider et d'assister nos clients à évaluer leur propre aptitude à satisfaire leurs responsabilités et obligations à l'égard de ce nouveau règlement.

## Présentation

La protection des données est un droit fondamental en vertu duquel toute personne concernée a droit à la protection de ses données à caractère personnel. Le règlement général sur la protection des données (RGPD) est applicable depuis le 25 mai 2018 et a pour objectif de donner plus de contrôle aux personnes concernées sur leurs données à caractère personnel. Il s'agit d'un ensemble de règles communes applicable à l'ensemble de l'UE qui peut être complété dans certains domaines par la législation nationale des États membres.

Le RGPD impose des obligations aux entreprises ou aux organismes qui collectent, utilisent et traitent des données à caractère personnel. L'exigence à laquelle sont tenus les entreprises et les organismes, d'une part, d'afficher une transparence totale sur la façon dont ils utilisent et protègent les données à caractère personnel et, d'autre part, d'être en mesure de prouver leur responsabilité à l'égard de leurs activités de traitement des données constitue l'essence du RGPD. De telles données doivent être traitées de façon loyale pour des finalités déterminées et le traitement doit être fondé sur le consentement de la personne concernée ou sur une autre base juridique légitime.

Même si Vanderbilt met à disposition de ses clients des fonctionnalités de produits flexibles et intuitives destinées à faciliter le respect du nouveau règlement, nous ne collectons pas ni ne contrôlons, utilisons ou traitons les données à caractère personnel stockées dans les produits hébergés dans nos locaux. Par conséquent, il incombe au responsable du traitement et au sous-traitant des données à caractère personnel de veiller au respect des obligations stipulées dans le RGPD.

En cas de doute, ou si vous n'êtes pas certain de l'identité du responsable du traitement et/ou du sous-traitant de vos données, nous vous recommandons de vous rapprocher de votre conseiller juridique.

## Que sont les données à caractère personnel ?

Le terme « données à caractère personnel » désigne toute information relative à une personne vivante identifiée ou identifiable.

Une personne est identifiable si elle peut être identifiée directement ou indirectement par référence à un « identifiant ». Parmi les exemples d'identifiants, le RGPD mentionne notamment les noms, les numéros d'identification et les données de localisation. Une personne peut également être identifiable par référence à des éléments spécifiques propres à son identité, tels que des éléments physiques, génétiques ou culturels.

Les données à caractère personnel qui sont anonymisées, cryptées ou pseudonymisées, mais qui peuvent être utilisées pour identifier de nouveau une personne, restent des données à caractère personnel et relèvent du champ d'application du RGPD. Si des données à caractère personnel ont été anonymisées de telle sorte que la personne concernée ne peut plus être identifiée, celles-ci ne sont

pas considérées comme des données à caractère personnel. Pour que des données soient véritablement considérées comme anonymisées, l'anonymisation doit être irréversible.

Le règlement protège les données à caractère personnel indépendamment de la technologie ou de la méthode utilisée pour traiter lesdites données et il s'applique aussi bien au traitement automatisé que manuel. Cela vaut également pour la façon dont les données à caractère personnel sont conservées, qu'il s'agisse d'un système informatique, au moyen d'une vidéo surveillance ou sur papier, dans tous les cas, les données à caractère personnel sont soumises aux exigences de protection stipulées dans le RGPD.

## Qu'est-ce qui constitue un traitement de données ?

Le terme « traitement » désigne un large éventail d'opérations effectuées sur des données à caractère personnel, y compris par des moyens manuels ou automatisés. Il inclut 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 de données à caractère personnel.

Le règlement général sur la protection des données (RGPD) s'applique au traitement, en tout ou partie, de données à caractère personnel par des moyens automatisés ainsi qu'au traitement non automatisé dans la mesure où celui-ci résulte d'un fichier structuré.

## Agissez-vous en qualité de responsable du traitement ou de sous-traitant ?

Le terme « responsable du traitement » désigne la personne physique ou morale qui contrôle et est responsable de la conservation et de l'utilisation des informations personnelles sur un ordinateur ou dans des fichiers manuels structurés. En tant que responsable du traitement, il vous incombe des responsabilités légales. De ce fait, vous devez impérativement savoir si ces responsabilités s'appliquent à vous-même ou à votre entreprise.

Si vous ou votre entreprise contrôlez et êtes responsable des données à caractère personnel que vous détenez, c'est-à-dire si c'est vous qui décidez des informations personnelles qui doivent être conservées et des finalités de leur utilisation, alors vous ou votre entreprise êtes le responsable du traitement.

À titre d'exemple, parmi les cas de figure dans lesquels le responsable du traitement est une personne physique nous pouvons citer les médecins généralistes, les pharmaciens, les hommes politiques et les commerçants individuels dès lors que ces personnes conservent des informations personnelles sur leurs patients, leurs clients, leurs concitoyens, etc.

Si vous ou votre entreprise détenez des données à caractère personnel, mais qu'une autre personne ou entreprise décide et est responsable de ce qui advient aux données, cette autre personne ou entreprise est le responsable du traitement et vous ou votre entreprise agissez en qualité de « sous-traitant ».

À titre d'exemple, parmi les sous-traitants figurent les entreprises de gestion de paie, les comptables et les sociétés d'études de marché, lesquels peuvent détenir ou traiter des informations personnelles pour le compte d'un tiers.

## Qu’est-ce qu’un consentement et devez-vous en tenir compte ?

Afin de traiter de façon licite des données à caractère personnel, les entreprises et les organismes doivent en amont identifier et documenter la base juridique du traitement. Parmi les divers moyens licites de traiter des données, il existe :

- **L’obtention du consentement de la personne concernée** : obtenir le consentement de la personne concernée est approprié si celle-ci se voit offrir un véritable choix et un contrôle sur la façon dont ses données sont utilisées.
- **L’existence d’intérêts vitaux :** il s’agit d’un cas de figure en vertu duquel le traitement s’avère nécessaire dans le but de protéger les intérêts vitaux de la personne concernée, p. ex., pour protéger sa vie.
- **Le respect d’une obligation légale :** il est également possible de traiter des données si ce traitement est requis pour une finalité spécifique en vertu d’une loi de l’UE.
- **L’exécution d’un contrat avec la personne concernée :** il s’agit d’une situation dans laquelle le traitement se révèle nécessaire à l’exécution d’un contrat auquel la personne concernée est partie, p. ex., pour fournir les biens ou les services demandés.

Si vous n’êtes pas certain d’avoir obtenu un consentement suffisant pour traiter des données à caractère personnel, nous vous recommandons de vous rapprocher de votre conseiller juridique.

## Qu’est-ce qu’un contrat de traitement de données et devez-vous en tenir compte ?

Si vous détenez ou traitez (c’est-à-dire que vous saisissez, modifiez ou conservez) des données à caractère personnel (sous-traitant) au nom de votre client (responsable du traitement), vous devez conclure un contrat pour régir le traitement des données. Nous vous recommandons de vous rapprocher de votre conseiller juridique afin de vous assurer que le contrat stipule des mesures de sécurité appropriées ainsi que d’autres mesures de protection des données. Nous conseillons à nos clients d’y intégrer une liste de contrôle en ce qui concerne la gestion des données et le transfert du système de sécurité.

## Connaître votre rôle et vos responsabilités

L’évolution de la loi vers le RGPD est indiscutable et vous devez en tenir en compte dans la planification de votre système de sécurité. Vous devez identifier et traiter divers aspects susceptibles d’entraîner des problèmes de conformité en vertu du RGPD. Dans le cadre du RGPD, les personnes concernées sont en droit d’obtenir des informations claires au sujet de l’utilisation de leurs données.

La première étape pratique consiste à identifier votre rôle et vos responsabilités à l’égard du RGPD. Agissez-vous en tant que responsable du traitement ou en tant que sous-traitant ou les deux ? En cas de doute, ou si vous n’êtes pas certain de l’identité du responsable du traitement et/ou du sous-traitant de vos données, nous vous recommandons de vous rapprocher de votre conseiller juridique.

La deuxième étape consiste à assumer vos responsabilités. Tenez compte de toutes les données à caractère personnel que vous gérez via votre système de sécurité et passez-les en revue en prenant en considération les questions suivantes :

- Quelles données à caractère personnel sont conservées ?
- Sur quelle base juridique repose le traitement des données à caractère personnel ?

- Où sont conservées les données ?
- De quelle façon les données sont-elles protégées ?
- Pendant combien de temps les données sont-elles conservées ?
- Quelle est la politique en matière de gestion des demandes d'accès des personnes concernées ?
- Quelle est la procédure si une personne concernée demande son retrait du système ?
- Qui a accès aux données ?
- Les données à caractère personnel sont-elles transférées en dehors de l'EEE ?

# ACT Enterprise et RGPD

Les informations suivantes décrivent la façon dont le système ACT Enterprise de Vanderbilt peut être utilisé en vue de faciliter le respect du RGPD.

## Quelles données à caractère personnel sont conservées ?

Il n'est pas nécessaire de conserver des données à caractère personnel pour faire fonctionner correctement le système ACT Enterprise.
La photo, le nom, l'adresse e-mail et le numéro de téléphone sont des champs prédéfinis dans le système, mais l'utilisateur peut se servir de champs personnalisables pour saisir diverses données à caractère personnel.

## Sur quelle base juridique repose le traitement des données à caractère personnel ?

La saisie de données et leur conservation sont contrôlées par le responsable du traitement et le sous-traitant du site. En tant que tel, il incombe au responsable du traitement et/ou au sous-traitant de s'assurer d'obtenir la base juridique nécessaire pour traiter les données à caractère personnel.

Il n'existe aucune procédure explicite intégrée au logiciel ACT Enterprise qui permette d'obtenir le consentement de l'utilisateur ou de l'enregistrer.

## Où sont conservées les données ?

Les données sont conservées dans la base de données ACT Enterprise hébergée sur le serveur ainsi que dans les sauvegardes. Certaines données à caractère personnel, telles que les noms, peuvent être conservées dans les contrôleurs du système. Toutefois, cette option peut être désactivée par le propriétaire du système.

## De quelle façon les données sont-elles protégées ?

Pour accéder au contenu de la base de données ACT Enterprise, il convient d'utiliser un logiciel client (ACT Manage, ACT Monitor ou ACT Install). Un identifiant et un mot de passe permettent de protéger l'accès au logiciel.
Nous ne cryptons aucune donnée à caractère personnel. L'utilisateur final peut choisir d'appliquer lui-même une forme de cryptage au niveau de la base de données (SQL Server ou SQL Compact).
Le personnel de Vanderbilt n'a pas accès au système du client, sauf s'il a été autorisé à se connecter à distance.

## Pendant combien de temps les données sont-elles conservées ?

Dans ACT Enterprise, les données relatives à un détenteur de badge sont conservées tant que la personne en a besoin. L'utilisateur peut définir des dates de fin de validité applicables aux badges dans le système, mais il lui appartient de procéder à la suppression des données du détenteur du badge lorsque ce dernier expire. Vanderbilt propose une fonctionnalité de génération de rapport d'expiration des badges pour faciliter cette procédure manuelle.

En outre, il existe une fonctionnalité personnalisable par l'utilisateur qui permet de purger les évènements de journal postérieurs à une période de mois définie. Par défaut, les évènements sont conservés pendant une période de temps indéfinie.
Lorsque l'utilisateur supprime le compte d'un détenteur de badge, le système ne supprime pas par défaut les évènements de journal qui lui sont associés. Toutefois, il est possible de modifier ce paramètre par défaut afin de supprimer les évènements de journal dès lors qu'un compte de détenteur de badge est supprimé.

## Quelle est la politique en matière de gestion des demandes d'accès des personnes concernées ?

En cas de demande, il incombe au responsable du traitement et/ou au sous-traitant d'exposer la politique et de fournir les données en temps opportun conformément aux dispositions du RGPD.

ACT Enterprise offre la possibilité, d'une part, de générer différents rapports qui permettent de consulter les informations détenues au sujet d'une personne concernée, telles que les évènements de journal récents, et, d'autre part, un moyen d'exporter ces données sous forme de rapports au format PDF ou CSV.

## Quelle est la procédure si une personne concernée demande son retrait du système ?

En cas de demande, il incombe au responsable du traitement et/ou au sous-traitant d'exposer la politique et de supprimer les données en temps opportun conformément aux dispositions du RGPD.

L'utilisateur peut supprimer manuellement les données relatives à un détenteur de badge du système ACT Enterprise. Le système ne supprime pas par défaut les évènements de journal qui lui sont associés. Toutefois, il est possible de modifier ce paramètre par défaut afin de supprimer les évènements de journal dès lors qu'un compte de détenteur de badge est supprimé.

## Qui a accès aux données ?

Il incombe au responsable du traitement et/ou au sous-traitant de divulguer l'identité des personnes qui ont accès aux données à caractère personnel du système ACT Enterprise installé sur le site. Il appartient au responsable du traitement et/ou au sous-traitant d'élaborer et d'appliquer de telles procédures.

ACT Enterprise dispose d'un système d'utilisateurs de bases de données qui permet d'accorder des droits à des personnes spécifiques selon le logiciel client. Tous les accès au système sont vérifiés, y compris les connexions, les modifications apportées aux données des utilisateurs et les actions.

## Les données à caractère personnel sont-elles transférées en dehors de l'EEE ?

Dans le cadre d'un fonctionnement normal, les données relatives aux utilisateurs d'ACT Enterprise ne sont pas partagées en dehors du système. Il incombe au responsable du traitement et/ou au sous-traitant d'informer les utilisateurs si le système est configuré de sorte à transférer des données en dehors de l'EEE.