



Le RGPD appliqué à Coswin

Les bonnes pratiques

Documentation

Version : 3.1
Date : 02/11/2022
Auteur(s) : Vincent Gosselin
Copyright : Siveco Group - R&D - Service Produits et Testing

Table des matières

1. Introduction	4
1.1. Objet du document	4
1.2. Méthodologie	4
1.3. Rappels et définitions	4
2. Délimitation du contexte des traitements	7
2.1. Qui est concerné par le RGPD ?	7
2.2. Contexte des traitements des données personnelles dans Coswin	7
3. Données personnelles et traitements	9
3.1. Les principes de la protection des données	9
3.2. Identification des données personnelles dans Coswin	10
3.3. Gestion des utilisateurs dans Coswin	10
3.4. Enregistrements sans données personnelles directes	11
3.4.1. Utilisateurs	11
3.4.1.1. Inventaire des données et des traitements	11
3.4.1.2. Conservation des données	12
3.4.1.3. Centrage de la carte par rapport à la position de l'utilisateur	13
3.4.2. Demandeurs	14
3.4.2.1. Inventaire des données et des traitements	14
3.4.2.2. Conservation des données	14
3.4.3. Superviseurs	14
3.4.3.1. Inventaire des données et des traitements	15
3.4.3.2. Conservation des données	15
3.4.4. Contacts	15
3.4.4.1. Inventaire des données et des traitements	15
3.4.4.2. Conservation des données	16
3.4.4.3. Gestion du consentement des contacts	16
3.5. Gestion des signatures dans Coswin	17
3.5.1. Signature dans les enregistrements	17
3.5.2. Signature dans l'historique des circuits de validation	19
3.6. Messagerie instantanée	19
3.6.1. Gestion des utilisateurs sur le serveur de messagerie instantanée	20
3.6.2. Conservation des données	20
3.7. Enregistrements avec données personnelles directes - Employé	20
3.7.1. Inventaire des données et des traitements	21
3.7.2. Conservation des données	22
3.7.3. Calendrier de l'employé	22
3.7.3.1. Contenu du calendrier de l'employé	22
3.7.3.2. Conservation des données du calendrier	23
3.7.4. Gestion de la géolocalisation des personnes dans Coswin	24
3.8. Données pour l'administration de Coswin	25
3.8.1. Éditeur de rapports	25
3.8.2. Console d'administration	26
3.8.3. Audit trail	26

4. Droits des personnes concernées	27
4.1. Consentement de l'utilisateur	27
4.1.1. Message à la connexion	28
5. Sécurisation des données	29
5.1. Sécurité de l'application Coswin	29
5.2. Sécurité de la plate-forme Coswin	31
6. Annexe	33
6.1. Définitions (complément)	33
6.2. Les 8 règles d'or	34
6.3. Données sensibles	35
6.3.1. Définition	36
6.3.2. Exceptions	36
6.4. Liste des champs Coswin anonymisable / pseudonymisable	36
6.5. Conservation des données	39
6.6. Évaluation des mesures protectrices des droits des personnes concernées	40
6.7. Appréciation des risques : les atteintes potentielles à la vie privée	40

1. Introduction

Coswin est une des composantes de votre système d'information. Il est susceptible de contenir et de traiter des données à caractère personnel. Les traitements de ces données doivent donc être consignés dans le registre prévu par le **RGPD**.

Ce document se base sur les fonctionnalités de la version **Coswin 8i.9**.

1.1. Objet du document

Ce document a vocation à aider le DPO (délégué à la protection des données) à mener un PIA (Privacy Impact Assessment - *Analyse d'impact relative à la protection des données*) :

1. [Constituer le registre de vos traitements](#) de données appliqués à Coswin.
2. [Faire le tri dans les données](#) en appliquant les bonnes pratiques dans Coswin.
3. [Respecter les droits des personnes](#) identifiées dans Coswin.
4. [Sécuriser les données personnelles](#) des personnes identifiées dans Coswin.

1.2. Méthodologie

Ce document se base sur la méthodologie préconisée par la CNIL dans ces trois guides téléchargeables sur son site :

<https://www.cnil.fr/fr/PIA-privacy-impact-assessment>

Analyse d'impact relative à la protection des données — *Privacy Impact Assessment (PIA)* :

- LA MÉTHODE
- LES MODÈLES
- LES BASES DE CONNAISSANCES

1.3. Rappels et définitions

RGPD

“ L'acronyme RGPD signifie **Règlement Général sur la Protection des Données** (en anglais « *General Data Protection Regulation* » ou *GDPR*).

Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne.

(...)

Ce nouveau règlement européen s'inscrit dans la continuité de la Loi française Informatique et Libertés de 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant.

Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels. Il permet de développer leurs activités numériques au sein de l'UE en se fondant sur la confiance des utilisateurs.

(source CNIL)

Textes officiels sur :

<https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR>



Données personnelles

“ Une **donnée personnelle** est toute information se rapportant à une personne physique identifiée ou identifiable.

Une personne peut être identifiée :

- **directement (exemple : nom, prénom)**
- ou **indirectement** (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image).



(source CNIL)

Traitement des données personnelles

“ Un **traitement de données personnelles** est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement).



Remarque

“ Un traitement de données doit avoir un **objectif**, une **finalité**, c'est-à-dire que vous ne pouvez pas collecter ou traiter des données personnelles simplement au cas où cela vous serait utile un jour.

À chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de votre activité professionnelle.



(source CNIL)

Aller plus loin

Chapitre > Définitions (complément) ^[p.33].

2. Délimitation du contexte des traitements

2.1. Qui est concerné par le RGPD ?

Le RGPD s'applique à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non, dès lors :

- Qu'elle est établie sur le territoire de l'**Union européenne**.
- Que son activité cible directement des **résidents européens**.



Exemple

Une société établie en **France**, qui exporte l'ensemble de ses produits au **Maroc** pour ses clients moyen-orientaux **doit respecter le RGPD**.



De même, une société établie en **Chine**, proposant un site de e-commerce en français livrant des produits en **France** **doit respecter le RGPD**.



2.2. Contexte des traitements des données personnelles dans Coswin

Coswin est un logiciel de GMAO (gestion de la maintenance assistée par ordinateur).

Il a pour objectif de gérer la maintenance des équipements référencés dans sa base de données.

La programmation des travaux de maintenance nécessite de connaître des informations sur les personnels intervenants :

- La disponibilité d'une personne (présence, positionnement).
- Les compétences, qualifications, habilitations d'une personne.

Important

Toutes autres **informations à caractère privé n'ont pas vocation à être consignées dans Coswin**. Il conviendra dans tous les cas :

- D'en informer les personnes.
- De mettre en œuvre les mesures de protection de ces informations.
- De soumettre le consentement des utilisateurs.

De plus **aucune donnée sensible** (au sens du RGPD) n'a vocation à être consignée dans Coswin.

Leur traitement est par principe interdit.



Aller plus loin

Chapitre > Données sensibles ^[p.35].

Remarque

Pour des besoins d'administration informatique, des raisons de traçabilité (contraintes réglementaires, contractuelles) ou de facilité d'usage, des informations pouvant identifier une personne de façon indirecte peuvent être consignées dans Coswin :

- Adresse IP
- Accès à l'application
- Horodatage de commentaire
- Historique de changement d'état
- Historique de validation
- Position GPS

3. Données personnelles et traitements

3.1. Les principes de la protection des données

Le RGPD encadre la collecte, l'utilisation et la conservation des données personnelles par **8 règles d'or** auxquelles tout organisme privé ou public doit se conformer.

8

Aller plus loin

Chapitre > Les 8 règles d'or ^[p.34].

Ces 8 règles d'or peuvent être résumées en **4 bons réflexes** :

4

1. Ne collecter que les données vraiment nécessaires

Posez-vous les questions suivantes :

- Quels sont les **objectifs** ?
- Ces données sont-elles **indispensables** pour atteindre ces objectifs ?
- Ai-je le **droit** de collecter ?
- Est-ce **pertinent** ?
- Dois-je recueillir l'**accord** des personnes ?



2. Être transparent

Vous devez fournir une **information claire et complète** aux personnes sur l'usage qui sera fait de leurs données personnelles.



3. Respecter le droit des personnes

Vous devez répondre dans les meilleurs délais aux demandes :

- D'**accès**
- De **rectification**
- De **suppression**



des données.

4. Sécuriser les données

La sécurité informatique, la sécurité physique doit être adaptée à la **sensibilité des données** et aux **risques** en cas d'incident.



3.2. Identification des données personnelles dans Coswin

Cet inventaire est constitué sur la base des modules standards de Coswin. Il conviendra au client de l'adapter en fonction de l'usage qu'il peut faire d'autres modules (modules libres par exemple).

Il concerne principalement :

- La fiche employé (qui peut contenir des données personnelles **directes**).

Entrent en jeu également d'autres modules (qui peuvent contenir des données personnelles **indirectes**) :

- Les contacts des sociétés
- La liste des demandeurs
- Les signatures des utilisateurs sur les enregistrements de Coswin
- L'horodatage des champs de texte riche (OT, DI et Devis)
- L'historique des connexions à Coswin
- L'historique des circuits de validation
- L'audit des transactions

3.3. Gestion des utilisateurs dans Coswin

Seuls les utilisateurs référencés dans la base de données Coswin peuvent avoir accès aux informations qui y sont stockées (et parmi celles-ci des données personnelles).

Sont consignées dans la base de données des personnes qui peuvent être désignées comme :

- Des **utilisateurs** (*personnes utilisatrices de Coswin pouvant consulter, modifier, créer ou supprimer des données en fonction de leur profil*).
- Des **employés** (*personnes chargées d'effectuer des tâches de maintenance auxquelles on affecte un travail et qui consignent leurs temps passés dans Coswin*).
- Des **demandeurs** (*personnes qui émettent des besoins – demande d'intervention, demande d'achat – qui sont détenteurs ou mainteneurs des équipements référencés dans Coswin, etc.*).
- Des **superviseurs** (*personnes responsables des travaux et qui supervisent le travail de leurs employés*).
- Des **contacts** (*personnes référencées chez des fournisseurs, des entités ou des magasins*).

Nouveauté 8i.9

→ À partir de la version **8i.9**, Coswin dispose d'une fonction de **renommage** sur chacun de ces modules et d'une fonction d'**anonymisation** des utilisateurs.

Pour des questions de facilité d'utilisation, il est possible d'associer un **utilisateur** Coswin à :

- Un employé
- Un demandeur

- Un superviseur

Remarque

Les codes [Utilisateur](#) , [Employé](#) , [Demandeur](#) et [Superviseur](#) peuvent être différents les uns des autres.

Bonne pratique

Pour référencer ces personnes dans la base de données Coswin, préférez un matricule à un code nominatif qui permettrait d'identifier directement la personne.

Si cela est nécessaire, indiquez les noms et prénom dans la description associée au code.

Exemple :


Déconseillé		Préférable	
Code	Description	Code	Description
DUPONT A	Dupont Alexandre	M436T	Dupont Alexandre

Si la personne demande à ce que son nom n'apparaisse plus dans Coswin, il suffit alors de modifier la description associée au code.

→ L'application **IOD** permet le renommage des codes [Utilisateur](#) , [Employé](#) , [Demandeur](#) et [Superviseur](#) .

3.4. Enregistrements sans données personnelles directes

3.4.1. Utilisateurs

Emplacement :  Outils > Sécurité et profils > Utilisateurs

3.4.1.1. Inventaire des données et des traitements

Il n'est pas nécessaire de consigner des données personnelles sur ce module.

En revanche, des informations permettent d'identifier la personne :

- Description (1)
- Signature (1)
- Adresse électronique
- Photo / avatar de l'utilisateur



(1) voir chapitre [Gestion des signatures dans Coswin](#) ^[p.17].

💡 Bonne pratique

Les numéros de téléphone, les adresses électroniques consignés doivent être des coordonnées professionnelles.

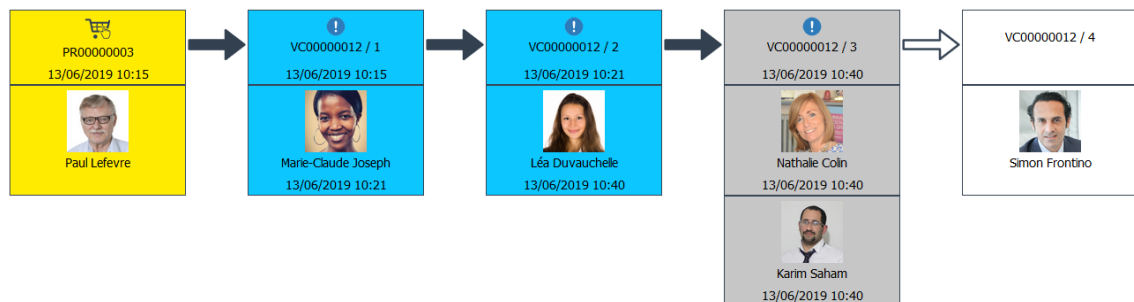


La photo / avatar spécifié de l'utilisateur est visible :

- Par lui-même dans le menu utilisateur



- Par les autres utilisateurs dans l'historique des circuits de validation



- Sur la fenêtre du chat de la messagerie instantanée (nouveau 8i.9).

3.4.1.2. Conservation des données

Les informations liées à cet enregistrement doivent être **supprimées ou anonymisées** une fois que la relation contractuelle est terminée.

- Suppression des informations (données personnelles) associées à l'enregistrement.
- Pseudonymisation — au besoin — du code de l'enregistrement avec l'option **IOD**.



Aller plus loin

Chapitre > Conservation des données [p.39].

Si l'utilisateur n'a plus à se connecter à Coswin, par exemple suite à :

- Un changement de poste
- Un départ
- Une fin de mission
- etc.

son compte Coswin doit être supprimé (ou à défaut verrouillé).

LDAP

Si l'authentification de l'utilisateur est faite au travers d'un annuaire LDAP, c'est à ce niveau que la suppression ou la suspension du compte doit être faite.

Remarque

L'employé, le demandeur ou le superviseur associés à l'utilisateur peuvent être conservés dans la base de données même si le compte utilisateur est supprimé.

Nouveauté 8i.9

→ Depuis la version [Coswin 8i.9](#), ce module dispose d'une fonction **anonymisation**.

3.4.1.3. Centrage de la carte par rapport à la position de l'utilisateur

Lorsqu'un utilisateur charge le module [Géolocalisation](#) de Coswin, il ouvre une carte sur une emprise qui est fonction du paramétrage.

Emplacement : [Outils > Sécurité et profils > Utilisateur > champ Ouverture de la carte](#) (disponible dans l'éditeur de ressources) :

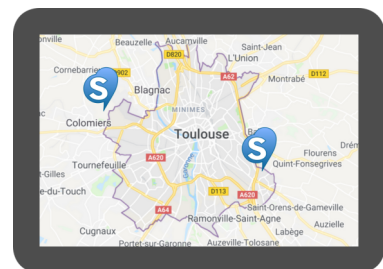
- GPS/IP (1) la carte sera centrée sur la position GPS de sa tablette.
- Employé la carte sera centrée sur la dernière position (latitude / longitude) connue de l'employé associé à l'utilisateur connecté.

(1) cette information est récupérée de la fonction de localisation du navigateur mais **n'est pas stockée dans Coswin**.

Exemple avec l'option GPS/IP

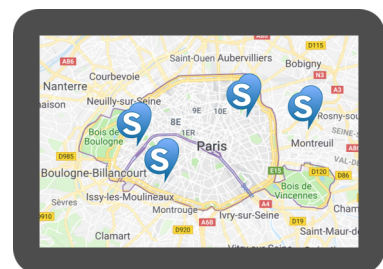
- L'utilisateur est physiquement à **Toulouse**, depuis sa tablette, il ouvre le module Géolocalisation :

→ La carte est chargée sur **Toulouse**.



- L'utilisateur est physiquement à **Paris**, depuis sa tablette, il ouvre le module Géolocalisation :

→ La carte est chargée sur **Paris**.



L'utilisateur n'est pas matérialisé par un marqueur sur la carte, sa position détermine uniquement le centrage de la carte.

Les marqueurs indiquent la position des objets Coswin géolocalisés.

Aller plus loin

Chapitre > Gestion de la géolocalisation des personnes dans Coswin ^[p.24]

3.4.2. Demandeurs

Emplacement :  Communs > Demandeurs

3.4.2.1. Inventaire des données et des traitements

Il n'est pas nécessaire de consigner des données personnelles sur ce module.

En revanche, des informations permettent d'identifier la personne :

- Description
- Adresse électronique
- Téléphone
- Photo / avatar du demandeur



Bonne pratique

Les numéros de téléphone, les adresses électroniques consignés doivent être des coordonnées professionnelles.



3.4.2.2. Conservation des données

Les informations liées à cet enregistrement doivent être **supprimées ou anonymisées** une fois que la relation contractuelle est terminée.

- Suppression des informations (données personnelles) associées à l'enregistrement.
- Pseudonymisation — au besoin — du code de l'enregistrement avec l'option **IOD**.




Aller plus loin

Chapitre > Conservation des données ^[p.39].

Nouveauté 8i.9

→ Depuis la version **Coswin 8i.9**, ce module dispose d'une fonction **renommage**.

3.4.3. Superviseurs

Emplacement :  Maintenance > Ressources > Superviseurs

3.4.3.1. Inventaire des données et des traitements

Il n'est pas nécessaire de consigner des données personnelles sur ce module.
En revanche, cette information permet d'identifier la personne :

- Description



Remarque

La description du superviseur peut se limiter à sa fonction (responsable des services techniques, responsable du secteur X, etc.).

3.4.3.2. Conservation des données

Les informations liées à cet enregistrement doivent être **supprimées ou anonymisées** une fois que la relation contractuelle est terminée.

- Suppression des informations (données personnelles) associées à l'enregistrement.
- Pseudonymisation — au besoin — du code de l'enregistrement avec l'option **IOD**.



Aller plus loin

Chapitre  Conservation des données ^[p.39].

Nouveauté 8i.9

→ Depuis la version **Coswin 8i.9**, ce module dispose d'une fonction **renommage**.

3.4.4. Contacts

Emplacement :  Communs > Contacts

3.4.4.1. Inventaire des données et des traitements

Il n'est pas nécessaire de consigner des données personnelles sur ce module.
En revanche, des informations permettent d'identifier la personne :

- Description
- Adresse électronique
- Téléphone(s)



💡 Bonne pratique

Les numéros de téléphone, les adresses électroniques consignés doivent être des coordonnées professionnelles.



3.4.4.2. Conservation des données

Les informations liées à cet enregistrement doivent être **supprimées ou anonymisées** une fois que la relation contractuelle est terminée.

- Suppression des informations (données personnelles) associées à l'enregistrement.
- Pseudonymisation — au besoin — du code de l'enregistrement avec l'option **IOD**.



Aller plus loin

Chapitre > Conservation des données ^[p.39].

Lorsque qu'un fournisseur est déréférencé de votre organisation, vous devez supprimer les contacts qui lui sont rattachés.

Si vous avez demandé le consentement au contact et que celui-ci l'a refusé ou n'a pas répondu

→ Vous devez supprimer les données associées au contact.

Voir chapitre > Gestion du consentement des contacts ^[p.16].

🗨️ Nouveauté 8i.9

→ Depuis la version [Coswin 8i.9](#), ce module dispose d'une fonction **renommage**.

3.4.4.3. Gestion du consentement des contacts

Depuis la version Coswin 8i.8, deux champs relatifs au consentement des contacts ont été mis à disposition dans l'éditeur de ressources.

Consentement	<input checked="" type="checkbox"/> Case à cocher
Date du consentement	

1 Extraction des personnes à contacter

Utilisez les outils d'extraction (export Excel ou rapport) pour dresser la liste des personnes à contacter pour recueillir leur consentement.

2 Menez une campagne de requalification de vos contacts

Profitez de l'occasion pour faire le ménage dans vos contacts !

Précisez la finalité de l'opération :

- Ce que vous ferez de ces informations.
- Ce que vous ne ferez pas.

Exemple de mailing

En conformité avec les articles 6 et 7 du RGPD, XXX requiert votre consentement pour la collecte des informations ci-dessous (merci de les confirmer ou de les rectifier le cas échéant) :

- Société
- Prénom, Nom
- Courriel professionnel
- Téléphone professionnel
- Nature du contact (Commercial / Technique / Autre)

Ces données ont pour seul objectif de **mettre à jour notre référentiel fournisseur**.

XXX s'engage à ne pas communiquer ces informations à un tiers ni les utiliser dans une démarche publicitaire ou commerciale.

À tout moment, vous pouvez retirer votre consentement en contactant YYY.

Je donne mon consentement à l'utilisation de ces données uniquement pour la finalité mentionnée.

3 Mettez à jour Coswin

1. Utilisez les outils (Clic-Clac, mise à jour en masse) pour mettre à jour Coswin.
2. Supprimez les contacts qui ont refusé de donner leur consentement.
3. Maintenez à jour votre liste de contacts en relançant régulièrement cette campagne de requalification.

3.5. Gestion des signatures dans Coswin

Pour des questions de traçabilité, lorsqu'un utilisateur crée une donnée statique ou une transaction, sa signature est consignée sur l'enregistrement.

La signature de l'utilisateur se définit dans le module :

 Outils > Sécurité et profils > Utilisateurs > champ [Signature](#) .

Par défaut, la signature est initialisée avec la description de l'utilisateur.

3.5.1. Signature dans les enregistrements

Important

La modification de cette valeur n'entraîne pas la modification des enregistrements existants.

Seuls les prochains enregistrements seront consignés avec cette nouvelle signature.

Aller plus loin

Chapitre > Liste des champs Coswin anonymisable / pseudonymisable ^[p.36].

Gestion de l'horodatage des commentaires

Les transactions :

- OT
- DI
- Devis

disposent d'un paramètre [Interdire la modification des commentaires déjà saisis](#) qui, s'il est actif, permet d'horodater les commentaires de l'utilisateur. Cette date est préfixée par la signature de l'utilisateur :

#[Cédric] - 31-12-2020 16:30:08
 Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc mattis interdum odio ut accumsan. Proin lectus velit, suscipit vitae eleifend eget, luctus vitae lorem. Aliquam erat volutpat. Integer diam sem, porttitor id tristique nec, aliquam id ex. Pellentesque leo felis, porttitor et semper sed, pretium ut massa. Proin enim metus, vestibulum sit amet tristique quis, tempus nec lacus. Integer ac scelerisque lectus. Aliquam vitae elit lorem.

Signature / Description de l'utilisateur

Depuis la version 8i.8, deux paramètres permettent de préciser la nature de cette information :

Utiliser la description de l'utilisateur dans les commentaires de l'OT

- La signature de l'utilisateur sera utilisée dans les commentaires de l'OT.
- La description de l'utilisateur sera utilisée dans les commentaires de l'OT (si elle existe, sinon c'est la signature de l'utilisateur).

Utiliser la description de l'utilisateur dans le problème de la DI

- La signature de l'utilisateur sera utilisée dans le problème de la DI.
- La description de l'utilisateur sera utilisée dans le problème de la DI (si elle existe, sinon c'est la signature de l'utilisateur).

Suppression de la signature des commentaires à l'archivage des OT et des DI

Depuis la version [Coswin 8i.9](#), la signature du champ commentaire de l'OT et du champ problème de la DI est encadrée par les signes `# [et]`.

Deux paramètres permettent, lors de l'archivage de ces transactions de supprimer cette signature :

Supprimer la signature de l'utilisateur (ou sa description) des commentaires lors de l'archivage

- La signature de l'utilisateur est conservée dans l'horodate des commentaires de l'OT lors de l'archivage

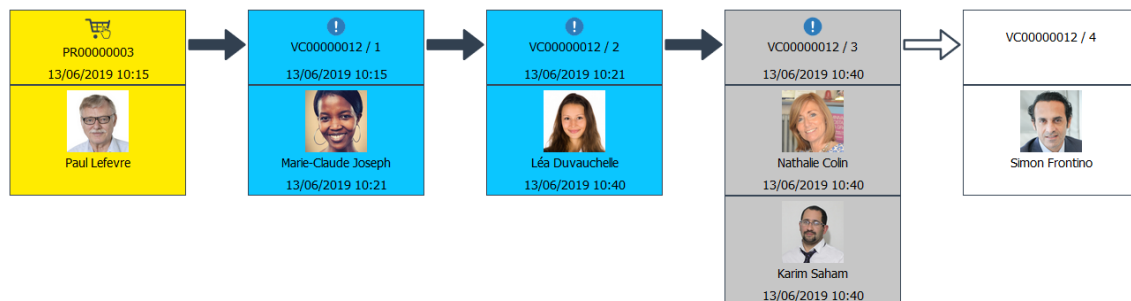
- La signature de l'utilisateur est effacée de l'horodate des commentaires de l'OT lors de l'archivage.

Supprimer la signature de l'utilisateur (ou sa description) du problème lors de l'archivage

- La signature de l'utilisateur est conservée dans l'horodate du problème de la DI lors de l'archivage.
- La signature de l'utilisateur est effacée de l'horodate du problème de la DI lors de l'archivage.

3.5.2. Signature dans l'historique des circuits de validation

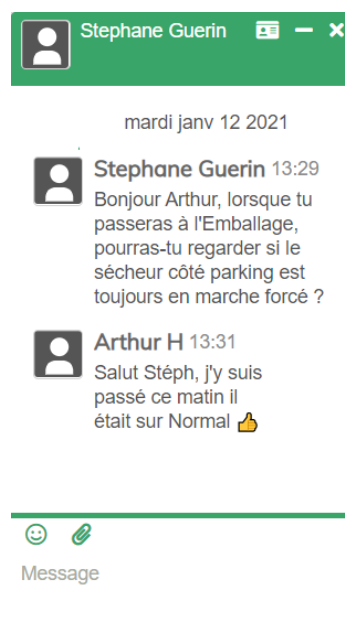
La signature est également prise en compte au niveau de l'historique des circuits de validation. Ce diagramme est généré *à la volée*. Par conséquent, la signature de la personne ayant été notifiée, ayant validé ou refusé l'étape, est celle en vigueur au moment où l'on affiche ce diagramme (et non pas la signature telle qu'elle existait au moment où l'étape a été traitée).



3.6. Messagerie instantanée

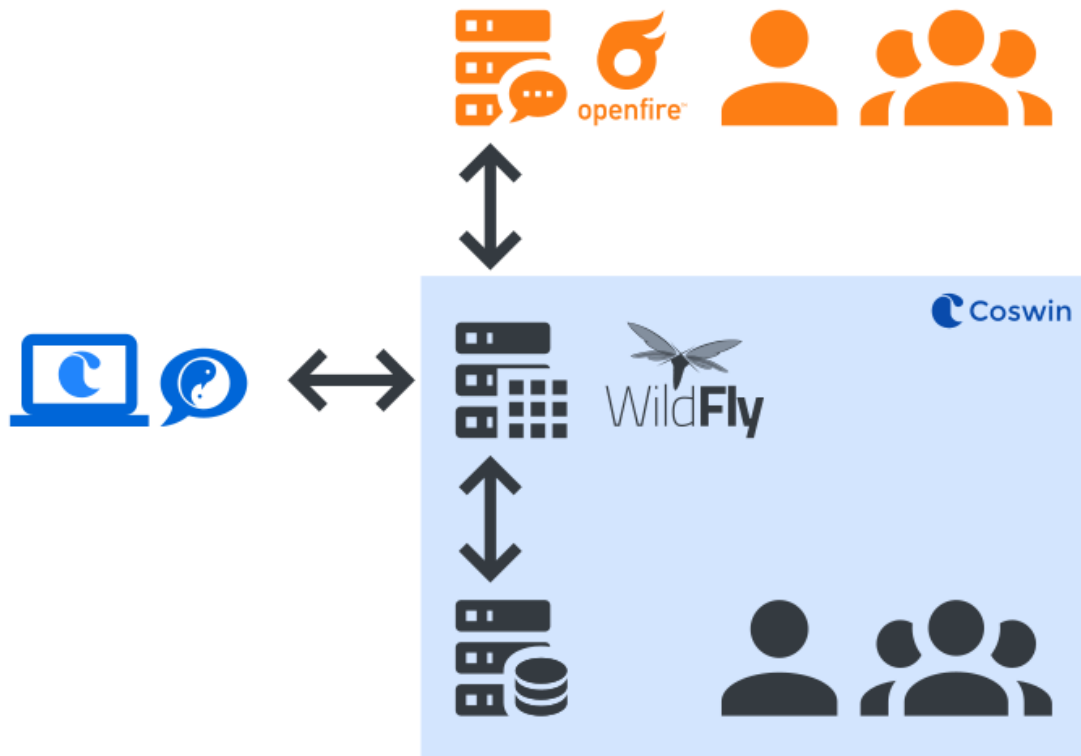
Nouveauté 8i.9

→ Depuis la version [Coswin 8i.9](#), les utilisateurs peuvent converser au travers une messagerie instantanée lorsqu'ils sont connectés à Coswin.



3.6.1. Gestion des utilisateurs sur le serveur de messagerie instantanée

- Les utilisateurs Coswin et les groupes de messagerie sont dupliqués sur la base de données du serveur de messagerie (Openfire – externe à Coswin).
- Des processus automatiques et manuels permettent de synchroniser – sur le serveur de messagerie – ces référentiels (code, description, entité et avatar).
- Lorsqu'un utilisateur Coswin est désactivé ou supprimé de Coswin, il est automatiquement supprimé de la base de données du serveur de messagerie.



3.6.2. Conservation des données

- Les messages (chat et diffusion de message interne) ne font que transiter sur le serveur de messagerie.
- Dès que le destinataire accède au message, celui-ci est supprimé du serveur de messagerie.
- Le fil de discussion est conservé dans le [WebStorage](#) du navigateur (de façon persistante [localStorage](#)).

3.7. Enregistrements avec données personnelles directes - Employé



Emplacement : [Outils > Sécurité et profils > Utilisateurs](#)

C'est sur le module employé que des données personnelles peuvent être consignées.

Il faudra :

- Procéder à leur inventaire.
- Justifier de leur pertinence.
- Déterminer et mettre en œuvre les actions qui visent à minimiser ces données.

3.7.1. Inventaire des données et des traitements

Nom de la colonne	Étiquette	Position
REEM_DESCRIPTION	Description de l'employé	Entête
REEM_BAR_CODE	Code à barres	Onglet  Détails
REEM_EMAIL	Courriel	
REEM_EMERGENCY_CONTACT	Contact d'urgence	
REEM_FAX	Fax	
REEM_PHONE	Téléphone	
REEM_ADR_TO_GEOLOC	Adresse de géolocalisation (1)	Onglet  Identité
REEM_LATITUDE	Latitude (1)	
REEM_LONGITUDE	Longitude (1)	
REEM_SEX	Sexe (2)	
REEM_PIN	Code confidentiel	
REEM_WORKER_ID	N° de l'employé	

Seuls les champs **Description de l'employé** et **Sexe** sont obligatoires.

Les autres champs sont facultatifs au fonctionnement de Coswin.

Nouveauté 8i.9

→ Depuis la version [Coswin 8i.9](#), il est possible de chiffrer les [champs en bleu](#) (voir chapitre [Les 3 principes de la sécurité \(cf. Sécurité de l'application Coswin\)](#) ^[p.29]).

Bonne pratique

Les numéros de téléphone, les adresses électroniques consignés doivent être des coordonnées professionnelles.



(1) voir chapitre [Gestion de la géolocalisation des personnes dans Coswin](#) ^[p.24].

Nouveauté 8i.9

(2) Gestion du champ [sexe](#)

À partir de la version Coswin 8i.9, le radio-box **Sexe** (qui ne prenait auparavant que deux valeurs Masculin / Féminin) est remplacé par une liste de choix proposant les valeurs :

- Non renseigné
- Masculin
- Féminin
- Neutre

En création employé, ce champ est par défaut initialisé à **Non renseigné**.

Le module **Qualifications** recense les :

- Compétences
- Habilitations
- Certificats
- etc.



de l'employé nécessaires à la bonne exécution des travaux.

Cette information, utile dans le processus d'affectation du travail et pour des raisons légales, peut être conservée dans le temps.

3.7.2. Conservation des données

La durée de conservation de ces informations peut faire l'objet d'une obligation légale.

Exemple

Pour des questions de **traçabilité du cycle de vie** de certains équipements, vous devez être en mesure de prouver que les opérations de maintenance ont été effectuées dans les règles de l'art et par un intervenant qualifié (habilitation, niveau de compétence, etc.).

3.7.3. Calendrier de l'employé

Le calendrier de l'employé a pour finalité de connaître la disponibilité de l'employé.

Les absences de l'employé (congrés, heure ou jour d'absence) doivent donc être consignées dans son calendrier pour permettre une planification et une affectation du travail.

3.7.3.1. Contenu du calendrier de l'employé

Raisons d'absence

Coswin a besoin de savoir si une personne est disponible ou pas.

La raison de l'indisponibilité n'est par conséquent qu'un critère d'utilisation.

Bonne pratique

Assurez-vous de spécifier des raisons d'absence qui ne soient pas considérées comme des données sensibles au sens de la loi.

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

■ <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20110224>

Déconseillé	Préférable
Délégation syndicale	Indisponible
Grève	
Examen médical	

Les raisons d'absence se définissent dans :

🔗 Outils > Paramètres > Maintenance > Contrôle calendrier bouton Raison de l'absence .

3.7.3.2. Conservation des données du calendrier

Chaque année, le processus de **contrôle des calendriers** doit être lancé pour supprimer les anciennes données (dont celles relatives aux employés) qui n'ont pas vocation à être conservées.

→ L'objectif du calendrier étant de connaître la disponibilité des personnes pour les travaux en cours et à venir.

💡 Bonnes pratiques

Nous vous conseillons de travailler par période glissante, par exemple sur 3 années, avec :

- année -1
- année courante
- année +1

Le contrôle calendrier est à lancer à chaque début d'année.

Glissement des périodes du contrôle calendrier



Aller plus loin

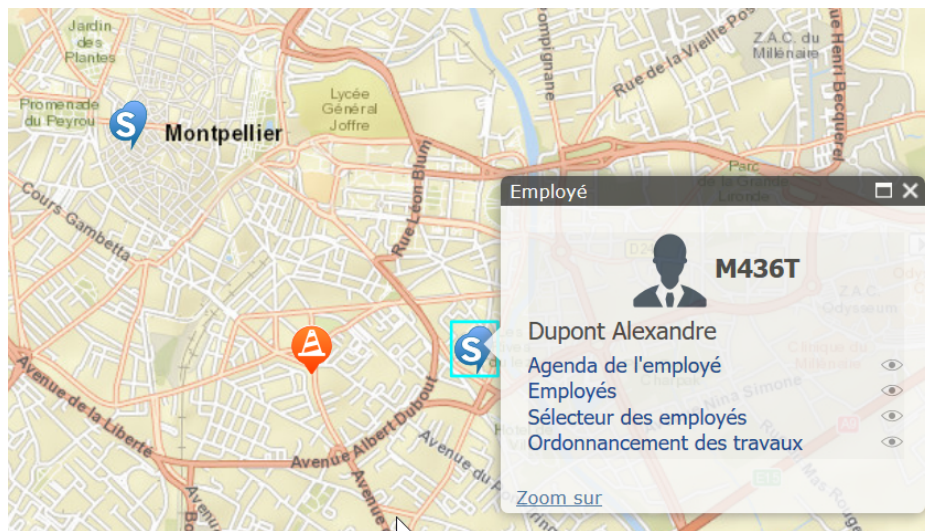
Chapitre > Conservation des données ^[p.39].

3.7.4. Gestion de la géolocalisation des personnes dans Coswin

L'objectif de la géolocalisation de l'employé est de connaître son emplacement pour pouvoir lui affecter du travail.

1. Pour des facilités d'usage.
2. Pour des questions de sécurité (travailleur isolé par exemple).

Exemple



Pour affecter le travail sur l'OT  à un employé , il est intéressant de connaître la position des employés à proximité pour choisir la bonne personne.

Mise à jour de la position de l'employé

Le positionnement de l'employé sur la carte se fait :

- Manuellement sur la carte par la personne en charge de l'affectation des travaux
- Automatiquement via le Coswin Nom@d

Mise à jour de la position via Coswin Nom@d

La mise à jour de la position requiert toujours le **consentement** de l'utilisateur.

L'administrateur doit en premier lieu indiquer si l'utilisateur Nom@d peut être ou non géolocalisé.

[Outils](#) > [Sécurité et profils](#) > [Utilisateurs](#) > Onglet [Détails](#) > Section [Coswin Nom@d](#)

Case à cocher Géolocalisable

- L'utilisateur n'est pas géolocalisable.
- L'utilisateur est géolocalisable sur Coswin Nom@d.

Dans le cas où l'option est cochée, à l'ouverture de la session sur le terminal Coswin Nom@d, une question sera posée à l'utilisateur :

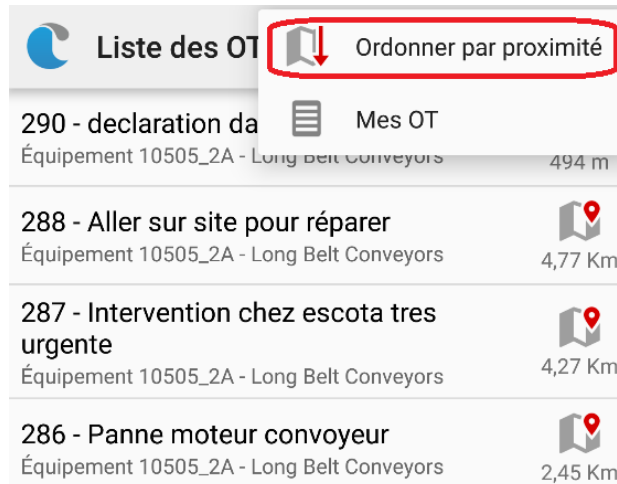
[Voulez-vous être géolocalisé ?](#)

Non sa position ne sera pas envoyée à Coswin

Oui sa position sera **envoyée à Coswin** et réactualisée dès que les données seront transférées

Remarque

En cas de non géolocalisation, l'utilisateur Nom@d peut connaître la position des équipements et des travaux à proximité.



En revanche la position de l'employé n'est **jamais** envoyée à Coswin.

⚠ Important - Pas de tracking

Lorsque la nouvelle position de l'employé est envoyée à Coswin, celle-ci écrase sa dernière position (et sa date heure associée).

Il n'est pas possible de visualiser l'itinéraire emprunté par l'employé.

3.8. Données pour l'administration de Coswin

Coswin dispose d'outils permettant son administration.

Ces outils peuvent avoir accès à des données personnelles, aussi il convient de limiter leur usage uniquement aux administrateurs de la GMAO :

- Éditeur de rapports [p.25]
- Console d'administration [p.26]
- Audit trail [p.26]

3.8.1. Éditeur de rapports

L' [éditeur de rapports](#) permet à l'administrateur GMAO de créer des états sur la base de données.

Il s'agit d'une application indépendante de Coswin qui se connecte directement à la base de données.



→ Il s'agit donc d'une application critique dont il convient de limiter l'accès aux seules personnes habilitées.



Bonne pratique

Une option permet d'afficher dans les info-bulles des champs des informations techniques sur les champs (nom de la table et de la colonne par exemple).

Il ne faut activer cette option que sur les groupes d'utilisateurs étant habilités à en avoir l'usage.

Emplacement :  Outils > Sécurité et profils > Groupes > onglet  Détails, champ [info-bulle](#).

3.8.2. Console d'administration

La [console d'administration](#) permet à l'administrateur GMAO de visualiser :

- Les connexions en cours
- L'historique des connexions concurrentes
- **L'historique des connexions utilisateurs**



→ L'affichage graphique permet de visualiser jusqu'à un an de connexion.

Nouveauté 8i.9

→ Depuis la version [Coswin 8i.9](#), une fonction vous permet de supprimer une partie de l'historique des connexions jusqu'à une date donnée.

3.8.3. Audit trail

L' [audit trail](#) permet à l'administrateur GMAO de visualiser — sur les modules où il est activé — le cycle de vie des enregistrements :

- Qui a créé l'enregistrement ?
- Qui a modifié quoi sur l'enregistrement ?



→ L'audit trail étant activé pour des raisons de traçabilité, ces données n'ont pas vocation à être supprimées.

Cependant Coswin permet de supprimer ces données jusqu'à une date spécifiée par l'administrateur.

4. Droits des personnes concernées

Informez les personnes

A chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des **mentions d'information**.

Vérifiez que l'information comporte les éléments suivants :

- Pourquoi vous collectez les données « la finalité ».
- Ce qui vous autorise à traiter ces données « fondement juridique ».
- Qui a accès aux données (indiquez des catégories : les services internes compétents, un prestataire, etc.).
- Combien de temps vous les conservez (exemple : « 5 ans après la fin de la relation contractuelle »).
- Les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits.
- Si vous transférez des données hors de l'UE : précisez le pays et l'encadrement juridique qui maintient le niveau de protection des données.



→ À l'issue de cette étape, vous avez répondu à votre **obligation de transparence**.

Permettez aux personnes d'exercer facilement leurs droits

- Les personnes dont vous traitez les données (clients, collaborateurs, prestataires, etc.) ont des droits sur leurs données, qui sont d'ailleurs renforcés par le RGPD : droit d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation du traitement.
- Mettez en place un processus interne permettant de garantir l'identification et le traitement des demandes dans des délais courts (**1 mois au maximum**).



Aller plus loin

Chapitre [Évaluation des mesures protectrices des droits des personnes concernées](#) [p.40].

4.1. Consentement de l'utilisateur

Introduction

Depuis la version Coswin 8i.8, trois champs relatifs au consentement des utilisateurs ont été mis à disposition dans l'éditeur de ressources.


Consentement requis	<input checked="" type="checkbox"/> Case à cocher
Consentement	<input checked="" type="checkbox"/> Case à cocher
Date du consentement	


Si la case à cocher **Consentement requis** est cochée et la case à cocher **Consentement** décochée, à la prochaine connexion à Coswin, l'utilisateur devra lire les termes ci-dessous et les accepter pour pouvoir accéder à Coswin.

Si l'utilisateur accepte, la case à cocher **Consentement** sera cochée et la **Date du consentement** indiquera la date à la laquelle le consentement a été donné.

Bonne pratique

Informez régulièrement vos utilisateurs (au moins une fois par an).

Dans  Outils > Paramètres > Général > Paramètres généraux > **Intervalle de rappel du consentement RGPD (en mois)**, indiquez le nombre de mois entre deux demandes de consentement.

Si vous modifiez vos traitements et/ou si vous personnalisez le contenu du fichier **gdpr_fr_FR.html** (dans le WebDAV interne  /coswin-repository/content/default/login), vous devrez obtenir le consentement des utilisateurs.

4.1.1. Message à la connexion

RGPD

L'accès à l'application Coswin requiert que l'utilisateur soit authentifié.

Cette authentification est associée à des éléments qui permettent d'identifier l'utilisateur :

- Directement (nom, prénom)
- Indirectement (matricule, courriel professionnel, téléphone professionnel)

Le cas échéant, d'autres données personnelles peuvent être consignées dans Coswin (agenda professionnel, qualifications professionnelles, position GPS, contact d'urgence).

Le détail de ces informations est disponible auprès du responsable de traitement de votre organisation.

La finalité des traitements de ces données est limitée à un usage professionnel dans Coswin pour l'accomplissement et le suivi des tâches associées à l'exploitation du logiciel dans la gestion de la maintenance, du stock et des achats :

- Identification des personnes connectées.
- Identification des personnes qui créent et modifient des enregistrements.
- Identification de la disponibilité des employés en vue de l'affectation de travaux.
- Identification des qualifications des employés en vue de l'affectation de travaux.
- Identification de la position des employés en vue de l'affectation de travaux.

Aucune donnée sensible (définie dans l'article 9-1 du RGPD) n'est utilisée dans Coswin.

Aucune donnée personnelle ne sera communiquée à un tiers ni utilisée dans une démarche publicitaire ou commerciale.

Vous bénéficiez d'un droit de retrait du consentement.

Plus d'information sur <https://www.siveco.com/fr/infoprod>

Termes inappropriés

L'utilisateur Coswin s'engage à ne pas utiliser des termes inappropriés dans les champs de Coswin, notamment les commentaires.

Termes inappropriés peuvent être des mots perçus comme sexistes, racistes ou injurieux.

En cliquant *Accepter*, je donne mon consentement à l'utilisation de ces données.

5. Sécurisation des données

Le RGPD traite des risques liés à la sécurité des données en relation avec les personnes. Vous devez évaluer ce risque (gravité et vraisemblance) et adopter les mesures pour minimiser ce risque au maximum.

Exemple de risque

Les techniciens de votre organisation sont amenés à intervenir chez des particuliers. Vous avez consigné dans Coswin les codes d'accès des digicodes permettant l'accès aux immeubles de ces particuliers.

→ Vous devrez envisager un scénario hypothétique où ces informations se retrouveraient "dans la nature", évaluer les conséquences que cet incident représenterait et prendre les dispositions pour éviter que cet incident ne survienne (de façon accidentelle ou malintentionnée).

Aller plus loin

Chapitre > Appréciation des risques : les atteintes potentielles à la vie privée [p.40].

Les mesures à prendre

Vous devez mettre en place les mesures de sécurité :

- Au niveau de l'application Coswin.
- Au niveau de la plate-forme Coswin.

5.1. Sécurité de l'application Coswin

Les 3 principes de la sécurité

Le principe de **confidentialité** : les données personnelles ne doivent être accessibles qu'aux personnes autorisées.

Le principe d'**intégrité** : les données personnelles ne doivent pas être altérées ou modifiées.

Le principe de **disponibilité** : les données personnelles doivent être en permanence accessibles par les personnes autorisées.

→ Il s'agit d'un processus continu. Les mesures doivent être régulièrement ajustées en fonction de l'évolution du risque.



3

Coswin permet de répondre à ces obligations à différents niveaux :

- L'accès au module.
- L'accès à des champs du module.
- L'accès à certains enregistrements du module.
- La possibilité de chiffrer les champs du module employé qui contiennent des données personnelles

L'accès au module

Les accès aux modules se définissent au niveau des droits des groupes d'utilisateurs (l'utilisateur hérite de la somme des droits des groupes auxquels il est rattaché).

Emplacement :  Outils > Sécurité et profils > Groupes > onglet  Droits



→ Si vous ne jugez pas nécessaire qu'un profil d'utilisateurs ait accès aux informations d'un module, retirez-lui l'accès à ce module.

Bonnes pratiques

- Restreindre l'accès à un module (par exemple la fiche Employé) n'empêche pas de pouvoir sélectionner un enregistrement de ce module depuis un autre module.
→ La sélection de cet enregistrement pouvant se faire via un sélecteur, pensez à ne pas afficher les données personnelles dans ce sélecteur.
- Pensez également qu'il est possible pour l'utilisateur d'**exporter** le contenu d'un sélecteur dans un fichier **Excel** ou d'**imprimer** un rapport qui retournerait des données personnelles de ces enregistrements.
→ Vous pouvez retirer pour ces modules le droit **Imprimer** (qui permet l'impression **et** l'exportation vers Excel).

L'accès à des champs du module

L'**éditeur de ressources** vous permet de masquer l'accès à des champs (ou des onglets) d'un écran :

- **Systématique** (ex. le champ n'est jamais visible / accessible).
- **Conditionnel** (ex. le champ n'est visible / accessible que si la condition est remplie).



L'accès à certains enregistrements du module

L'accès aux enregistrements peut se restreindre avec :

- Les accès aux données
- Les filtres administrateurs



Nouveauté 8i.9

→ Depuis la version **Coswin 8i.9**, il est possible de chiffrer les champs de la **fiche employé** contenant des données personnelles.

Chiffrement possible des champs suivants :

- REEM_EMAIL (Courriel)
- REEM_EMERGENCY_CONTACT (Contact d'urgence)
- REEM_FAX (Fax)
- REEM_PHONE (Téléphone)
- REEM_PIN (Code confidentiel)
- REEM_WORKER_ID (N° de l'employé)



La donnée chiffrée est visible uniquement si la base de données accède à la clé de cryptage.

Sans accès à cette clé – unique par base de données – le contenu des champs n'est pas exploitable :

	REEM_EMAIL	REEM_EMERGENCY_CONTACT
1	07DABAD3BF4C000C1204CE34386B42D9	0BD42575EB573FDA56255394B3CC083B0FD045D25C3305FB6A3A7CBED2B84071

5.2. Sécurité de la plate-forme Coswin

Gestion des utilisateurs

Mettez en place des protocoles pour vous assurer que :

- Lorsqu'un utilisateur quitte votre organisation, son compte utilisateur soit supprimé.
- Lorsqu'un utilisateur change de fonction / de service, ses droits en relation avec des modules traitant de données personnelles soient mis à jour en conséquence.



À savoir


Le processus d'anonymisation des utilisateurs de Coswin ne traite que des enregistrements de la base de données.

- La **signature** de l'utilisateur apparaît dans les journaux d'impression (fichiers `coswin-print.log` et `coswin-print.aaaa-mm-jj hh`)
- Emplacement `/wildfly-18.0.0.Final/standalone/log`
- Ce document indique :
 - La signature de l'utilisateur qui a imprimé le rapport.
 - Le nom du rapport.
 - La date d'impression.

→ Si l'administrateur souhaite faire disparaître la signature d'un utilisateur de ces fichiers, il devra le faire manuellement avec un éditeur de texte (fonction chercher / remplacer).

Mot de passe robuste

Mettez en place une politique de mot de passe robuste. L'utilisateur est authentifié :



- Soit au travers d'un annuaire LDAP
 - C'est au gestionnaire de l'annuaire de mettre en place cette politique
- Soit au niveau de la base de données *
 - Sur la version Oracle de Coswin, emplacement :  Outils > Sécurité et profils > Profils vous pouvez activer la gestion des profils permettant d'utiliser les options de gestion des mots de passe Oracle (voir guide de l'utilisateur en ligne).



* L'algorithme de cryptage du mot de passe dépend de la version du SGBDR :

Base de données		Algorithme
Oracle	10g	DES
	11g	SHA-1
	12c et supérieur	SHA-512
SQL Server	2012 et supérieur	SHA-512
PostgreSQL	10	MD5

Bonne pratique

- Sensibilisez les utilisateurs à prendre l'habitude de verrouiller leur poste de travail lorsqu'ils quittent leur session de travail.
- Activez le contrôle du temps d'inactivité
 - Emplacement :  Outils > Sécurité et profils > Groupes > Onglet  Détails :
 - Cocher la case Compter le temps d'inactivité .

Mise à jour de Coswin

Les mises à jour de Coswin garantissent l'intégrité de la solution.

- Utilisez les versions récentes de Coswin.
- Installez les patches cumulatifs.

Maintenez à jour les composants (base de données, serveur d'applications, serveur d'impression) de la plate-forme Coswin :

- Patch de sécurité du système d'exploitation des composants.
- Patch de sécurité de la base de données.



6. Annexe

6.1. Définitions (complément)

CNIL - Commission Nationale de l'Informatique et des Libertés

La Commission Nationale de l'Informatique et des Libertés est le régulateur des données personnelles en France. Elle accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits.











CEPD - Comité européen de la protection des données

Le Comité européen de la protection des données (ou EDPB - European Data Protection Board) coordonne l'action des commissions en charge de l'application du RGPD de l'ensemble des États membres de l'UE au moyen d'avis et de décisions.



Il conseille la Commission Européenne sur des questions relatives au RGPD.

Liste des membres du CEPD

Pays		Comité	Site web
	Austria	Österreichische Datenschutzbehörde	http://www.dsb.gv.at/
	Belgium	Autorité de la protection des données (APD-GBA)	https://www.autoriteprotectiondonnees.be/
	Bulgaria	Commission for Personal Data Protection	https://www.cpdp.bg/
	Croatia	Croatian Personal Data Protection Agency	https://azop.hr/
	Cyprus	Commissioner for Personal Data Protection	http://www.dataprotection.gov.cy/
	Czech Republic	Office for Personal Data Protection	http://www.uouu.cz/
	Denmark	Datatilsynet	http://www.datatilsynet.dk/
	Estonia	Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)	http://www.aki.ee/

	UE	European Data Protection Supervisor	http://www.edps.europa.eu/EDPSWEB/
	Finland	Office of the Data Protection Ombudsman	https://tietosuoja.fi/etusivu/
	France	Commission Nationale de l'Informatique et des Libertés - CNIL	http://www.cnil.fr/
	Germany	Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	http://www.bfdi.bund.de/
	Greece	Hellenic Data Protection Authority	http://www.dpa.gr/
	Hungary	Hungarian National Authority for Data Protection and Freedom of Information	http://www.naih.hu/
	Ireland	Data Protection Commission	http://www.dataprotection.ie/
	Italy	Garante per la protezione dei dati personali	http://www.garanteprivacy.it/
	Latvia	Data State Inspectorate	http://www.dvi.gov.lv/
	Lithuania	State Data Protection Inspectorate	http://www.ada.lt/
	Luxembourg	Commission Nationale pour la Protection des Données	http://www.cnpd.lu/
	Malta	Office of the Information and Data Protection Commissioner	http://www.idpc.org.mt/
	Netherlands	Autoriteit Persoonsgegevens	https://autoriteitpersoonsgegevens.nl/nl
	Poland	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	https://uodo.gov.pl/
	Portugal	Comissão Nacional de Protecção de Dados - CNPD	https://www.cnpd.pt/
	Romania	The National Supervisory Authority for Personal Data Processing	http://www.dataprotection.ro/
	Slovakia	Office for Personal Data Protection of the Slovak Republic	http://www.dataprotection.gov.sk/
	Slovenia	Information Commissioner of the Republic of Slovenia	https://www.ip-rs.si/
	Spain	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es/
	Sweden	Datainspektionen	https://www.datainspektionen.se/
	United Kingdom	The Information Commissioner's Office	https://ico.org.uk

6.2. Les 8 règles d'or

Licéité du traitement

Un traitement ne peut être mis en œuvre que s'il est **fondé sur une des 6 conditions de licéité** :

1. La personne concernée a **consenti au traitement de ses données à caractère personnel** pour une ou plusieurs finalités spécifiques.

2. Le traitement est nécessaire à l'**exécution d'un contrat** auquel la personne concernée est partie ou à l'exécution de mesures pré-contractuelles prises à la demande de celle-ci.
3. Le traitement est nécessaire au **respect d'une obligation légale** à laquelle le responsable du traitement est soumis.
4. Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.
5. Le traitement est nécessaire à l'**exécution d'une mission d'intérêt public** ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.
6. Le traitement est nécessaire aux fins des **intérêts légitimes** poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Finalité du traitement

Les données personnelles collectées ne peuvent être **traitées que pour une finalité définie précisément et légitime**.

Minimisation des données

Seules les **données strictement nécessaires pour atteindre la finalité** peuvent être collectées et traitées.

Protection particulière des données sensibles

Les données sensibles ne peuvent être **collectées et traitées que dans certaines conditions**.

Conservation limitée des données

Les données doivent être **archivées, supprimées ou anonymisées** dès que la finalité pour laquelle elles ont été collectées est atteinte.

Obligation de sécurité

Au regard des risques, **des mesures** doivent être mises en œuvre pour **s'assurer de la sécurité des données traitées**.

Transparence

Les personnes doivent être **informées de l'utilisation des données les concernant et de la manière d'exercer leurs droits**.

Droits des personnes

Les personnes bénéficient de **nombreux droits qui leur permettent de garder la maîtrise de leurs données**.

6.3. Données sensibles

Le traitement des données sensibles est strictement encadré par la loi.

6.3.1. Définition

RGPD - Article 9-1

Tout traitement, comme la collecte ou la consultation, de données dites **sensibles** **est par principe interdit** par le RGPD puisque ces données sont relatives à l'intimité de la vie privée.

Les données sensibles sont celles qui relèvent ou concernent :

- Les origines raciales ou ethniques.
- Les opinions politiques.
- Les convictions philosophiques ou religieuses.
- L'appartenance syndicale.
- La santé (physique ou mentale).
- La vie sexuelle ou orientation sexuelle.
- Les origines génétiques.
- Les données biométriques aux fins d'identifier une personne physique de manière unique.

6.3.2. Exceptions

RGPD - Article 9-2

Il existe cependant des exceptions à ce principe d'interdiction, qui permettent le traitement de ces données lorsqu'elles sont :

- Fournies par la personne concernée avec son **consentement explicite**.
- Nécessaires à l'**exécution des obligations** en droits du travail et social (ex : déclaration des accidents du travail).
- Nécessaires à la **sauvegarde des intérêts vitaux de la personne**.
- Traitées pour la gestion des membres d'un **organisme à but non lucratif** (politique, philosophique, religieux ou syndical).
- **Manifestement rendues publiques** par la personne concernée (ex : opinions politiques d'un élu).
- Nécessaires à la **constatation, à l'exercice ou de la défense d'un droit en justice**.
- Nécessaires pour des **motifs d'intérêts public importants**.
- Nécessaires pour des **fins médicales** (médecine préventive, diagnostics médicaux, gestion des services de santé, etc.).
- Nécessaires pour des **motifs d'intérêts public dans le domaine de la santé publique**.
- Nécessaires à des **fins d'archives dans l'intérêt public et de recherche scientifique** (ex : recherche médicale) **ou historique ou à des fins statistiques** sous réserve de garanties.

6.4. Liste des champs Coswin anonymisable / pseudonymisable

Liste des champs Créateur

Module	Table	Colonne
Agréments	AGREEMENT	AGAG_CREATOR

Agréments en historique	H_AGREEMENT	HAGAG_CREATOR
Ajustements	ADJUSTMENT	ADAD_CREATOR
Ajustements en historique	H_ADJUSTMENT	HADAD_CREATOR
Amortissements	DEPRECIATION	EFDP_CREATOR
Arrivages	RECEIPT	RCRC_CREATOR
Arrivages en historique	H_RECEIPT	HRCRC_CREATOR
Atelier	WORKSHOP	WSWS_CREATOR
Avenants de la commande	ADDITIONAL_CLAUSE	POAC_CREATOR
Avenants de la commande en historique	H_ADDITIONAL_CLAUSE	HPOAC_CREATOR
Avis de mouvement	TRANSPORT_NOTICE	TNTN_CREATOR
Avoirs	CREDIT	CNCR_CREATOR
Avoirs en historique	H_CREDIT	HCNCR_CREATOR
Bons de sortie de transport (BST)	TRANSPORT_OUTPUT_FORM	TNOF_CREATOR
Cartes	MAPLAYERS	CWML_CREATOR
Cartes du secteur d'intervention	WORKING_AREA_MAPLAYERS	CWWM_CREATOR
Certifications	CERTIFICATION	PDCE_CREATOR
Circuits de validation	VALIDATION_CIRCUIT	WFVC_CREATOR
Circuits des états des demandes d'intervention	JR_STATUS_CIRCUIT	JRSC_CREATOR
Circuits des états OT	WO_STATUS_CIRCUIT	WOSC_CREATOR
Clauses du contrat	CONTRACT_CLAUSE	ERCC_CREATOR
Colis de l'ordre de transit en historique	H_PACKAGE	HPPPA_CREATOR
Commandes	ORDER_	POPO_CREATOR
Commandes en historique	H_ORDER	HPOPO_CREATOR
Configurations de liste	FS_CONFIG	FSIC_CREATOR
Couches de carte	MAP_REF_SERVICES	CWMS_CREATOR
Définitions de graphiques	GRAPH_CONFIG	GRCO_CREATOR
Demandes d'achat	REQUEST	PRPR_CREATOR
Demandes d'achat en historique	H_REQUEST	HPRPR_CREATOR
Demandes de prix	QUOTATION	PQPQ_CREATOR
Demandes de prix en historique	H_QUOTATION	HPQPQ_CREATOR
Demandes d'intervention en cours	JOB_REQUEST	JRJR_CREATOR
Demandes d'intervention en historique	H_JOB_REQUEST	HJRJR_CREATOR
Devis	ESTIMATE	ESES_CREATOR
Enregistrements factures	INVOICE	PIPI_CREATOR

EPI affectés aux employés	EMPLOYEE_SAFETY	REEF_CREATOR
Factures du devis	ESTIMATE_BILL	ESBI_CREATOR
Factures en historique	H_INVOICE	HPIPI_CREATOR
Factures OT	BILL_WORK_ORDER	BIWO_CREATOR
Fichiers liés	LINKED_FILES	CWLF_CREATOR
Historique des calculs de disponibilité stock	PLAN_AVAILABILITY	PLAV_CREATOR
Historique des taux de change	CURRENCY_HISTORY	PDCH_CREATOR
Intersection entre la section de la page d'accueil et les indicateurs	SECTION_INDICATOR	CWSI_CREATOR
Intersection entre les cartes et les couches de carte	MAPLAYERS_REF_SERVICE	CWMR_CREATOR
Interventions	JOB	MDJB_CREATOR
Inventaires	COUNT	SCSC_CREATOR
Inventaires en historique	H_COUNT	HSCSC_CREATOR
Jeux de conditions	WORKFLOW_CONDITION_SET	WFCS_CREATOR
Mises à jour de l'état de l'équipement	STATUS_UPDATE	ERSU_CREATOR
Modèles d'EPI de la ressource	RESOURCE_MODEL	REMO_CREATOR
Modèles d'EPI de l'employé	EMPLOYEE_MODEL	REEO_CREATOR
Modifications des prix de l'article chez le fournisseur	PRICE_MODIFICATION	PSPM_CREATOR
Notifications des travaux	WORK_NOTIFICATION	NNWN_CREATOR
Ordres de transit	TRANSIT_ORDER	PPTO_CREATOR
Ordres de travail	WORK_ORDER	WOWO_CREATOR
Ordres de travail en historique	H_WORK_ORDER	HWOWO_CREATOR
Pages d'accueil	WELCOME_PAGE	CWWP_CREATOR
Pages d'accueil par groupe d'utilisateurs	GROUP_PAGE	CWGP_CREATOR
Permis de travail	WORK_PERMIT	WPWP_CREATOR
Procès verbaux d'étalonnage	CALIBRATION_REPORT	CACR_CREATOR
Projets	PROJECT	PLPO_CREATOR
Projets BIMServer	BIM_SERVER_PROJECT	BMSP_CREATOR
Réconciliations de factures	RECONCILE	PIRE_CREATOR
Réconciliations des factures en historique	H_RECONCILE	HPIRE_CREATOR
Reconductions du contrat	CONTRACT_EXTENSION	EREX_CREATOR
Réservations	DEMAND	DMDM_CREATOR
Réservations en historique	H_DEMAND	HDMDM_CREATOR
Secteurs d'intervention	WORKING_AREA	CWWA_CREATOR

Sorties	ISSUE	ISIS_CREATOR
Sorties en historique	H_ISSUE	HISIS_CREATOR
Spécifications d'étalonnage	CALIBRATION	CACA_CREATOR
Suivi des modifications de l'amortissement	DEPRECIATION_ADD_CLAUSE	EFDA_CREATOR
Transferts	TRANSFER	TRTR_CREATOR
Transferts en historique	H_TRANSFER	HTRTR_CREATOR
Vue des ordres de travail	V_WORK_ORDER	VWOWO_CREATOR

Liste des champs Dern. modification par

Module	Table	Colonne
Projets BIMServer	BIM_SERVER_PROJECT	BMSP_LAST_MODIFIED_BY
Demandes d'intervention en historique	H_JOB_REQUEST	HJRJR_LAST_MODIFIED_BY
Ordres de travail en historique	H_WORK_ORDER	HWOWO_LAST_MODIFIED_BY
Demandes d'intervention en cours	JOB_REQUEST	JRJR_LAST_MODIFIED_BY
Vue des ordres de travail	V_WORK_ORDER	VWOWO_LAST_MODIFIED_BY
Ordres de travail	WORK_ORDER	WOWO_LAST_MODIFIED_BY

Liste des champs Utilisateur (dans l'onglet historique des états de transaction)

Module	Table	Colonne
Historique des états de l'OT en historique	H_WO_HISTORY_STATUS	HWOHS_USER
Historique des états de la DI	JR_HISTORY_STATUS	JRHS_USER
Historique des états de l'OT en cours	WO_HISTORY_STATUS	WOHS_USER
Historique des états du permis de travail	WP_HISTORY_STATUS	WPHS_USER

6.5. Conservation des données

Pour chaque traitement, vous devez déterminer :

- Une durée fixe de conservation
- Ou un critère objectif utilisé pour déterminer cette durée.

Exemple

Le temps de la relation contractuelle.

Lorsque l'organisme a satisfait l'objectif poursuivi par la collecte des données, ces données doivent :

- Être **effacées**.

- Ou faire l'objet d'un **processus d'anonymisation ou de pseudonymisation**.
- Ou être **archivées** sous certaines conditions.

Les questions à vous poser

- Jusqu'à quand ?
- Suis-je soumis à une obligation légale de conserver les données ?
- Si oui, quel est le périmètre exact de l'obligation. Quelles sont les données devant nécessairement être conservées et pour combien de temps ?

Exemple

| Contentieux, recours en justice.

6.6. Évaluation des mesures protectrices des droits des personnes concernées

Méthodologie préconisée par la CNIL

- Identifier ou déterminer, et décrire, les **mesures retenues** (existantes ou prévues) pour respecter les exigences suivantes (nécessitant d'expliquer comment il est prévu de les mettre en œuvre) :
 1. Information des personnes concernées (traitement loyal et transparent).
 2. **Recueil du consentement**, le cas échéant : exprès, démontrable, retirable.
 3. Exercice des **droits d'accès et à la portabilité**.
 4. Exercice des **droits de rectification et d'effacement**.
 5. Exercice des **droits de limitation du traitement et d'opposition**.
 6. **Sous-traitance** : identifiée et contractualisée.
 7. **Transferts** : respect des obligations en matière de transfert de données en dehors de l'Union européenne.
- Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer chaque mesure et sa description, conformément au RGPD.
- Le cas échéant, revoir leur description ou proposer des mesures complémentaires.

6.7. Appréciation des risques : les atteintes potentielles à la vie privée

Qu'est-ce qu'un risque sur la vie privée ? (définition de la CNIL)

Un risque est un scénario hypothétique qui décrit un événement redouté et toutes les menaces qui permettraient qu'il survienne.

Le niveau d'un risque est estimé en termes de gravité et de vraisemblance :

- La **gravité** représente l'ampleur d'un risque. Elle dépend essentiellement du caractère préjudiciable des impacts potentiels.
- La **vraisemblance** traduit la possibilité qu'un risque se réalise. Elle dépend essentiellement des

vulnérabilités des supports face aux menaces et des capacités des sources de risques à les exploiter.

Méthodologie préconisée par la CNIL

- Pour chaque événement redouté (un accès illégitime à des données, une modification non désirée de données, et une disparition de données) :
 1. Déterminer les **impacts** potentiels sur la vie privée des personnes concernées s'ils survenaient.
 2. Estimer sa **gravité**, notamment en fonction du caractère préjudiciable des impacts potentiels et, le cas échéant, des mesures susceptibles de les modifier.
 3. Identifier les **menaces** sur les supports des données qui pourraient mener à cet événement redouté et les **sources de risques** qui pourraient en être à l'origine.
 4. Estimer sa **vraisemblance**, notamment en fonction des vulnérabilités des supports de données, des capacités des sources de risques à les exploiter et des mesures susceptibles de les modifier.
- Déterminer si les risques ainsi identifiés peuvent être jugés acceptables compte tenu des mesures existantes ou prévues.
- Dans la négative, proposer des mesures complémentaires et ré-estimer le niveau de chacun des risques en tenant compte de celles-ci, afin de déterminer les risques résiduels.