



GDPR applied to Coswin

Best practices

Documentation

Version : 2.1
Date : 02/11/2022
Author(s) : Vincent Gosselin, Emmanuelle Denormandie
Copyright : Siveco Group - R&D - Products and Testing Service

Table of contents

1. Introduction	4
1.1. Purpose of the document	4
1.2. Methodology	4
1.3. Reminders and definitions	4
2. Delimitation of the context of processing	7
2.1. Who is affected by GDPR?	7
2.2. Context of personal data processing in Coswin	7
3. Personal data and processing	9
3.1. The principles of data protection	9
3.2. Identification of personal data in Coswin	10
3.3. Users management in Coswin	10
3.4. Records without direct personal data	11
3.4.1. Users	11
3.4.1.1. Inventory of data and processing	11
3.4.1.2. Data retention	12
3.4.1.3. Centering of the map in function of the user position	13
3.4.2. Requesters	13
3.4.2.1. Inventory of data and processing	14
3.4.2.2. Data retention	14
3.4.3. Supervisors	14
3.4.3.1. Inventory of data and processing	14
3.4.3.2. Data retention	15
3.4.4. Contacts	15
3.4.4.1. Inventory of data and processing	15
3.4.4.2. Data retention	16
3.4.4.3. Contacts consent management	16
3.5. Signature management in Coswin	17
3.5.1. Signatures in records	17
3.5.2. Signatures in the history of validation circuits	18
3.6. Instant messaging	19
3.6.1. Users management on the instant messaging server	19
3.6.2. Data retention	20
3.7. Records with direct personal data - Employee	20
3.7.1. Inventory of data and processing	20
3.7.2. Data retention	22
3.7.3. Employee calendar	22
3.7.3.1. Employee calendar content	22
3.7.3.2. Calendar data retention	23
3.7.4. Management of geolocation of people in Coswin	23
3.8. Data for the administration of Coswin	25
3.8.1. Report editor	25
3.8.2. Administration console	25
3.8.3. Audit trail	26

4. Rights of persons concerned	27
4.1. User consent	27
4.1.1. Connection message	28
5. Securing data	29
5.1. Security of the Coswin application	29
5.2. Security of the Coswin platform	31
6. Annex	33
6.1. Definitions (complement)	33
6.2. The 8 golden rules	34
6.3. Sensitive data	35
6.3.1. Definition	35
6.3.2. Exceptions	36
6.4. List of Coswin fields that can be anonymized/pseudo-anonymized	36
6.5. Data retention	39
6.6. Evaluation of protective measures for the rights of data subjects	40
6.7. Risk assessment: potential invasion of privacy	40

1. Introduction

Coswin is one of the components of your information system. It may contain and process personal data. The processing of this data must be recorded in the register provided by the **GDPR**.

This document is based on the functionalities of **Coswin 8i.8** version.

1.1. Purpose of the document

This document is designed to help the DPO (Data Protection Officer) to lead a PIA (Privacy Impact Assessment):

1. [To constitute the record of your data processing activities](#) applied to Coswin.
2. [To sort data](#) by applying best practices to Coswin.
3. [Respect the rights of persons](#) identified in Coswin.
4. [Secure personal data](#) of the persons identified in Coswin.

1.2. Methodology

This document is based on the methodology requested by the CNIL (*Commission Nationale de l'Informatique et des Libertés*, National Commission for Information Technology and Civil Liberties), in these three guides downloadable on its website:

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

Privacy Impact Assessment (PIA) :

- METHODOLOGY
- TEMPLATE
- KNOWLEDGE BASES

1.3. Reminders and definitions

GDPR

“ The acronym **GDPR** stands for **General Data Protection Regulation** .

The **GDPR** regulates the processing of personal data within the territory of the European Union.

(...)

This new European regulation draws on the continuity of the French law Information Technology and Liberties of 1978 and consolidates the control by the citizens of the use that could be done on data about them.

It harmonizes the rules in Europe by offering a unique legal framework to professionals. It makes it possible to develop digital business within the European Union based on user confidence.

(source CNIL)

Official texts on:

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



Personal data

“ **Personal data** are any information relating to an identified or identifiable natural person.

An individual can be identified:

- **directly (example : name, first name)**
- or **indirectly** (example : by an ID (customer number), a number (phone number), biometric data, several specific elements proper to his identity : physical, physiological, genetic, psychic, economic, cultural or social identity, but also the voice or image).



(source CNIL)

Personal data processing

“ **Personal data processing** is an operation or a wide range of operations performed on personal data, whatever the method used (collecting, recording, storage, organization, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment).



Remark

“ Data processing must have an **objective**, a **purpose**, that is you can't collect or process personal data only in case it could be useful one day. To every data processing must be assigned a purpose, that must be obviously legal and legitimate in relation to your professional activity.



(source CNIL)

To go further

Chapter > Definitions (complement) [p.33].

2. Delimitation of the context of processing

2.1. Who is affected by GDPR?

The GDPR applies to every organization, public or private, that processes personal data on its behalf or not, if:

- It is established within the **European Union** territory.
- Its activity targets directly **European residents**.



Example

A company in **France**, that exports all its products to **Morocco** for its Mid-Eastern customers **must respect the GDPR**.



Similarly, a company in **China**, offering an e-commerce website in French that delivers products in **France must respect the GDPR**.



2.2. Context of personal data processing in Coswin

Coswin is a CMMS (Computerized Maintenance Management System).

Its purpose is to manage the maintenance of the equipment referenced in its database.

Scheduling maintenance work requires knowing information about staff involved:

- Availability of a person (presence, position).
- Skills, qualifications, authorizations of a person.

Important

Any other **private information should not be recorded in Coswin**. In any case, it will be necessary to:

- Inform the people.
- Implement the measures of protection of this data.
- Submit the user consent.



No sensitive data (in terms of GDPR) should be recorded in Coswin. Processing sensitive data in Coswin is, on principle, forbidden.

To go further

Chapter [Sensitive data \[p.35\]](#).

Remark

For reasons of IT administration, traceability (regulatory and contractual constraints) or ease of use, some information that can identify a person in an indirect way may be recorded in Coswin:

- IP address
- Application access
- Comment time stamp
- Status change history
- Validation history
- GPS position

3. Personal data and processing

3.1. The principles of data protection

The GDPR regulates the collection, use and storage of personal data through **8 golden rules** that every private or public organization has to comply with.



To go further

Chapter > The 8 golden rules ^[p.34].

These 8 golden rules can be summarized in **4 good reflexes** :



1. Collect only the data absolutely necessary

Ask yourself the following questions:

- What are the **objectives**?
- Is this data **essential** in order to achieve these objectives?
- Am I **allowed** to collect it?
- Is this **relevant**?
- Do I have to secure people's **consent**?



2. Be transparent

You must provide **clear and comprehensive information** to people about what will be done with their personal data.



3. Respect people rights

You must meet the demands of:

- **Access**
- **Modification**
- **Deletion**



of data.

4. Secure data

Computer security, physical security must be adapted to **sensitivity of data** and **risks** in case of incident.



3.2. Identification of personal data in Coswin

This inventory is established on the basis of the Coswin standard modules. It should be adapted in function according to the use of other modules (free modules for example).

It mainly concerns:

- The employee file (that may contain **direct** personal data).

Others modules are also involved (that may contain **indirect** personal data):

- Society's contacts
- Requesters list
- The users signatures on Coswin records
- Time stamp of rich text fields (Work order, Job request and Estimate)
- History of connections to Coswin
- History of validation circuits
- Transactions audit

3.3. Users management in Coswin

Only the users referenced in the Coswin database can access the information stored therein (and personal data among it).

In the database are recorded persons that may be identified as:

- **Users** (*users that can see, modify, create or delete data in function of their profiles*).
- **Employees** (*persons in charge of performing maintenance tasks to whom a work is assigned and who record the time passed in Coswin*)
- **Requesters** (*persons who issue needs – job requests, purchase requests – who are holders or maintainers of the equipment referenced in Coswin, etc.*).
- **Supervisors** (*persons in charge of works and who supervise the work of their employees*).
- **Contacts** (*persons referenced by suppliers, entities or stores*).

New 8i.9

→ Since **Coswin 8i.9** version, Coswin has a **renaming** function on each module and a users **anonymization** function.

For ease of use questions, it's possible to associate a Coswin **user** to:

- An employee
- A requester
- A supervisor

Remark

The [User](#) , [Employee](#) , [Requester](#) and [Supervisor](#) codes can be different from each other.

Best practices

In order to reference these people in the Coswin database, you should use a numeric code rather than a nominative code that would make possible to identify the person directly.

If it's necessary, indicate the names and first names in the description associated with the code.

Example :

Discouraged		Preferable	
Code	Description	Code	Description
HAMILTON A	Hamilton Alexander	M436T	Hamilton Alexander

If the person requests that his/her name doesn't appear anymore in Coswin, you just need to modify the description associated with the code.

→ The **IOD** application can be used to modify the [User](#) , [Employee](#) , [Requester](#) and [Supervisor](#) codes.

3.4. Records without direct personal data

3.4.1. Users

Location:  [Tools > Security and profiles > Users](#)

3.4.1.1. Inventory of data and processing

You don't need to record personal data on this module.
However, some data make it possible to identify the person:

- Description (1)
- Signature (1)
- Email address
- User photograph/avatar



(1) see chapter [Signature management in Coswin](#) [p.17].

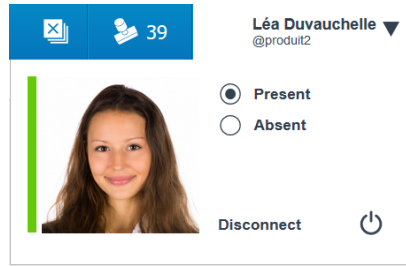
Best practices

Phone numbers and emails recorded must be business contact information.

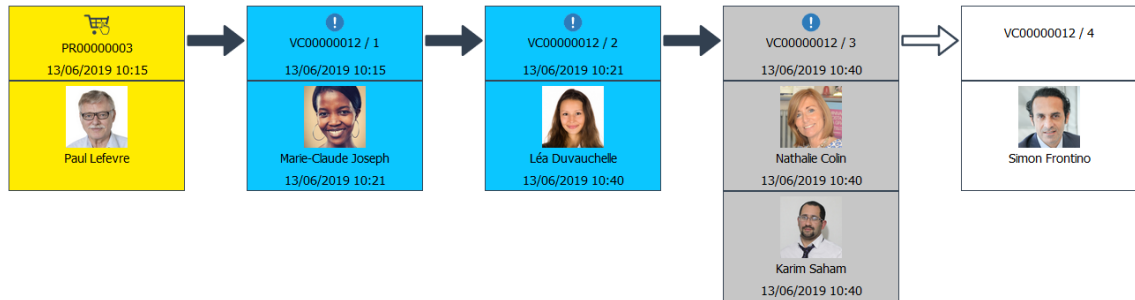


The photograph/avatar specified for the user can be seen:

- By themselves in the user menu



- By the others users in the validation circuits history



- On the chat window of the instant messaging (new 8i.9).

3.4.1.2. Data retention

Information linked to this record must be **deleted or anonymized** once the contractual relationship is finished.

- Deletion of information (personal data) associated with the record.
- Pseudo-anonymization — if required — of the record code with the **IOD** program.



To go further

Chapter > Data retention [p.39].

If the user doesn't need to connect to Coswin, for example after:

- A change of job
- A departure
- An end of mission
- etc.

their Coswin account must be deleted (or otherwise locked).

LDAP

If the authentication of the user is done by means of a LDAP directory, the deletion or suspension of the account must be done at that level.

Remark

The employee, the requester or the supervisor linked to the user can be kept in the database even if

the user account is deleted.

News 8i.9

→ Since **Coswin 8i.9** version, this module has an **anonymization** function.

3.4.1.3. Centering of the map in function of the user position

When a user loads the Coswin **Geolocation** module, he opens a map on an area that depends on the configuration.

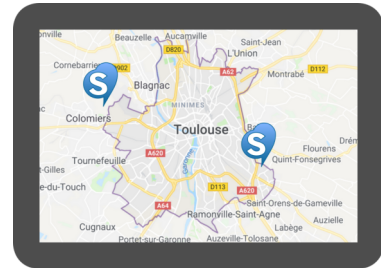
Location: **Tools > Security and profiles > Users >** field **Open position type** (available in the resource editor) :

- **GPS/IP (1)** The map will be centered on the GPS position of his tablet.
- **Employee** The map will be centered on the last recorded position (latitude / longitude) of the employee linked to the connected user.

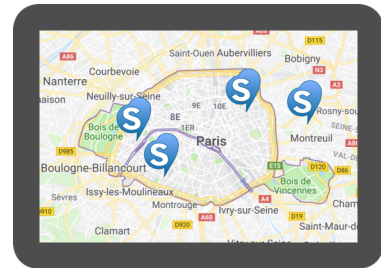
(1) this information is recovered from the browser location function but **it's not stored in Coswin.**

Example with GPS/IP option

- The user is located in **Toulouse**, from his tablet he opens the **Geolocation** module:
→ The map is loaded on **Toulouse**.



- The user is located in **Paris**, from his tablet he opens the **Geolocation** module:
→ The map is loaded on **Paris**.




The user is not displayed as a marker on the map, their position only determines the map centre point.

The markers indicate the position of the geolocated Coswin objects.

To go further

Chapter **(cf. Management of geolocation of people in Coswin)** [p.23] **Management of geolocation of people in Coswin** [p.23].

3.4.2. Requesters

Location:  Common > Requesters/Buyers

3.4.2.1. Inventory of data and processing

You don't need to record personal data on this module.
However, some data make it possible to identify the person:

- Description
- Email address
- Phone number
- Requester photography/avatar



Best practices

Phone numbers and emails recorded must be business contact information.



3.4.2.2. Data retention

Information linked to this record must be **deleted or anonymized** once the contractual relationship is finished.

- Deletion of information (personal data) associated with the record.
- Pseudo-anonymization — if required — of the record code with the **IOD** program.



To go further

Chapter  Data retention ^[p.39].

New 8i.9

→ Since [Coswin 8i.9](#) version, this module has a **renaming** function.

3.4.3. Supervisors

Location:  Maintenance > Resources > Supervisors

3.4.3.1. Inventory of data and processing

It's not necessary to record personal data on this module.
On the other hand, this information makes possible to identify the person:

- Description



Remark

The supervisor description can be limited to his/her function (technical services manager, responsible for the sector X, etc.).

3.4.3.2. Data retention

Information linked to this record must be **deleted or anonymized** once the contractual relationship is finished.

- Deletion of information (personal data) associated with the record.
- Pseudo-anonymization — if required — of the record code with the **IOD** program.




To go further

Chapter > Data retention ^[p.39].

New 8i.9

→ Since [Coswin 8i.9](#) version, this module has a **renaming** function.

3.4.4. Contacts

Location :  [Common > Contacts](#)

3.4.4.1. Inventory of data and processing

You don't need to record personal data on this module.
However, some data make it possible to identify the person:

- Description
- E-mail
- Phone number(s)



💡 Best practices

Phone numbers and emails recorded must be business contact information.



3.4.4.2. Data retention

Information linked to this record must be **deleted or anonymized** once the contractual relationship is finished.

- Deletion of information (personal data) associated with the record.
- Pseudo-anonymization — if required — of the record code with the **IOD** program.



To go further

Chapter > Data retention [p.39].

When a supplier is removed from your organization references, you must delete the contacts attached to it.

If you asked the contact for their consent and they refused or didn't answer

→ You must remove the data associated with the contact.

See chapter > Contacts consent management [p.16].

🗨️ New 8i.9

→ Since **Coswin 8i.9** version, this module has a **renaming** function.

3.4.4.3. Contacts consent management

From Coswin 8i.8, two fields relating to contact consent are available in the resource editor.

Consent	<input checked="" type="checkbox"/> Check box
Consent date	

1 Extraction of contact persons

Use extraction tools (Excel export or report) in order to list the contact persons and obtain their consent.

2 Conduct a campaign of re qualification of your contacts

Take the opportunity to clean up your contacts!

Specify the purpose of the operation:

- What you will do with this information.

- What you will not do.

Example of mailing

In accordance with articles 6 and 7 of GDPR, XXX requires your consent for the collection of the information listed below (Please confirming that the information is correct):

- Society
- First name, Name
- Professional e-mail
- Professional phone
- Type of contact (Commercial/Technical/Other)

This data will only be used to **update our suppliers' directory**.

XXX undertakes not to disclose this data to a third party neither to use it in a advertising or commercial approach.

You can withdraw your consent at any time by contacting YYY.

- I give my consent to the processing of my personal data in accordance with the specified purpose only.

Update Coswin

1. Use tools (ClicClac, mass modification) in order to update Coswin.
2. Delete contacts who refused to give their consent.
3. Maintain your contacts list by regularly completing this re qualification campaign.

3.5. Signature management in Coswin

For questions of traceability, when a user creates a static datum or a transaction, their signature is recorded on the record.

The user signature is defined in the module:

 [Tools > Security and profiles > Users > field Signature](#) .


By default, the signature is initialized with the user description.

3.5.1. Signatures in records

Important

The modification of this value doesn't update the existing records.
Only new records will be recorded with this new signature.

To go further

Chapter  [List of Coswin fields that can be anonymized/pseudo-anonymized](#) ^[p.36].

Management of the comments time stamp

The transactions :

- Work orders
- Job requests

■ Estimates

have the parameter [Make work order notes/job request remarks read-only](#) / [Split Estimate notes](#) that, if it's activated, makes possible to time stamp the user comments. This date is prefixed by the user signature:

#[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 / User description

Since 8i.8, two parameters make possible to specify the nature of this information:

Use the user description for Work order feedback notes

- The user signature is displayed in the time stamp date of the feedback note.
- The description signature is displayed in the time stamp date of the feedback note (if it does exist, otherwise it's the user signature).

Use the user description for the remarks

- The user signature is displayed in the time stamp date of the job request remarks.
- The description signature is displayed in the time stamp date of the job request remarks (if it does exist, otherwise it's the user signature).

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

Since [Coswin 8i.9](#) version, the signature of the WO Notes field and the JR Problem field is boxed with characters `# [` and `]`.

Two parameters make possible to remove this signature when the transactions are archived:

Remove the user signature from feedback notes when archiving

- The user signature is kept in the feedback notes timestamp when archiving.
- The user signature is removed from the feedback notes timestamp when archiving.

Remove the user signature from remarks when archiving

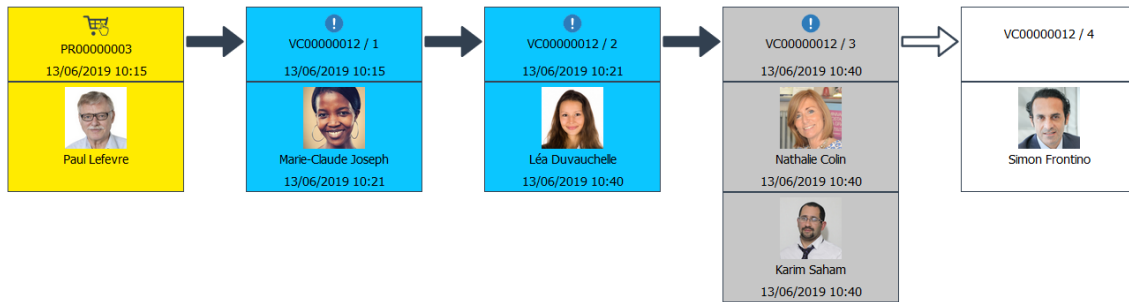
- The user signature is kept in the remarks timestamp when archiving.
- The user signature is removed from the remarks timestamp when archiving.

3.5.2. Signatures in the history of validation circuits

The signature is also taken into account in the validation circuit history.

The signature of the person who has been notified, who validated or refused the step, is the one in force at the time when this diagram is displayed (and not the signature as it existed at the time when the step

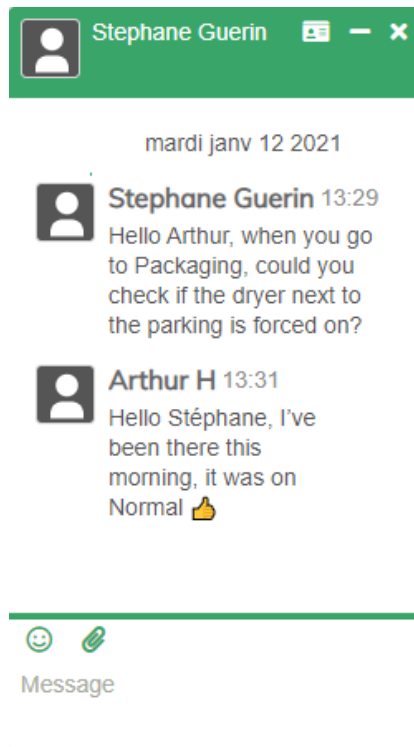
has been processed).



3.6. Instant messaging

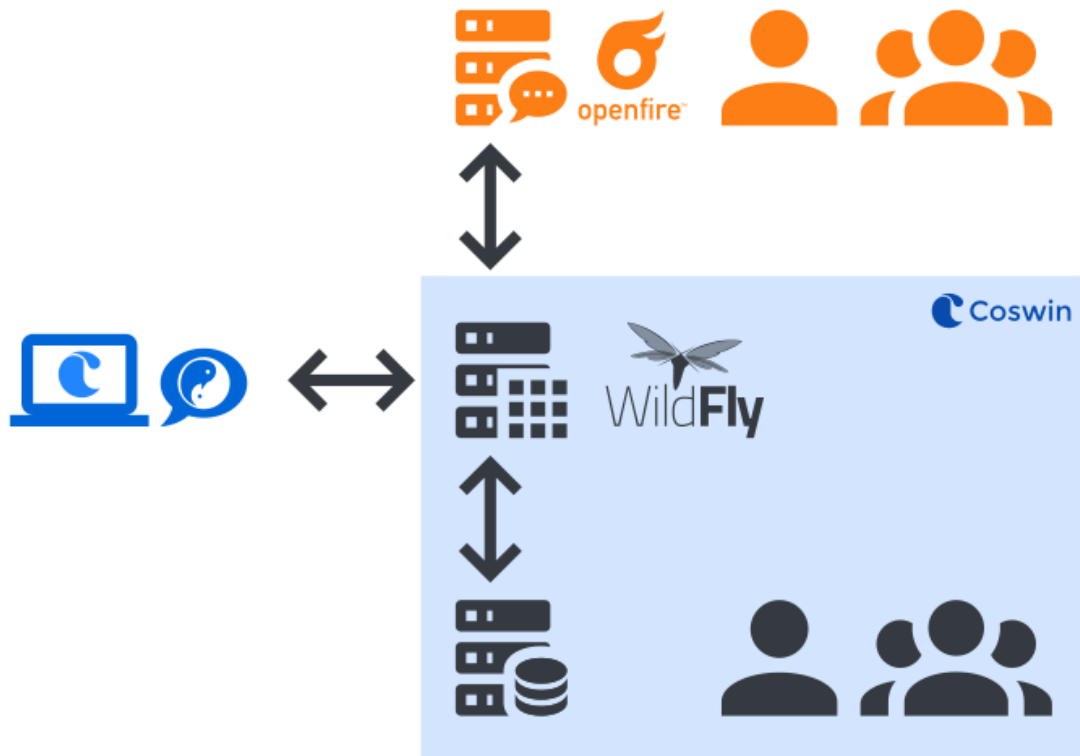
New 8i.9

→ Since [Coswin 8i.9](#) version, users can chat through an instant messaging when they are connected to Coswin.



3.6.1. Users management on the instant messaging server

- Coswin users and messaging groups are duplicated on the messaging server database (Openfire – external to Coswin).
- Automatic and manual processes make possible to synchronise – on the messaging server – these reference sources (code, description, entity and avatar).
- When a Coswin user is deactivated or removed from Coswin, he is automatically removed from the messaging server database.



3.6.2. Data retention

- Messages (chat and internal messaging) only route through the messaging server.
- When the recipient accesses the message, this one is removed from the messaging server.
- The discussion thread is stored in the browser [WebStorage](#) (persistently [localStorage](#)).

3.7. Records with direct personal data - Employee



Location: [Tools > Security and profiles > Users](#)

Personal data can be recorded in the Employee module.

It will be necessary to:

- Conduct a personal data inventory.
- Justify the relevance.
- Identify and implement actions aimed at minimizing these data.

3.7.1. Inventory of data and processing

Column name	Label	Position
REEM_DESCRIPTION	Employee description	Header
REEM_BAR_CODE	Bar code	 Details tab
REEM_EMAIL	E-mail	
REEM_EMERGENCY_CONTACT	Emergency contact	
REEM_FAX	Fax	
REEM_PHONE	Phone	
REEM_ADR_TO_GEOLOC	Address to geolocalise (1)	 ID details tab
REEM_LATITUDE	Latitude (1)	
REEM_LONGITUDE	Longitude (1)	
REEM_SEX	Sex (2)	
REEM_PIN	PIN	
REEM_WORKER_ID	Employee ID	

Only fields **Employee description** and **Sex** are mandatory.
The others fields are optional in Coswin.

New 8i.9

→ Since [Coswin 8i.9](#) version, it is possible to encrypt the fields in blue (see chapter [The 3 principles of security \(cf. Security of the Coswin application\)](#)^[p.29]).

Best practices

Phone numbers and emails recorded must be business contact information.



(1) see chapter [Management of geolocation of people in Coswin](#)^[p.23].

New 8i9

(2) Management of the [Sex](#) field

Since Coswin 8i.9, the radio button [Sex](#) (that before had only two values Male/Female) is replaced by a choice list with the following values:

- Not informed
- Male
- Female
- Neutral

When an employee record is created, this field is initialized with [Not informed](#) by default.

The **Skills** module identifies the employee's:

- Skills
- Authorizations
- Certifications
- etc.



necessary for the efficient execution of the work.

This information, which may be useful in the work assignment process and for legal reasons, can be retained for a period of time.

3.7.2. Data retention

The period of retention of this information may be subject to a legal obligation.

Example

For questions of **traceability of the life cycle** of certain equipment, you must be able to prove that maintenance operations have been executed according to the rules and by a qualified person (authorization, skill level, etc.).

3.7.3. Employee calendar

The purpose employee calendar is to keep track of the employee's availability.

The employee absences (holidays, absence hours or days) must be recorded in their calendar to make planning and assignment of the work possible.

3.7.3.1. Employee calendar content

Absence reason

Coswin needs to know if a person is available or not.


The reason for unavailability is therefore only a use criteria.

Best practices

Be sure to specify absence reasons that are not considered as sensitive data in the legal sense.

Discouraged	Preferable
Trade union delegation	Unavailable
Strike	
Medical examination	

The absence reasons are defined in:

 Tools > Parameters > Maintenance > Calendar control button Reason for absence .

3.7.3.2. Calendar data retention

Every year, the **calendar control** process must be launched in order to delete the old data (including the data related to the employees) that are not supposed to be stored.

→ The purpose of the calendar is to know the availability of the persons for work orders in progress and upcoming.

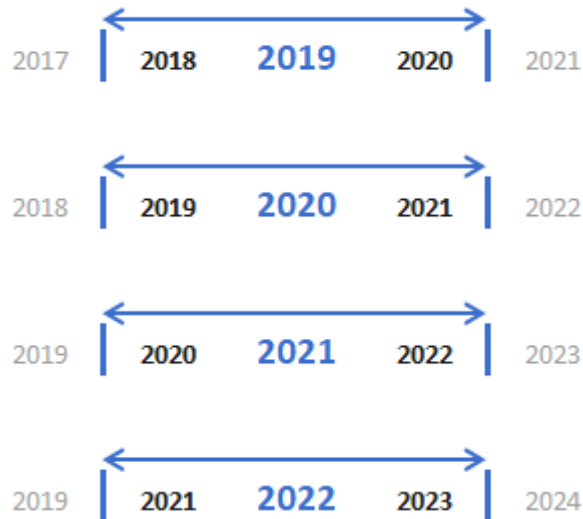
Best practices

We recommend to work by sliding period, for example on 3 years, with:

- year -1
- current year
- year +1

The calendar control has to be launched at the beginning of every year.

Sliding period of calendar control



To go further

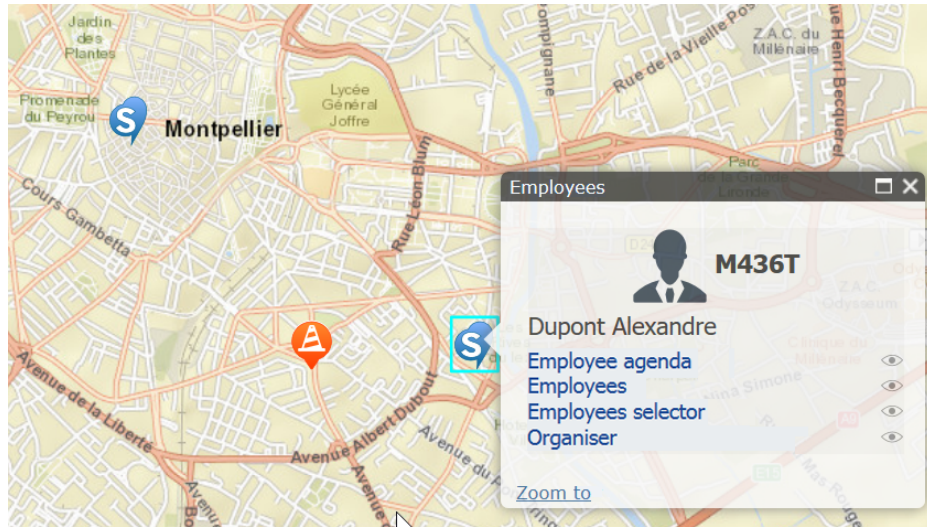
Chapter [Data retention \[p.39\]](#).

3.7.4. Management of geolocation of people in Coswin

The objective of employee geolocation is to know their positions in order to assign work.

1. For ease of use.
2. For security issues (lone worker for example).

Example



In order to assign work on the work order **A** to an employee **S**, it is useful to know the position of the employees nearby.

Update of the employee position

The positioning of the employee on the map is done:

- Manually on the map by the person responsible of the works assignment
- Automatically through Coswin Nom@d

Update of the position through Coswin Nom@d

The update of the position always requires the user **consent**.

The administrator must firstly indicate if the Nom@d user's position is to be used.

Tools > Security and profiles > Users > Tab Details > Section Coswin Nom@d

Check box Locatable

- The user is not geolocatable.
- The user is geolocatable in Coswin Nom@d.

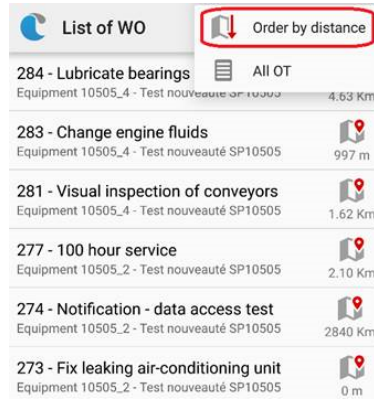
In case the option is checked, when the session is opened on the Coswin Nom@d terminal, a question will be asked to the user:

Do you accept to be geolocated ?

- No their position won't be sent to Coswin
- Yes their position will be **sent to Coswin** and updated when data is transferred.

Remark

In case of no geolocation, the Nom@d user can know the position of the equipment or works nearby.



List of WO		Order by distance
284 - Lubricate bearings	Equipment 10505_4 - Test nouveauté SP10505	4.63 Km
283 - Change engine fluids	Equipment 10505_4 - Test nouveauté SP10505	997 m
281 - Visual inspection of conveyors	Equipment 10505_4 - Test nouveauté SP10505	1.62 Km
277 - 100 hour service	Equipment 10505_2 - Test nouveauté SP10505	2.10 Km
274 - Notification - data access test	Equipment 10505_2 - Test nouveauté SP10505	2840 Km
273 - Fix leaking air-conditioning unit	Equipment 10505_2 - Test nouveauté SP10505	0 m

The employee position **does not need** to be sent to Coswin to do this.

⚠ Important - No tracking

When the new position of the employee is sent to Coswin, it overwrites the last position (and its associated date/time).

It's not possible to view the itinerary taken by the employee.

3.8. Data for the administration of Coswin

Coswin offers several administration tools.

These tools can access personal data, so it is appropriate to limit their use to asset management administrators only:

- Report editor [p.25]
- Administration console [p.25]
- Audit trail [p.26]

3.8.1. Report editor

The [reports editor](#) enables the CMMS administrator to create statuses in the database. It is an application independent of Coswin that connects directly to the database.

→ Therefore it is a critical application which access should be limited to authorized persons only.



💡 Best practices

An option makes possible to display technical information about the field (name of the table and the column for example) in the field tooltips.

This option must be enabled only for user groups that are authorized to use it.

Location: [Tools > Security and profiles > Groups > tab Details](#), field [Tooltip](#).

3.8.2. Administration console

The [Administration console](#) enables the asset management administrator to view:

- Current connections
- Concurrent connections statistics history
- **Users connections statistics history**



→ The Statistics graph makes possible to view up to one year of connections.

New 8i9

→ Since Coswin 8i.9, it's possible to delete the connections history either entirely or in dated sections.

3.8.3. Audit trail

The [audit trail](#) enables the asset management administrator to view — on the modules where it is activated — the life cycle of the records:

- Who created the record?
- Who modified what on the records?



→ The audit trail is activated for traceability purposes, so these data are not supposed to be deleted. However, it is possible to delete this data up to a date specified by the administrator.

4. Rights of persons concerned

Inform people

Every time you collect personal data, the support used (form, questionnaire, etc.) must have **informative notices**.

Check that the data includes the following elements:

- Why are you collecting data: «the purpose».
- What authorize you to process these data: «legal basis».
- Who has access to data (indicate classes: relevant internal services, provider, etc.).
- How long you store them (example: «5 years after the end of the contractual relationship»).
- The modalities by which the persons concerned can exercise their rights.
- If you transfer data outside the EU: specify the country and the legal framework that maintain the level of data protection.



→ At the end of this stage, you met your **obligation of transparency**.

Enable persons to exercise easily their rights

- Persons whose data is processed (customers, collaborators, providers, etc.) have rights on their data, that are moreover reinforced by the GDPR: right of access, rectification, objection, deletion, portability and limitation of the processing.
- Establish an internal process that enables to guarantee the identification and the processing of the requests within a short time (**maximum 1 month**).



To go further

Chapter > Evaluation of protective measures for the rights of data subjects ^[p.40].

4.1. User consent

Introduction

Since Coswin 8i.8, three fields related to users' consent have been made available in the resource editor.

Consent required	<input checked="" type="checkbox"/> Check box
Consent	<input checked="" type="checkbox"/> Check box
Consent date	

If the check box **Consent required** is checked and the check box **Consent** unchecked, then, at the next connection to Coswin, the user will have to read the terms below and accept them in order to access Coswin.

If the user accepts, the check box **Consent** will be checked and the **Consent date** will indicate the date on which the consent has been given.

Best practices

Inform the users regularly (at least one a year).

In [Tools > Parameters > General > General parameters > GDPR consent recall interval \(in month\)](#), indicates the number of months between two consent requests.

If you modify your processing and/or you customize the content of the file **gdpr_en_EN.html** (in the internal WebDAV [/coswin-repository/content/default/login](#)), you must obtain the users' consent.

4.1.1. Connection message

GDPR

Access to the Coswin application requires the user to be authenticated.

This authentication is associated with elements that make it possible to identify the user:

- Directly (name, first name)
- Indirectly (employee code, business email address, business phone number)

Where required, other personal data can be recorded in Coswin (business agenda, professional skills, GPS position, emergency contact).

The details of this information is available from the person who is responsible for processing the personal data of your organisation.

The purpose of the data processing is limited to professional use in Coswin for the completion and the follow-up of the tasks associated with the software exploitation for the maintenance, stock and purchase management:

- Identification of the connected users.
- Identification of the users that create and modify records.
- Identification of the employees availability in order to assign works.
- Identification of the employees skills in order to assign works.
- Identification of the employees position in order to assign works.

No sensitive personal data (defined in the article 9.1 of the GDPR) is used in Coswin.

No personal data will be communicated to third parties or used for publicity or commercial reasons.

You have the right to withdraw your consent at any time.

Further information in <https://www.siveco.com/fr/infoprod>

Improper terms

The Coswin user commits to not using improper terms in Coswin fields, particularly in remarks. Improper terms can be words perceived as sexist, racist or otherwise offensive.

By clicking on *Accept*, I give my consent for the use of this data.

5. Securing data

The GDPR deals with the risks linked to the data security in relation to persons. You must assess this risk (severity and likelihood) and adopt measures to minimize this risk as much as possible.

Example of risk

The technical staff of your organization are obliged to work in private homes. You recorded in Coswin the access codes of the keypad that make possible the access to the buildings of these individuals.

→ You will have to consider a hypothetical scenario where this information would be in the middle of nowhere, evaluate the consequences that would cause this incident and make the arrangements to ensure this incident does not occur (either accidentally or deliberately).

To go further

Chapter  Risk assessment: potential invasion of privacy ^[p.40].

Measures to be taken

You must establish security measures:

- At the Coswin application level.
- At the Coswin platform level.

5.1. Security of the Coswin application

The 3 principles of security

Principle of **confidentiality**: personal data must be accessible to authorized persons only.

Principle of **integrity**: personal data can't be altered or modified.

Principle of **availability**: personal data must be permanently accessible to authorized persons.

→ It is a continuous process. Measures must be regularly adjusted in function of the evolution of risk.



3

Coswin makes it possible to meet these obligations at different levels:

- Access to the module.
- Access to module fields.
- Access to certain records of the module.
- The possibility of encrypting the fields of employee module that contain personal data.

Access to the module

Access to modules is granted at the level of the user group rights (the user inherits the sum of the rights of groups he is linked to).

Location:  Tools > Security and profiles > Groups > tab  Rights

→ If you think it's not necessary for a user profile to have access to the information of a module, access to that module should not be granted.



Best practices

- Restrict the access to a module (for example the Employee details) doesn't mean the user can't select a record of this module from another.
 - Since the selection of this record can be done through a selector, personal data shouldn't be displayed in that selector.
- The user has the possibility to **export** the content of a selector in an **Excel** file or to **print** a report that could include personal data of these records.
 - For these modules, you can remove the right **Print** (that makes possible printing **and** export to Excel).

Access to module fields

The **Resource editor** makes possible to hide the access to fields (or tabs) of a screen:

- **Systematic** (ex. the field is never visible/enabled).
- **Conditional** (ex. the field is visible/enabled only if the condition is fulfilled).



Access to certain records of the module

The access to records can be restricted with:

- Data access
- Administrator filters



New 8i.9

→ Since **Coswin 8i.9** version, it's possible to encrypt the fields of the **employee record** that contains personal data.

Encryption allowed for the following fields:

- REEM_EMAIL (Email)
- REEM_EMERGENCY_CONTACT (Emergency contact)
- REEM_FAX (Fax)
- REEM_PHONE (Phone)
- REEM_PIN (PIN)
- REEM_WORKER_ID (Worker ID)



The encrypted data can be seen only if the database accesses the encryption key. Without access to this key – unique for each database – the fields content can't be used.



5.2. Security of the Coswin platform

Users management

Establish protocols in order to ensure that:

- When a user leaves your organization, their user account is deleted.
- When a user changes function/service, his rights in relation to modules that process personal data are updated accordingly.



Note

The anonymization process of Coswin users only processes records of the database.

- The user **signature** is displayed in the print logs (files `coswin-print.log` and `coswin-print.yyyy-mm-dd hh`)
- Location `/wildfly-18.0.0.Final/standalone/log`
- This document indicates:
 - The signature of the user who printed the report.
 - The name of the report.
 - The date of the printing.

→ If the administrator wants to delete the signature of one of the users of these files, he will have to do it manually with a text editor (function search/replace).

Strong password

Establish a strong password policy. The user is authenticated either:



- through an LDAP directory
 - The manager of the directory must establish this policy.
- or at the level of the database *
 - On the Oracle version of Coswin, location: `Tools > Security and profiles > Profiles` you can activate the profiles management that make possible to use the options of Oracle passwords management (see the online user guide).



* The password encryption algorithm depends on the RDBMS version:

Database		Algorithm
Oracle	10g	DES
	11g	SHA-1
	12c and above	SHA-512
SQL Server	2012 and above	SHA-512
PostgreSQL	10	MD5

Best practices

- Raise users awareness to get into the habit to lock their computer when they leave their work session.
- Activate idle time control
 Location :  Tools > Security and profiles > Groups > Tab  Details :
 Check the box Use idle time .

Update of Coswin

The updates of Coswin guarantee the integrity of the solution.

- Use recent versions of Coswin.
- Install cumulative patches.

Keep components updated (database, application server, printing server) of the Coswin platform:

- Security patch of the operating system of the components.
- Security patch of the database.



6. Annex

6.1. Definitions (complement)

CNIL - Commission Nationale de l'Informatique et des Libertés

The *Commission Nationale de l'Informatique et des Libertés* (French National Commission for Information Technology and Civil Liberties) is in charge of the regulation of personal data. The CNIL assists professionals to comply with data protection and individuals to control their personal data and exercise their rights.











EDPB - European Data Protection Board

The *European Data Protection Board* coordinates the action of the *committees in charge of the application of the GDPR* of all the EU member states by means of notices and decisions.



The EDPB advises the European Commission on questions about GDPR.

List of EDPB members

Country	Committee	Website
 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.uoou.cz/
 Denmark	Datatilsynet	http://www.datatilsynet.dk/
 Estonia	Estonian Data Protection Inspectorate (Andmekaitse Inspeksioon)	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. The 8 golden rules

Lawfulness of processing

Processing shall be implemented only if it is **based on at least one of the following lawfulness conditions:**

1. The data subject has given **consent to the processing of their personal data** for one or more specific purposes.
2. Processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
3. Processing is necessary for **compliance with a legal obligation** to which the controller is subject.
4. Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
5. Processing is necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller.
6. Processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Processing purposes

The personal data collected should be **processed for an explicit, determined and legitimate purpose only**.

Data minimization

Only **data strictly necessary to achieve the purpose** can be collected and processed.

Protecting sensitive personal data

Sensitive data can only be **collected and processed in certain conditions**.

Limited data storage

Data must be **archived, erased** or **anonymized** as soon as the purposes for which they have been collected have been achieved.

Security requirement

In view of the risks, **measures** must be implemented in order to **ensure processed data security**.

Transparency

Individuals must be **informed of the use of data about them and the way they can exercise their rights**.

Rights of individuals

Individuals have **many rights that allow them to have control of their own data**.

6.3. Sensitive data

Processing of sensitive data is strictly regulated by law.

6.3.1. Definition

GDPR - Article 9.1

Processing, as well as collecting or consulting, of personal data defined as **sensitive** is in principle **prohibited** by the GDPR since this data is related to private life.

Sensitive data falls within or may concern:

- Racial or ethnic origins.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Health (physical or mental).
- Sex life or sexual orientation.
- Genetic data.
- Biometric data for the purpose of uniquely identifying a natural person.

6.3.2. Exceptions

GDPR - Article 9.2

However there are exceptions to this prohibition principle that enable the processing of these data when it is:

- Provided by the data subject with his **explicit consent**.
- Necessary for **carrying out the obligations** in employment and social protection law (ex: notification of occupational accidents).
- Necessary to **protect the vital interests of the data subject**.
- Carried out for the management of the members of a **not-for-profit organization** (political, philosophical, religious or trade union aim).
- **Manifestly made public** by the data subject (ex: political opinion of an elected official).
- Necessary for the **establishment, exercise or defense of legal claims**.
- Necessary for **reasons of substantial public interest**.
- Necessary for **medical purposes** (preventive medicine, medical diagnosis, management of health or social care systems and services, etc.).
- Necessary for **reasons of public interest in the area of public health**.
- Necessary for **archiving purposes in the public interest, scientific or historical research purposes** (ex: medical research) or **statistical purposes** subject to safeguards.

6.4. List of Coswin fields that can be anonymized/pseudo-anonymized

List of 'Creator' fields

Module	Table	Column
Agreement	AGREEMENT	AGAG_CREATOR

History agreement	H_AGREEMENT	HAGAG_CREATOR
Adjustments	ADJUSTMENT	ADAD_CREATOR
History adjustment	H_ADJUSTMENT	HADAD_CREATOR
Depreciation	DEPRECIATION	EFDP_CREATOR
Receipts	RECEIPT	RCRC_CREATOR
History receipt	H_RECEIPT	HRCRC_CREATOR
Workshop	WORKSHOP	WSWS_CREATOR
Purchase additional clause	ADDITIONAL_CLAUSE	POAC_CREATOR
History purchase additional clause	H_ADDITIONAL_CLAUSE	HPOAC_CREATOR
Transport notice	TRANSPORT_NOTICE	TNTN_CREATOR
Credit	CREDIT	CNCR_CREATOR
History credit	H_CREDIT	HCNCR_CREATOR
Transport output form	TRANSPORT_OUTPUT_FORM	TNOF_CREATOR
Map layers	MAPLAYERS	CWML_CREATOR
Working area map layers	WORKING_AREA_MAPLAYERS	CWWM_CREATOR
Certifications	CERTIFICATION	PDCE_CREATOR
Validation circuit	VALIDATION_CIRCUIT	WFVC_CREATOR
Job request status circuits	JR_STATUS_CIRCUIT	JRSC_CREATOR
Work order status circuits	WO_STATUS_CIRCUIT	WOSC_CREATOR
Contract clause	CONTRACT_CLAUSE	ERCC_CREATOR
History package	H_PACKAGE	HPPPA_CREATOR
Purchase orders	ORDER	POPO_CREATOR
History purchase orders	H_ORDER	HPOPO_CREATOR
List configurations	FS_CONFIG	FSIC_CREATOR
Map reference service	MAP_REF_SERVICES	CWMS_CREATOR
Graph configuration	GRAPH_CONFIG	GRCO_CREATOR
Purchase request	REQUEST	PRPR_CREATOR
History purchase request	H_REQUEST	HPRPR_CREATOR
Quotation	QUOTATION	PQPQ_CREATOR
History quotation	H_QUOTATION	HPQPQ_CREATOR
Job requests	JOB_REQUEST	JRJR_CREATOR
History job requests	H_JOB_REQUEST	HJRJR_CREATOR
Estimate	ESTIMATE	ESES_CREATOR
Invoices	INVOICE	PIPI_CREATOR

PPE assignment by employee	EMPLOYEE_SAFETY	REEF_CREATOR
Estimate bills	ESTIMATE_BILL	ESBI_CREATOR
History invoices	H_INVOICE	HPIPI_CREATOR
Work order bills	BILL_WORK_ORDER	BIWO_CREATOR
Linked files	LINKED_FILES	CWLF_CREATOR
Stock availability plan history	PLAN_AVAILABILITY	PLAV_CREATOR
Currency history	CURRENCY_HISTORY	PDCH_CREATOR
Intersection between homepage section and indicators	SECTION_INDICATOR	CWSI_CREATOR
Intersection between map layers and reference services	MAPLAYERS_REF_SERVICE	CWMR_CREATOR
Interventions	JOB	MDJB_CREATOR
Counts	COUNT	SCSC_CREATOR
History counts	H_COUNT	HSCSC_CREATOR
Conditions set	WORKFLOW_CONDITION_SET	WFCS_CREATOR
Equipment status update	STATUS_UPDATE	ERSU_CREATOR
Resource PPE model	RESOURCE_MODEL	REMO_CREATOR
Employee PPE model	EMPLOYEE_MODEL	REEO_CREATOR
Price supplier modification	PRICE_MODIFICATION	PSPM_CREATOR
Work notification	WORK_NOTIFICATION	NNWN_CREATOR
Transit order	TRANSIT_ORDER	PPTO_CREATOR
Work order	WORK_ORDER	WOWO_CREATOR
History work order	H_WORK_ORDER	HWOWO_CREATOR
Welcome page	WELCOME_PAGE	CWWP_CREATOR
User group welcome page	GROUP_PAGE	CWGP_CREATOR
Work permit	WORK_PERMIT	WPWP_CREATOR
Calibration report	CALIBRATION_REPORT	CACR_CREATOR
Projects	PROJECT	PLPO_CREATOR
BIMServer project	BIM_SERVER_PROJECT	BMSP_CREATOR
Invoice reconcile	RECONCILE	PIRE_CREATOR
History invoice reconcile	H_RECONCILE	HPIRE_CREATOR
Contract extension	CONTRACT_EXTENSION	EREX_CREATOR
Demands	DEMAND	DMDM_CREATOR
History demands	H_DEMAND	HDMDM_CREATOR
Working area	WORKING_AREA	CWWA_CREATOR
Issues	ISSUE	ISIS_CREATOR

History issues	H_ISSUE	HISIS_CREATOR
Calibration	CALIBRATION	CACA_CREATOR
Depreciation add clause follow up	DEPRECIATION_ADD_CLAUSE	EFDA_CREATOR
Transfers	TRANSFER	TRTR_CREATOR
History transfers	H_TRANSFER	HTRTR_CREATOR
Work order view	V_WORK_ORDER	VWOWO_CREATOR

List of 'Last modification by' fields

Module	Table	Column
BIMServer projects	BIM_SERVER_PROJECT	BMSP_LAST_MODIFIED_BY
History job requests	H_JOB_REQUEST	HJRJR_LAST_MODIFIED_BY
History work orders	H_WORK_ORDER	HWOWO_LAST_MODIFIED_BY
Job requests	JOB_REQUEST	JRJR_LAST_MODIFIED_BY
Work orders view	V_WORK_ORDER	VWOWO_LAST_MODIFIED_BY
Work orders	WORK_ORDER	WOWO_LAST_MODIFIED_BY

List of 'User' fields (in the tab Transaction status history)

Module	Table	Column
History of work order status history	H_WO_HISTORY_STATUS	HWOHS_USER
Job request status history	JR_HISTORY_STATUS	JRHS_USER
Work order status history	WO_HISTORY_STATUS	WOHS_USER
Work permit status history	WP_HISTORY_STATUS	WPHS_USER

6.5. Data retention

For each processing, you must define:

- A fixed duration of retention.
- Or an objective criteria used to define this duration.

Example

| The contractual relationship duration.

When the organization meets the goal of the data collection, this data must:

- Be **deleted**.
- Or be subject of an **anonymization or pseudo-anonymization process**.
- Or be **archived** under certain conditions.

Questions you should ask yourself

- For how long?
- Am I under a legal obligation to retain the data?
- If so, what is the exact scope of this obligation? What are the data that need to be retained and for how long?

Example

| Litigation, legal action.

6.6. Evaluation of protective measures for the rights of data subjects

Methodology recommended by the CNIL

- Identify or determine, and describe, the **controls** (existing or planned) selected to comply with the following legal requirements (it is necessary to explain how it is intended to implement them):
 1. **Information** for the data subjects (fair and transparent processing,).
 2. **Obtaining consent**, where applicable: express, can be demonstrated and withdrawn .
 3. Exercising the **right of access and right to data portability**.
 4. Exercising the **rights to rectification and erasure**.
 5. Exercising the **right to restriction of processing and right to object**.
 6. **Processors**: identified and governed by a contract.
 7. **Transfers**: compliance with the obligations bearing on transfer of data outside the European Union.
- Check that improving each control and its description, pursuant to the GDPR, is either not necessary or not possible.
- Where applicable, review their description or propose additional controls.

6.7. Risk assessment: potential invasion of privacy

What is a privacy risk? (CNIL's definition)

A risk is a hypothetical scenario that describes a feared event and all the threats that would allow this to occur.

The risk level is estimated in terms of severity and likelihood:

- **Severity** represents the magnitude of a risk. It primarily depends on the prejudicial nature of the potential impacts.
- **Likelihood** expresses the possibility of a risk occurring. It primarily depends on the level of vulnerabilities of the supporting assets when under threat and the level of capabilities of the risk sources to exploit them.

Methodology recommended by the CNIL

- For each feared event (illegitimate access to personal data, unwanted change of personal data, and disappearance of personal data):
 1. Determine the potential **impacts** on the data subjects' privacy if it occurred.
 2. Estimate its **severity**, particularly depending on the prejudicial nature of the potential impacts and, where applicable, controls likely to modify them.
 3. Identify the **threats** to personal data supporting assets that could lead to this feared event and the risk sources that could cause it.
 4. Estimate its **likelihood**, particularly depending on the level of vulnerabilities of personal data supporting assets, the level of capabilities of the risk sources to exploit them and the controls likely to modify them.
- Determine whether the risks identified in this way can be considered acceptable in view of the existing or planned controls.
- If not, propose additional controls and re-assess the level of each of the risks in view of the latter, so as to determine the residual risks.