Conseils pratiques relatifs au RGPD

Introduction

Il ne fait aucun doute qu'au sein de votre zone vous gérez des matières personnalisables qui sont traitées par toutes sortes de canaux et qui doivent être adéquatement protégées.

Avec l'entrée en vigueur du Règlement Général sur la Protection des Données (ci-après dénommé RGPD) le 25 mai 2018, cette protection est accrue.

C'est l'objet du contrat qu'AbiWare – en qualité de sous-traitant – conclut avec ses clients qui sont responsables du traitement des données.

Avec cette note complémentaire au contrat, nous souhaitons vous assister en dressant la liste des matières personnalisables de notre logiciel et les mesures que vous pouvez prendre.
En tant que sous-traitant, nous nous engageons à préserver l'intégrité de nos logiciels et à offrir une variété de fonctions de sécurité pour protéger vos données contre toute utilisation non autorisée.

Cette note vous donne un aperçu général des différentes données personnelles que vous gérez via notre logiciel et de ce que vous pouvez faire pour les sécuriser.
Pour plus d'informations et de soutien, veuillez contacter nos consultants AbiWare.

Notez que ce document ne traite pas des mesures de sécurité que vous devez prendre dans le cadre du stockage des données. Ceci est l'objet du sous-traitant qui gère le stockage des données.

Confidentialité

Dans le cadre du RGPD, il est important que les employés du sous-traitant et le responsable du traitement qui ont accès aux données personnalisables soient liés par une obligation légale, statutaire ou par une disposition contractuelle équivalente, afin de respecter la confidentialité des données concernées. Vous pouvez le faire, par exemple, au moyen d'une clause de confidentialité dans le règlement du travail ou d'un contrat de confidentialité séparé.

AbiWare bvba/sprl • ☎ 014/56 37.50 • fax : 014/56.37.55 mail: info@abiware.be • http//www.abiware.be

Sources des informations : registre des données

Si nous regardons les données personnalisables, nous les retrouvons pour différentes catégories de personnes impliquées :

Catégories concernées		Modules
1	Utilisateurs du logiciel	Administrateur Système
2	Personnel	GRH
3	Dossiers	Dossiers Préventions et Interventions
4	Données fournisseurs	Fournisseurs
5	Adresses de facturation	Facturation (intervention, ambulance, prévention)
6	Adresses d'intervention	Rapports d'intervention
7	Patients	Ambulance

Pour chacune de ces catégories, vous devez savoir précisément quelles données personnelles vous traitez et conservez. Pour chaque donnée, il doit y avoir une base légale dans le cadre de la RGPD. Vous n'êtes donc pas autorisés à conserver des données personnelles.

La conservation de ces données repose sur la nécessité d'en assurer le bon fonctionnement : organisation de formations, paiement des prestations, facturation, conservation d'informations utiles dans le cadre d'incidents.

Types de données personnelles	Catégorie(s) de pers. concernées
Données d'identification	1, 2, 3, 4, 5, 6, 7
Données d'identification électroniques (IP-adresses, …)	1
Numéro National	1, 2, 5, 7
Caractéristiques personnelles (âge, sexe, état civil, …)	2, 7
Composition de famille	2
Profession et emploi	2
Détails financiers	2
Etudes et formations	2
Données médicales ou relatives à la santé	2, 7

Pour chacune de ces données les règles de sécurité sont applicables :

- Confidentialité
  - Accès aux seules personnes autorisées
  - Attention particulière pour les données sensibles (données patient, personnelles)
  - S'assurer que les données ne soient pas divulguées
- Intégrité
  - Justesse des données
  - Vérification des données
- Disponibilité
  - Qui a accès à quoi, quand, où et comment

Utilisateurs et droits d'accès

Dans le cadre du RGPD, il est important de savoir qui a accès aux données et aux processus. Cela concerne la confidentialité et le (s) rôle (s) assigné (s).

Au sein de la plate-forme logicielle AbiWare, l'accès peut être accordé en fonction des droits en fonction :

- du poste, du cluster, de la zone
- du module
- d'une partie d'un module
- du processus (ex. : lecture, modification, suppression)
- de la personne (ex. : évaluations)

Dans le cadre du RGPD des droits d'accès spécifiques sont prévus pour les données personnelles sensibles.

Afin de savoir qui a accès à quelles données et de quelle manière, consultez la gestion de l'ordinateur. Vous pouvez rechercher tous les utilisateurs et leurs accès.

L'octroi des droits d'accès aux utilisateurs est généralement effectué par l'Administrateur système. Il est important de séparer ce rôle des autres rôles.
La personne qui remplit le rôle d'administrateur système n'a qu'une fonction technique, à savoir l'attribution des droits et est indépendante des autres rôles que cette personne aurait au sein de l'organisation. La politique d'attribution des droits doit être définie par les responsables de l'organisation. La cellule de sécurité de l'information peut également jouer un rôle à cet égard. Nous recommandons que la liste des profils d'accès et des utilisateurs soit validée (approuvée) par le responsable final au moins une fois par an.

Dans ce cadre, vous pouvez demander une vue d'ensemble concise ou détaillée des éléments suivants :

- les profils utilisateurs et les possibilités d'accès
- les utilisateurs et qui a accès à quels profils utilisateurs

Cet aperçu peut être imprimé et utilisé en tant que document de validation.

Droits de suppression : la suppression des données doit être effectuée de manière à éviter toute perte de données non autorisée. Il est préférable de ne pas accorder de droits de retrait sur des données qui ne peuvent en principe jamais être effacées (par exemple, le dossier personnel).

S'il est décidé de supprimer des données spécifiques pour lesquelles aucun droit de suppression n'a été accordé, il est toujours possible d'accorder des droits de suppression temporaire afin d'atteindre cet objectif.

Gestion mots de passe : nous recommandons de mettre en place une protection stricte par mot de passe si vous choisissez de vous connecter à l'aide d'un mot de passe.

Données personnelles GRH

Le module GRH contient de nombreuses informations personnelles.
Selon le rôle qui vous est assigné, vous verrez plus ou moins d'informations.
Selon le GDPR, certaines données personnelles sont plus sensibles que d'autres.

Les questions que vous devriez poser dans ce contexte comprennent, entre autres choses :

- quelles données doivent être visibles et pour quel rôle
- quelles données ont sensibles et doivent être protégées
- comment valider la véracité des données
- comment organiser le droit de consultation et le droit d'oubli

A savoir :

- Via les profils limiter les accès à sa propre fiche ou à plusieurs fiches, liés aux postes ou non.
- En accordant des droits, vous limitez l'accès aux données au niveau des sous-sections relatives au dossier personnel, à la performance, à la formation et aux congés.
- Au niveau de la formation, des évaluateurs et des superviseurs en fonction des éléments de formations.
- Avec AbiWeb possibilité pour les supérieurs fonctionnels et les coordinateurs d'effectuer des évaluations.
- Avec AbiFire et AbiWeb Personnel, chaque membre du personnel peut vérifier ses propres données. AbiWeb offre la possibilité de demander une rectification de données.

Données personnelles patient

Les renseignements patient contiennent des données très sensibles auxquelles vous devez accorder une attention particulière.

Dans le cadre d'AmbuReg, cela sera précisé dans l'A.R.

Pour des informations supplémentaires vous pouvez vous basé sur les circulaires de l'AMU.
Pour les incidents d'ambulance actuels, il y a déjà une circulaire concernant la sécurité des terminaux d'alarme (26-07-2017).

A savoir :

- Dans ce contexte, notre logiciel a déjà été adapté de façon à ce que les informations sensibles confidentielles sur le patient puissent être dissimulées aux personnes non autorisées. L'accès à ces informations est une initialisation distincte et a un impact sur les rapports, la fiche patient et les résultats de recherche.
- -Les patients ont des droits de regard dans leurs dossiers. Lorsqu'un patient le demande, nous recommandons qu'un formulaire de demande soit rempli avec authentification de l'identité. Lorsque vous imprimez la feuille de patient, vous pouvez joindre une lettre dans la pièce jointe qui indique la confidentialité des données, et est datée par la personne en charge du service d'ambulance.

Périodes de rétention et droit à l'oubli

Le RGPD déclare d'abord et avant tout que les données personnelles ne doivent pas être conservées plus longtemps que nécessaire pour atteindre les objectifs pour lesquels elles ont été obtenues ou traitées. Le stockage indéfini de données personnelles n'est qu'exceptionnellement admissible. En fonction de ces objectifs, vous devez donc déterminer combien de temps ces données doivent être conservées et si vous supprimez ou anonymisez les données. Cela peut également être déterminé par des normes imposées par la loi : factures, KB AmbuReg, circulaires, ...

Le droit d'oublier ou le droit à la modification des données est défini à l'article 17 de la RGPD.

L'exécution de ce droit doit être considérée dans le contexte de l'objet de l'enregistrement et des périodes de conservation spécifiées. Si les données personnelles ne sont pas nécessaires pour le bon fonctionnement et les fins légitimes de l'organisation, il n'y a pas d'objection à la suppression des données personnelles. En pratique, nous nous attendons à ce que ce droit soit rarement exercé dans le contexte de l'organisation du service d'incendie.