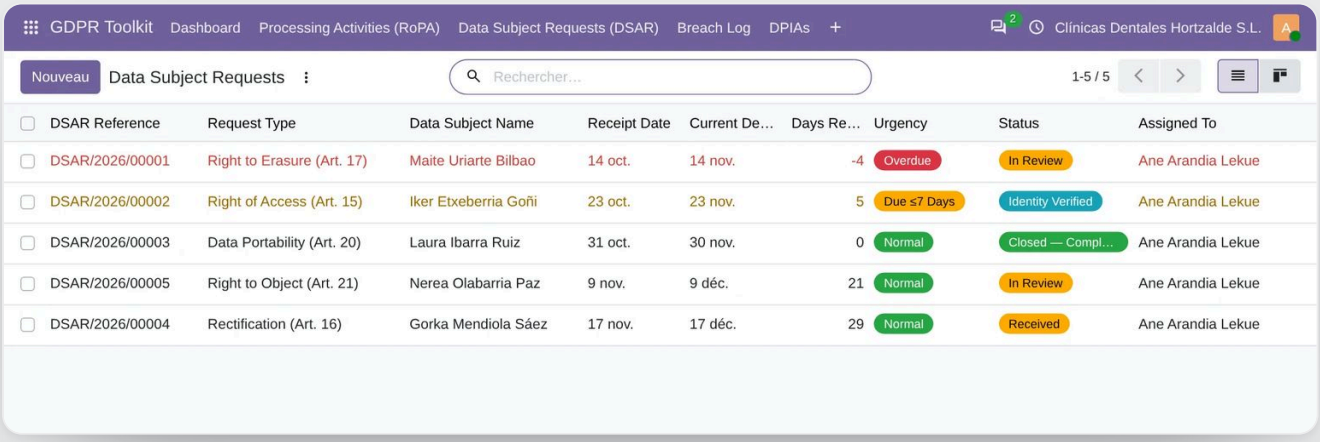
GUIDE DU MODULE · PROTECTION DES DONNÉES

GDPR Compliance pour Odoo

Le registre des activités, les demandes avec leur délai, les violations avec leurs 72 heures et les AIPD, directement dans Odoo.

Odoo 17 · 18 · 19 · 20 | 14 jours d'essai, sans carte | Édition du 19-11-2026





Capture réelle d'Odoo 20. Liste des demandes avec leur échéance et leur niveau d'urgence, et une violation de données avec le compte à rebours de 72 heures.

Sommaire

À droite, la page où commence chaque chapitre. Les menus et les boutons portent les noms d'Odoo en français. Les menus et boutons propres au module sont en anglais : le module n'est pas encore traduit en français.

1	**À qui s'adresse le module et ce qu'il résout**	3
2	**Le module en chiffres**	4
3	**Où le trouver dans votre Odoo**	5
4	**Ce dont vous avez besoin avant de commencer**	6
5	**L'essai de FlexigoTech Cloud**	6
6	**Mise en place pas à pas**	8
7	**Le registre des activités de traitement**	10
8	**Les demandes des personnes concernées et leurs délais**	13
9	**Portabilité, effacement et portail de confidentialité**	19
10	**Le registre des violations et les 72 heures**	22
11	**Les analyses d'impact (AIPD)**	25
12	**La conservation et ses révisions**	29
13	**Rapports, exports et journal d'audit**	33
14	**Autorités de contrôle et bases juridiques**	36
15	**Ce qui part vers FlexigoTech Cloud et ce qui revient**	39
16	**Ce qui se passe automatiquement**	40
17	**Les options du module et leurs valeurs par défaut**	41
18	**Sécurité et données personnelles**	43
19	**Plusieurs sociétés**	43
20	**En cas de problème**	44
21	**Autres façons de procéder**	45
22	**Formules et tarifs**	46
23	**Questions fréquentes**	47
24	**Glossaire**	50
25	**Liste de vérification et contact**	51

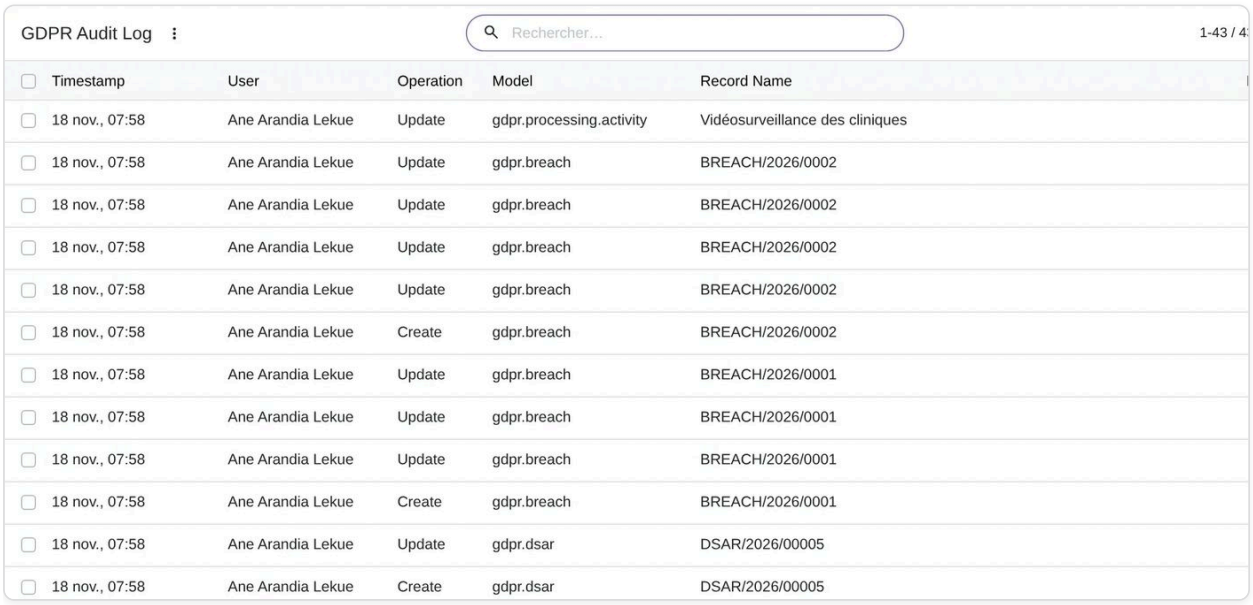
Ce guide décrit la version 20.0.1.1.13 du module (branche 20.0 d'Odoo, commit e15afc58d). Tout ce qu'il dit vient de son code publié, de la documentation officielle de la plateforme ou de captures réelles.

Les captures viennent d'une base Odoo 20 de test, avec une société et des données inventées et sans connexion réelle à FlexigoTech Cloud. Le module existe aussi pour Odoo 17, 18 et 19.

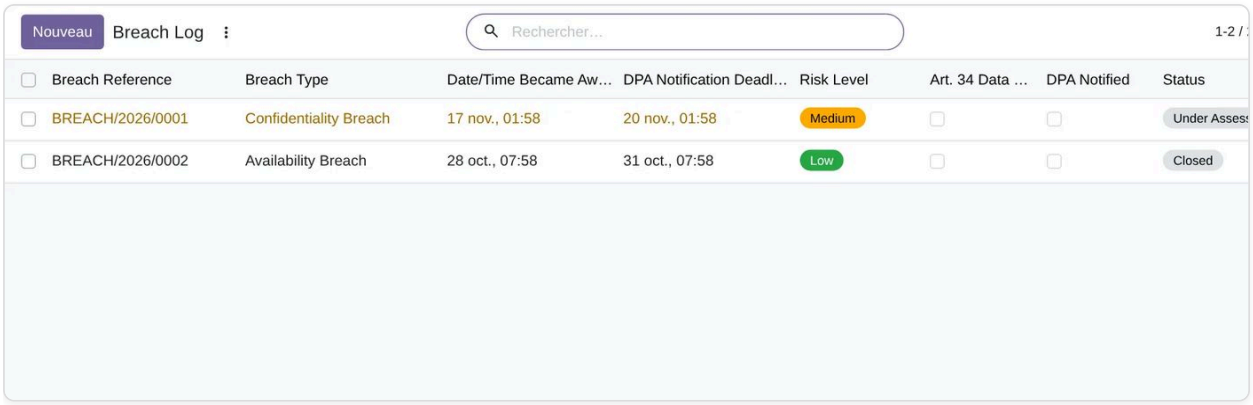
1 À qui s'adresse le module et ce qu'il résout

Sans le module, le registre des activités se trouve souvent dans des feuilles de calcul éparses. Les délais des demandes se calculent à la main et personne n'est alerté lorsqu'ils approchent. Il ne reste aucun historique de qui a modifié quoi ni quand. En cas de violation, personne ne tient le décompte des heures écoulées depuis que l'on en a eu connaissance.

Avec le module, tout cela se trouve dans Odoo, avec les délais visibles et un journal d'audit impossible à modifier.



- **Capture réelle d'Odoo 20.** Le **GDPR Audit Log** avec la date, l'utilisateur et l'opération de chaque modification.



- **Capture réelle d'Odoo 20.** La liste **Breach Log** avec le délai de notification de 72 heures de chaque violation.

Ce qui change au quotidien

- Chaque activité de traitement conserve ses finalités, ses bases juridiques, ses catégories de données et de personnes concernées, ses destinataires et sa durée de conservation, et chaque modification est enregistrée dans son historique.
- Les demandes des personnes concernées portent un délai d'un mois à compter de leur réception, prorogeable de deux mois si nécessaire, à condition de le motiver (art. 12.3). Des listes permettent de voir celles qui sont hors délai et celles qui arrivent à échéance cette semaine.
- Une violation commence à compter 72 heures à partir du moment où vous notez quand on en a eu connaissance (art. 33.1). Pendant ses 6 dernières heures, le module envoie un e-mail toutes les heures tant

que vous ne l'avez pas marquée comme notifiée.

- Une activité qui remplit deux critères des lignes directrices WP248 est marquée **DPIA Required** et le module n'autorise pas son activation tant qu'elle n'a pas d'AIPD approuvée. L'AIPD (art. 35) comporte cinq étapes et signale la consultation préalable lorsque le risque résiduel l'exige (art. 36).
- La personne concernée disposant d'un compte portail envoie sa demande depuis /my/privacy-rights et reçoit un accusé de réception par e-mail.

Ce qu'il ne fait pas

- Il ne supprime ni n'anonymise aucune donnée Odoo. La vérification de suppression recense les données existantes et enregistre votre décision ; c'est vous qui supprimez ou anonymisez.
- Il ne notifie pas l'autorité de contrôle et ne communique rien aux personnes concernées. Vous y consignez ce que vous avez fait : le statut, la date et l'heure, la méthode et la référence.
- Il n'envoie pas la lettre de réponse à la personne concernée. Vous la rédigez dans l'onglet de réponse à partir d'un modèle, puis vous l'envoyez vous-même.
- Il ne décide pas à votre place si une violation doit être notifiée ou si une AIPD est nécessaire. La matrice de risque (impact par probabilité) et ses seuils sont ceux du module, et non ceux du RGPD ni des lignes directrices du Comité européen ; la décision finale revient au responsable du traitement ou à son DPD.
- Ce n'est pas un conseil juridique.

GUIDE DU MODULE · GDPR COMPLIANCE

2 Le module en chiffres

155
tests automatiques

7 013
lignes de code dans Odoo Apps (branche 20.0)

32
autorités de contrôle

16
bases juridiques

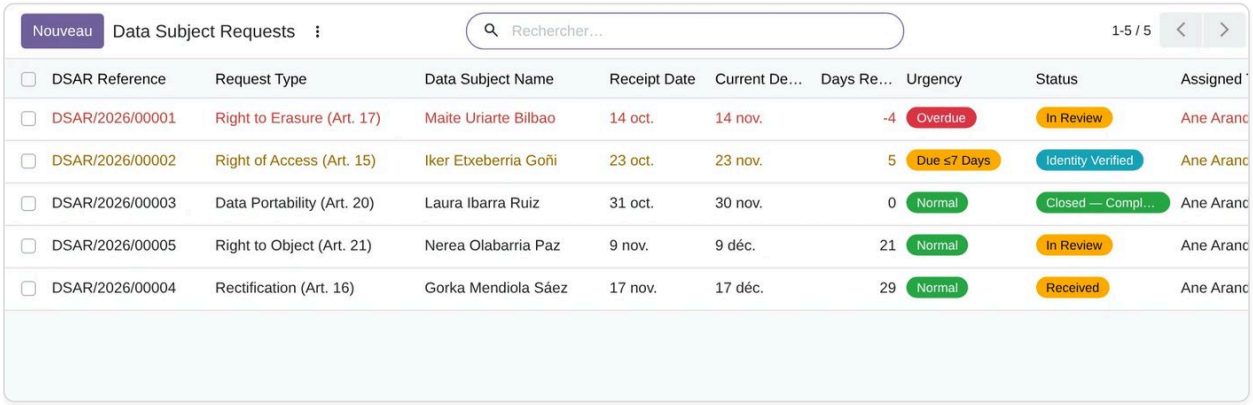
5
tâches planifiées

14
jours d'essai de FlexigoTech Cloud

Il ne dépend que de modules Odoo Community (base, mail et portail) et de `flexigotech_cloud`, il fonctionne donc sur Community comme sur Enterprise. Une version du module existe pour Odoo 17, 18, 19 et 20.

> Comment il a été testé : le module embarque 155 tests automatiques dans sa version Odoo 20. L'équipe de FlexigoTech l'a testé sur Odoo 17, 18, 19 et 20, sur des bases Community et sur Odoo.sh, et a vérifié ses délais par rapport au texte du RGPD publié sur EUR-Lex (articles 12.3, 33.1, 35 et 36). Aucune autorité n'a examiné le module et il ne constitue pas un conseil juridique : la décision finale vous revient, ou à votre DPD.

3 Où le trouver dans votre Odoo



- **Capture réelle d'Odoo 20.** La liste **Data Subject Requests** avec le délai en vigueur, les jours restants et l'urgence de chaque demande.

Tableau de bord	Trois boutons qui ouvrent des listes. Détails plus bas.
Processing Activities (RoPA)	**All Activities** et **DPIA Required**.
Data Subject Requests	**All Requests**, **Overdue** et **Due This Week**.
Breach Log	**All Breaches** et **Active Incidents**. Visible uniquement par **GDPR Toolkit / Manager**.
DPIA	**All DPIAs** et **Awaiting DPO Review**. Visible uniquement par **GDPR Toolkit / Manager**.
Retention Management	**Retention Schedule** et **Review History**. Visible uniquement par **GDPR Toolkit / Manager**.
Rapports	**Export RoPA (PDF)**, **Export RoPA (Excel)**, **DSAR History Report**, **Breach Log Report** et **DPIA Status Report**. Visible uniquement par **GDPR Toolkit / Manager**.
Configuration	**DPO & Settings**, **Supervisory Authorities**, **Categories of Data**, **Categories of Data Subjects**, **Categories of Recipients**, **Legal Bases** et **Audit Log**. Visible uniquement par **GDPR Toolkit / Manager**.

Le menu **Dashboard** ouvre la configuration de la société avec trois boutons : **View Open DSARs**, **View Active Breaches** et **DPIAs Pending Review**. Chaque bouton ouvre une liste. Il n'affiche ni chiffres ni indicateurs.

En dehors de son menu, le module ajoute le portail de confidentialité à l'adresse /my/privacy-rights de votre Odoo, pour les personnes disposant d'un compte portail. Le module n'ajoute aucun lien dans la page Mon compte du portail : c'est vous qui communiquez l'adresse à la personne concernée. Cinq tâches planifiées envoient des e-mails : le rappel quotidien des délais de demande, l'alerte de compte à rebours des violations, la vérification quotidienne de l'échéance de conservation, la remontée hebdomadaire des demandes hors délai et le rappel annuel de révision du RoPA.

4 Ce dont vous avez besoin avant de commencer

- Odoo 17, 18, 19 ou 20, sur Odoo.sh ou sur votre propre serveur. Odoo Online ne convient pas, car il n'autorise pas l'installation de modules tiers.
- Qui sera **GDPR Toolkit / Manager** et qui sera **GDPR Toolkit / User**. À l'installation du module, l'administrateur est **GDPR Toolkit / Manager**.
- Les coordonnées du DPD ou, à défaut, de la personne responsable de la confidentialité : nom, e-mail et téléphone.
- L'autorité de contrôle principale. Elle se choisit dans la configuration, parmi les autorités fournies par le module.
- Si vous souhaitez que les notes internes, la justification d'un refus ainsi que la description et les conséquences des violations soient stockées chiffrées, définissez la variable GDPR_FERNET_KEY sur le serveur. C'est à la personne qui l'administre de la renseigner. Sans elle, ces textes sont stockés en clair et **Encryption Key Configured** l'indique.
- Pour inclure des données de ventes ou d'employés dans l'export de portabilité, les applications Ventes et Employés doivent être installées.
- L'abonnement à FlexigoTech Cloud ou son essai de 14 jours. Il permet de surveiller chaque jour six sources officielles et d'être alerté lorsqu'une d'elles change.

> Le module ne supprime ni n'anonymise de données : la vérification de suppression recense les données existantes et enregistre votre décision. Il ne notifie pas non plus l'autorité de contrôle et ne communique rien aux personnes concernées : vous y consignez ce que vous avez fait. Il n'envoie pas la lettre de réponse à la personne concernée. La décision finale revient au responsable du traitement ou à son DPD, et le module ne constitue pas un conseil juridique.

L'installation se fait comme pour tout module Odoo tiers, sur Odoo.sh ou sur votre serveur. Odoo installe en même temps `flexigotech_cloud`, la connexion à FlexigoTech Cloud, ainsi que les applications Odoo dont il dépend : Discuss et le portail.

5 L'essai de FlexigoTech Cloud

1. **Cliquez sur Activer dans la barre supérieure**
   Ce bouton apparaît dès l'installation du module. Il ouvre la fenêtre **Activer FlexigoTech Cloud**, avec le forfait Standard et ses 14 jours gratuits, sans carte bancaire.



- **Capture réelle d'Odoo 20.** La fenêtre d'activation : lisez la liste des données, cochez la case et saisissez votre e-mail.

2 **Acceptez et saisissez votre e-mail**

Cochez « J'ai lu la liste et j'accepte, au nom de mon entreprise… » (cela inclut les conditions de l'abonnement et le contrat de sous-traitance) et saisissez l'**E-mail de la personne qui accepte**.

3 **Cliquez sur Connecter et démarrer l'essai**

Odoo enregistre la base auprès de FlexigoTech Cloud et démarre l'essai du module. Si vous préférez attendre, **Plus tard** ferme la fenêtre.

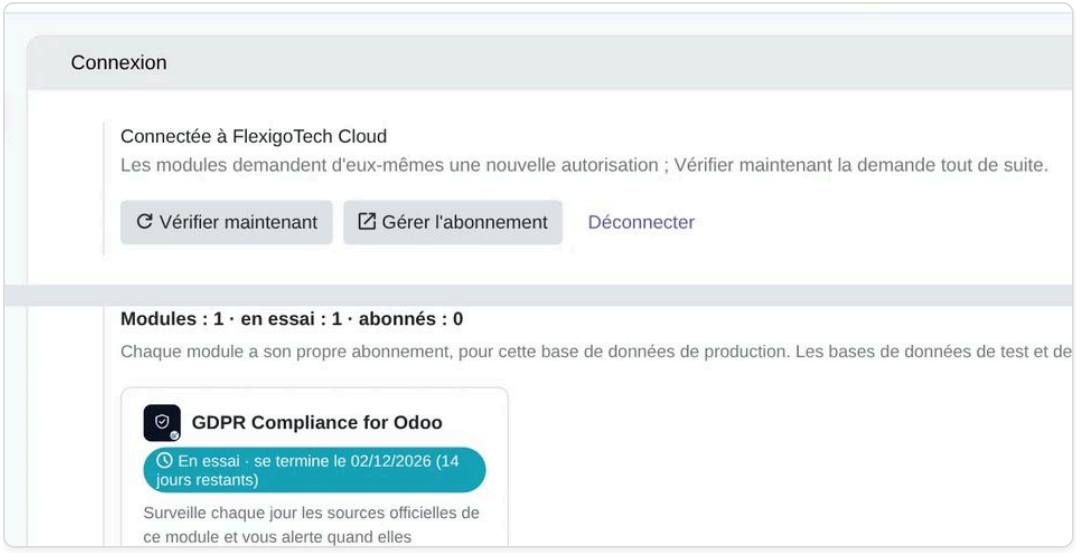
La même opération, depuis les Paramètres

Dans **Paramètres › FlexigoTech Cloud** figure la liste complète des données transmises par la base. Cochez la case, saisissez l'e-mail et cliquez sur **Accepter et connecter**. Si vous avez déjà un compte sur app.flexigotech.com, le champ **Vous avez un code de votre compte ?** relie la base à ce compte (le code est valable 10 minutes).



- **Capture réelle d'Odoo 20.** Paramètres › FlexigoTech Cloud, avant la connexion : la case cochée, l'e-mail et **Accepter et connecter**.

Une fois la base connectée, le bloc **Modules** affiche chaque module avec son statut : **En essai** et la date de fin, **Abonné**, etc. C'est là que l'on choisit le forfait (Standard ou Pro, mensuel ou annuel) et que l'on clique sur **S'abonner** : le paiement se fait sur la page Stripe, en dehors d'Odoo.



- **Capture réelle d'Odoo 20.** Paramètres › FlexigoTech Cloud avec la base connectée et le module en essai.

Prix hors TVA. Si vous ne vous abonnez pas à la fin de l'essai, le service s'arrête et rien n'est facturé ; vos données restent dans votre Odoo. **Vérifier maintenant** demande l'autorisation immédiatement (sinon le module la renouvelle automatiquement toutes les 6 heures).

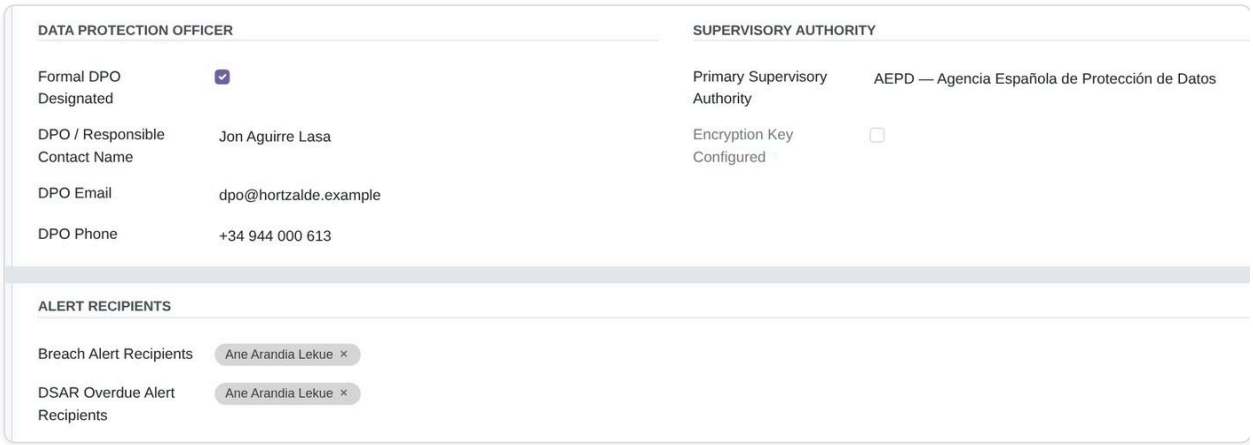
> Sur une copie neutralisée (staging) ou sur une base contenant des données de démonstration, il est impossible de démarrer un essai : Paramètres l'indique par le message « Cette base de données est une copie neutralisée ou contient des données de démonstration, on ne peut donc pas y démarrer d'essai. »

GUIDE DU MODULE · GDPR COMPLIANCE

6 Mise en place pas à pas

1 Ouvrez la configuration

Allez dans **GDPR Toolkit › Configuration › DPO & Settings**. La configuration RGPD de votre société s'ouvre ; si elle n'existe pas encore, Odoo la crée avec les valeurs par défaut.



- **Capture réelle d'Odoo 20.** La configuration RGPD de la société, avec les coordonnées du DPD, l'autorité de contrôle et les destinataires des alertes.

2 Renseignez les coordonnées du DPD

Renseignez **DPO / Responsible Contact Name**, **DPO Email** et **DPO Phone**. S'il n'y a pas de DPO désigné, décochez **Formal DPO Designated**.

3 **Choisissez l'autorité de contrôle**

Sélectionnez l'**Primary Supervisory Authority**.

4 **Indiquez les destinataires des alertes**

Renseignez **Breach Alert Recipients** et **DSAR Overdue Alert Recipients**. Si vous ne mettez personne, les alertes sont envoyées aux utilisateurs ayant **GDPR Toolkit / Manager** dans la société.

5 **Réglez les délais d'anticipation**

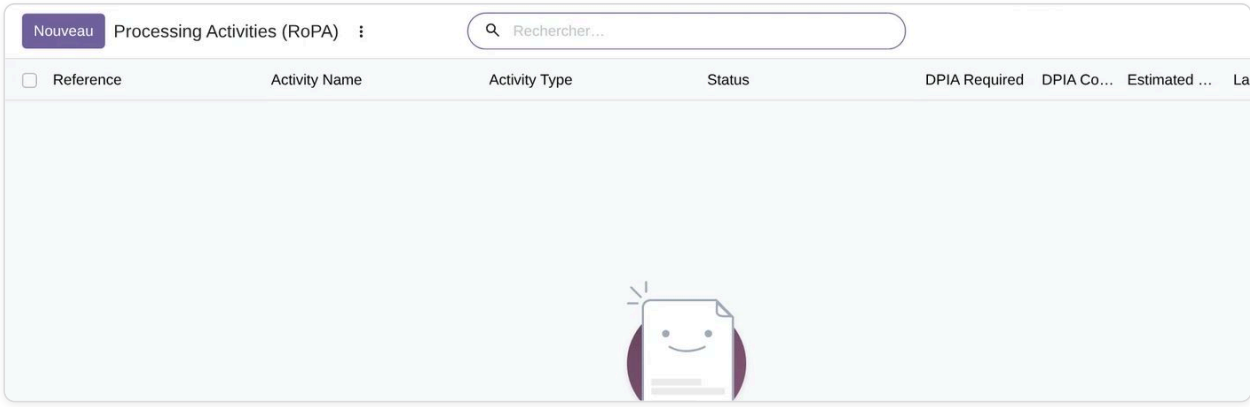
Vérifiez **Retention Advance Warning (days)**, réglé par défaut sur 30, et **DSAR Reminder Days Before Deadline**, réglé par défaut sur 7.

6 **Attribuez les groupes**

Attribuez **GDPR Toolkit / Manager** et **GDPR Toolkit / User** aux personnes concernées.

7 **Créez la première activité**

Allez dans **GDPR Toolkit › Processing Activities (RoPA) › All Activities**. Au départ, la liste est vide. Cliquez sur **Nouveau** et renseignez l'activité.



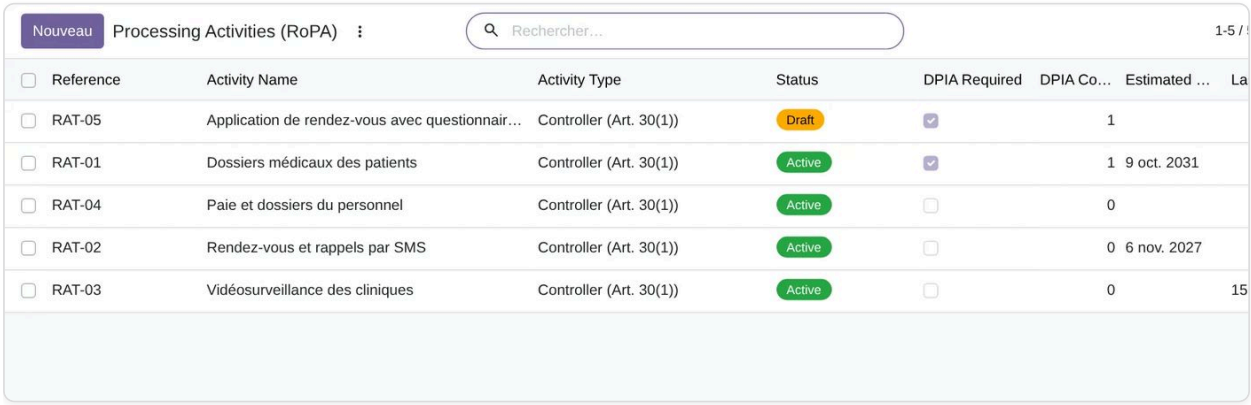
- **Capture réelle d'Odoo 20.** La liste des activités de traitement, encore vide.

8 **Communiquez l'adresse du portail**

Si vous voulez que les personnes concernées fassent leurs demandes via le portail, communiquez à chacune disposant d'un compte portail l'adresse /my/privacy-rights de votre Odoo. Le module n'ajoute aucun lien dans la page Mon compte.

Après cela, les tâches planifiées fonctionnent seules. Chaque jour, les rappels des demandes arrivant bientôt à échéance sont envoyés et la fin de conservation est vérifiée. Chaque heure, pendant les 6 dernières heures du délai d'une violation, son alerte est envoyée. Chaque semaine, un récapitulatif des demandes hors délai est envoyé et, une fois par an, un rappel de révision du registre des activités. Le rappel d'une demande est envoyé à la personne assignée ; les autres alertes vont aux destinataires que vous avez indiqués ou, à défaut, aux gestionnaires RGPD de la société.

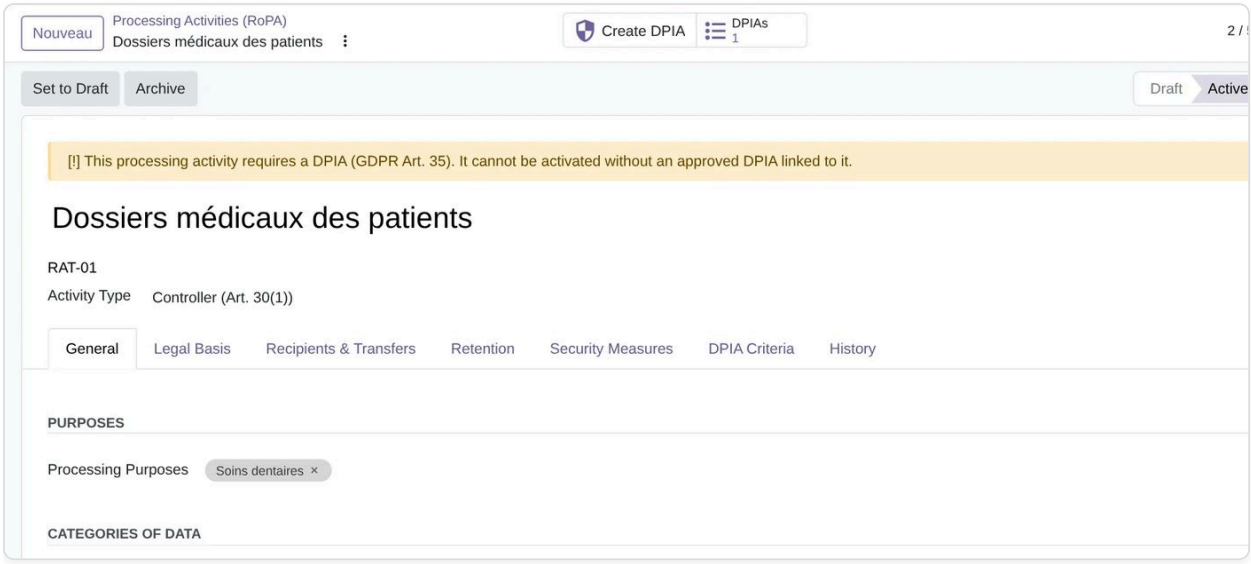
7 Le registre des activités de traitement



- **Capture réelle d'Odoo 20.** La liste **Processing Activities (RoPA)** avec ses cinq activités.

Chaque fiche contient ce qu'exige l'art. 30.1 si vous agissez en tant que responsable du traitement, ou l'art. 30.2 si vous agissez en tant que sous-traitant. Vous le choisissez dans **Type d'activité**. Vous renseignez les finalités, les catégories de personnes concernées, de données et de destinataires, la base juridique de l'art. 6 et celle de l'art. 9, les transferts vers des pays tiers avec leur garantie, la conservation et les mesures de sécurité.

Les catégories de données, de personnes concernées et de destinataires se choisissent dans les listes de **GDPR Toolkit › Configuration › Categories of Data**, **GDPR Toolkit › Configuration › Categories of Data Subjects** et **GDPR Toolkit › Configuration › Categories of Recipients**. Les finalités se créent en les saisissant directement dans la fiche. La **Reference** est attribuée par Odoo à la création de l'activité et n'est pas modifiable.



- **Capture réelle d'Odoo 20.** La fiche d'une activité avec ses onglets.

Set Active	Passe l'activité à **Active**. Le bouton n'apparaît pas lorsqu'elle est déjà active.
Set to Draft	Remet l'activité à **Brouillon**. N'apparaît que lorsqu'elle est active.
Archive	Fait passer l'activité à **Archived**. Il n'apparaît pas lorsqu'elle est déjà archivée.

États

- **Draft** : l'état initial de l'activité.
- **Active** : l'activité qui est en vigueur.

- **Archived** : l'activité qui n'est plus utilisée. Elle reste dans le registre.

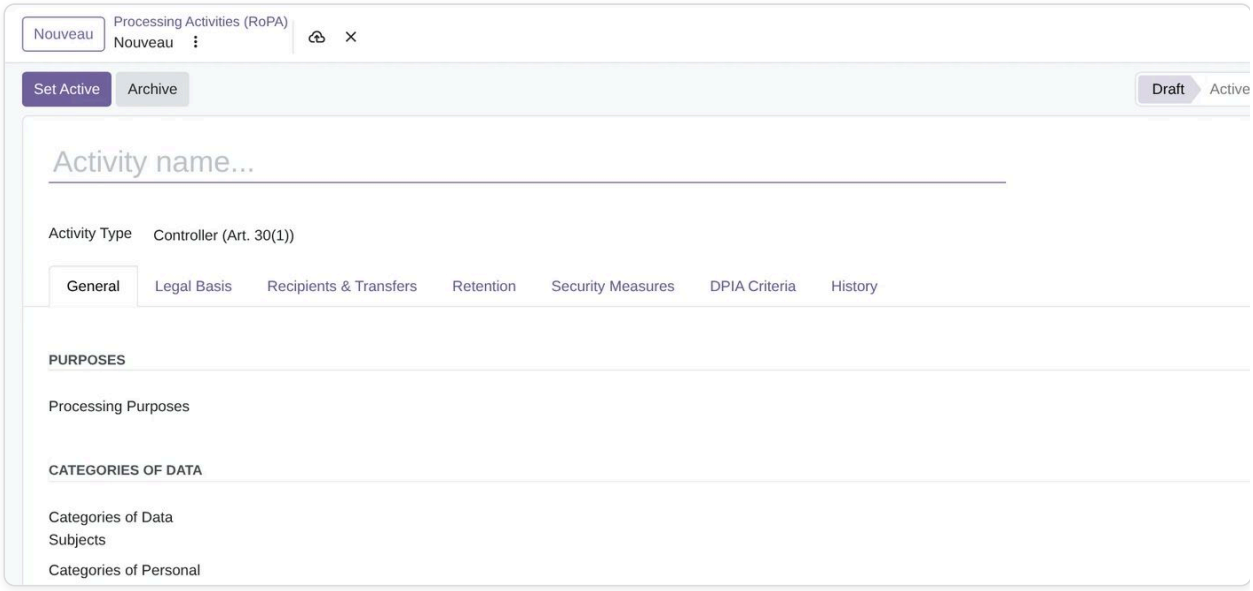
History

Chaque fois qu'une activité est créée ou qu'une modification est enregistrée, le module ajoute une entrée à l'historique, visible dans l'onglet **History**. Ces entrées ne peuvent être ni modifiées ni supprimées.

Créer une activité

1 **Crée l'activité**

Dans la liste **Processing Activities (RoPA)**, cliquez sur **Nouveau**.



- **Capture réelle d'Odoo 20.** Le formulaire d'une nouvelle activité à l'état **Draft**.

2 **Remplissez les onglets**

Complétez **General**, **Legal Basis**, **Recipients & Transfers**, **Retention** et **Security Measures**.

3 **Activez-la**

Cliquez sur **Set Active**.

> Une activité ne peut pas être supprimée : le module l'empêche afin de préserver la piste d'audit, et il faut l'archiver avec **Archive**. Une activité qui exige une AIPD ne peut pas non plus être activée si elle n'est pas liée à une AIPD approuvée.

Signification de chaque état

Draft	État initial. Vous pouvez remplir et corriger la fiche tant que vous la complétez.
Active	L'activité est en vigueur. Pour y parvenir, si elle exige une AIPD, celle-ci doit être liée et approuvée. Depuis cet état, **Set to Draft** la fait revenir à **Draft**.
Archived	L'activité est retirée de l'usage, mais sa fiche et son historique sont conservés. C'est le seul moyen de la retirer, puisqu'elle ne peut pas être supprimée.

Cas où le module vous empêche d'agir

- Activer une activité avec **DPIA Required** sans AIPD approuvée liée : le message « Cannot activate processing activity "...": a DPIA is required but no approved DPIA is linked. Please complete and approve a DPIA first. » s'affiche.
- Supprimer une activité : le message « Processing activity records cannot be deleted to preserve the audit trail. Please archive the record instead. » s'affiche.
- Modifier ou supprimer une entrée de l'historique : les messages « History records are immutable and cannot be deleted. They are part of the GDPR audit trail. » et « History records are immutable. » s'affichent.

Quand l'AIPD est obligatoire

DPIA Required se coche automatiquement lorsque deux critères ou plus de l'onglet **DPIA Criteria** sont remplis, ou lorsqu'on la force à la main avec **DPIA Required (Manual Override)**. Cette règle des deux critères provient des lignes directrices WP248 rév.01 et constitue une bonne pratique générale, non une obligation légale. Les critères sont **Systematic profiling**, **Automated decisions with legal effects**, **Systematic monitoring**, **Special categories at large scale**, **Large-scale processing**, **Data matching / combining**, **Vulnerable data subjects**, **New technology** et **Prevents exercise of rights**. **DPIA Criteria Met** indique combien sont remplis et **DPIA Requirement Reason** consigne la justification.

Onglets et champs de la fiche

General	**Activity Name**, **Activity Type**, les groupes **Purposes** et **Categories of Data**, ainsi que les données du sous-traitant, regroupées dans un groupe dédié, **Processor Details (Art. 30(2))**.
Legal Basis	**Legal Basis (Art. 6)** et **Special Category Legal Basis (Art. 9)**.
Recipients & Transfers	**Categories of Recipients**, **Third-Country Transfer**, **Third Countries**, **Transfer Safeguard** et **Safeguard Notes**.
Retention	**Retention Duration**, **Retention Unit** et **Retention Reference Point**, ainsi que **Reference Date (fixed)**, **Last Transaction Date**, **Estimated Retention End Date** et **Last Retention Review**.
Security Measures	**Technical & Organisational Security Measures**.
History	**Version History** : une entrée pour chaque modification.

Les options de **Transfer Safeguard** sont **Adequacy Decision**, **Standard Contractual Clauses (SCC)**, **Binding Corporate Rules (BCR)**, **EU-US Data Privacy Framework (DPF)**, **Other Safeguard** et **No Safeguard (document justification)**. Dans **Safeguard Notes**, on consigne la référence des CCT, le numéro de certification du DPF ou la justification. **Retention Reference Point** accepte **From End of Contract**, **From Last Transaction**, **From Withdrawal of Consent**, **Fixed Date** et **Other**.

Filtres et listes associées

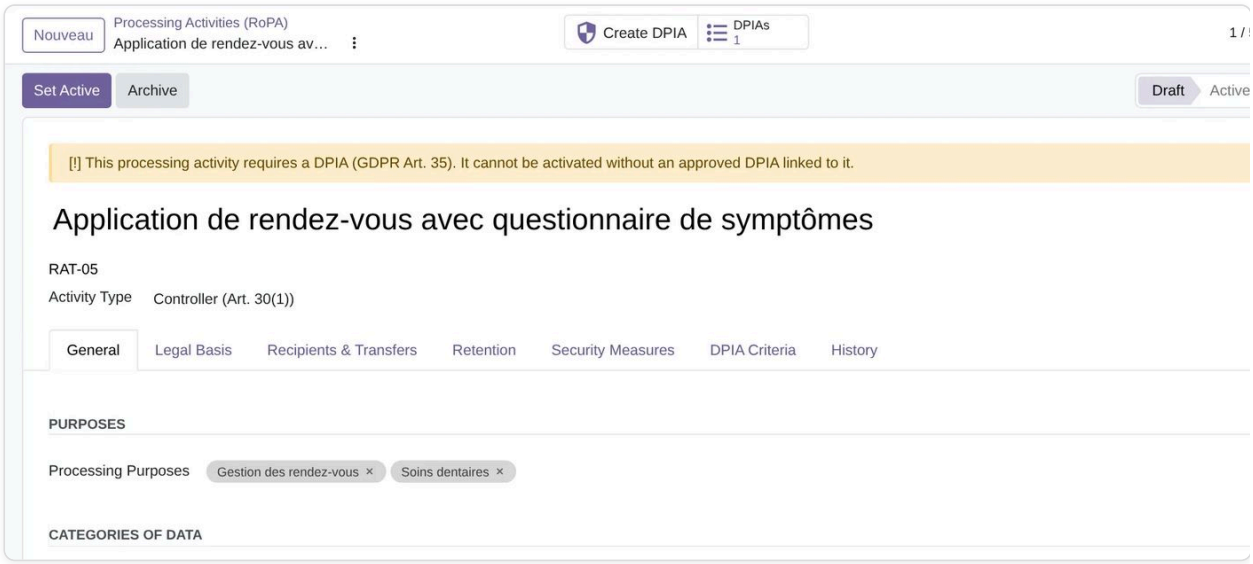
La recherche propose les filtres **Active**, **Draft** et **DPIA Required**, ainsi que les regroupements **By Type** et **By Status**. Le menu **GDPR Toolkit › Processing Activities (RoPA) › DPIA Required** ouvre les activités qui en ont besoin. Le menu **GDPR Toolkit › Retention Management › Retention Schedule** ouvre celles dont la durée de conservation est définie.

Exemple de bout en bout

Les écrans d'exemple montrent une clinique dentaire avec cinq activités. L'une d'elles, le dossier médical des patients, est active et exige une AIPD. Une autre, l'application de prise de rendez-vous en ligne avec questionnaire de symptômes, reste en **Draft** et exige elle aussi une AIPD.

1. **Créer et remplir**

   Vous cliquez sur **Nouveau**, saisissez le nom et complétez les finalités, les personnes concernées, les données, la base juridique, la conservation et les mesures de sécurité.



- **Capture réelle d'Odoo 20.** L'activité en **Draft**, avec l'avertissement qu'elle exige une AIPD.

2. **Tenter de l'activer**

   Vous cliquez sur **Set Active**. Tant qu'aucune AIPD approuvée n'est liée, le module l'empêche et affiche le message d'erreur.

3. **Traiter l'AIPD**

   Le bouton de création de l'AIPD, en haut de la fiche de l'activité, ouvre une nouvelle AIPD déjà liée à elle. Une fois approuvée, vous pouvez activer l'activité.

4. **Consulter l'historique**

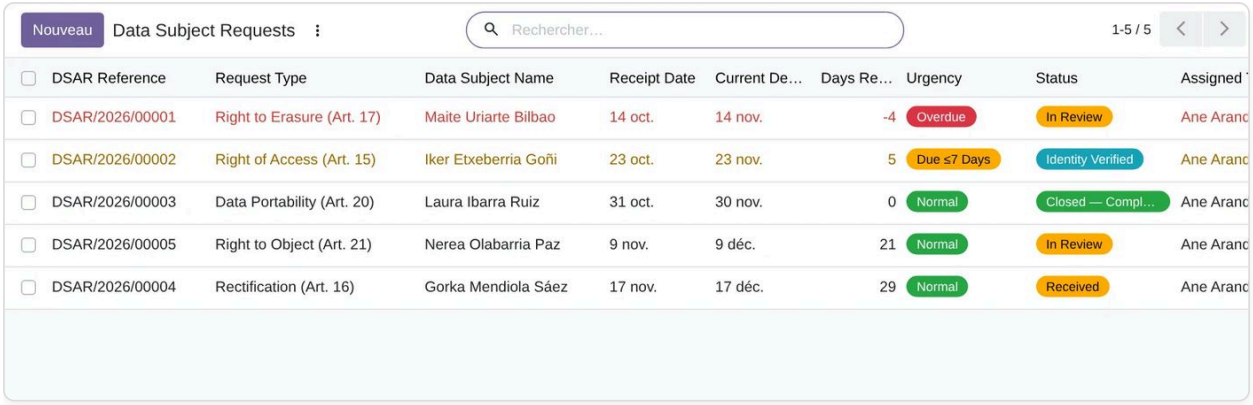
   Chaque modification figure dans l'onglet **History**.

GUIDE DU MODULE · GDPR COMPLIANCE

8 Les demandes des personnes concernées et leurs délais

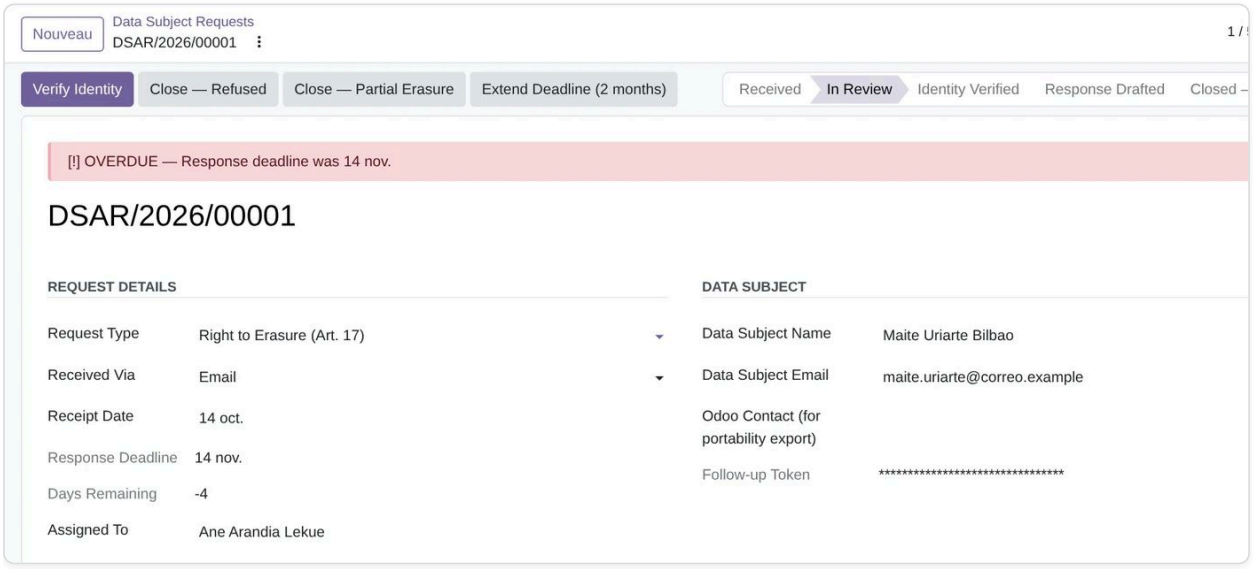
Il existe six types de demande : **Right of Access (Art. 15)**, **Rectification (Art. 16)**, **Right to Erasure (Art. 17)**, **Restriction of Processing (Art. 18)**, **Data Portability (Art. 20)** et **Right to Object (Art. 21)**. Le **Received Via** peut être **Portal Submission**, **Email**, **Letter**, **Phone** ou **Manual Entry**.

Le **Response Deadline** est d'un mois à compter de la **Receipt Date** (art. 12.3 du RGPD). Si nécessaire, il peut être prolongé de deux mois supplémentaires, également au titre de l'art. 12.3, et le **Current Deadline** devient alors le délai prolongé. La colonne **Days Remaining** compte jusqu'à ce délai en vigueur.



- **Capture réelle d'Odoo 20.** La liste des demandes avec leur délai en vigueur, les jours restants, l'urgence et la personne assignée.

La liste **Overdue** affiche les demandes ouvertes dont le délai est dépassé, et la liste **Due This Week** celles qui arrivent à échéance dans sept jours ou moins. La colonne **Urgency** distingue ces deux cas du reste, qui apparaît comme **Normal**.



- **Capture réelle d'Odoo 20.** Une demande avec l'alerte de dépassement de délai et les boutons de son état.

La personne qui traite chaque demande figure dans **Assigned To**. L'onglet **Identity Verification** conserve la méthode, la date et la personne qui a vérifié l'identité. Dans l'onglet **Response** se trouve la **Response Letter** : **Load Response Template** la remplit avec le modèle général et, comme **Draft Response**, fait passer la demande à **Response Drafted**. **Generate Refusal Letter** génère la lettre de refus sans changer l'état. La lettre n'est pas envoyée depuis le module.

Pour refuser, l'onglet **Refusal** demande la **Refusal Legal Basis** et la **Refusal Justification**. Sans justification, il est impossible de clôturer comme refusée.

Boutons de l'enregistrement

Start Review	Fait passer la demande de **Received** à **In Review**.
Verify Identity	Fait passer de **In Review** à **Identity Verified**.
Draft Response	Fait passer de **Identity Verified** à **Response Drafted** et charge le modèle.
Close — Completed	Clôture une demande dont la réponse a été rédigée.

Close — Refused	Disponible en revue, avec l'identité vérifiée ou avec la réponse rédigée.
Close — Partial Erasure	Uniquement pour les demandes d'effacement, dans ces mêmes états.
Extend Deadline (2 months)	Disponible tant que la demande reste ouverte et n'est pas déjà prolongée. Demande le motif.

États

Les états sont **Received**, **In Review**, **Identity Verified** et **Response Drafted**. Une demande se clôture comme complétée, comme refusée ou avec effacement partiel. Les états n'avancent que dans un sens : il est impossible de revenir à un état antérieur.

Rappels

La tâche **GDPR: DSAR Deadline Reminder** s'exécute chaque jour et envoie un courriel lorsqu'une demande ouverte n'a plus que le nombre de jours défini dans **DSAR Reminder Days Before Deadline** : à la personne assignée ; si elle n'a pas de courriel, aux gestionnaires RGPD ; et si personne ne peut être notifié, à l'adresse de la société. Si personne ne peut être notifié, cela est consigné sur la demande. La tâche **GDPR: DSAR Overdue Escalation** s'exécute chaque semaine et envoie le récapitulatif des demandes en dépassement aux **DSAR Overdue Alert Recipients** ou, à défaut, aux gestionnaires RGPD.

> Une demande ne se supprime pas : elle s'archive. Il est impossible de revenir à un état antérieur. Seuls les gestionnaires RGPD peuvent utiliser les boutons de la demande.

Les statuts, un à un

- **Received** : la demande vient d'arriver. Seul **Start Review** est visible.
- **In Review** : quelqu'un l'examine. On peut **Verify Identity**, la clôturer comme refusée, la clôturer avec effacement partiel (si c'est une demande d'effacement) ou prolonger le délai.
- **Identity Verified** : l'identité de la personne concernée est confirmée. On peut **Draft Response**, et depuis cet état clôturer comme refusée ou prolonger le délai.
- **Response Drafted** : le courrier est prêt. Vous pouvez **Close — Completed** ou clore comme refusée.
- Clôturée comme complétée : répondue et fermée.
- Clôturée comme refusée : fermée avec son fondement juridique et sa justification.
- Clôturée avec effacement partiel : uniquement pour les effacements, lorsque certaines données sont conservées.
- Clôturée avec délai prolongé : pas de bouton. Prolonger le délai laisse la demande dans son état et modifie le **Current Deadline**.

Règles et conditions

- Le statut ne revient pas en arrière. Si vous essayez, Odoo affiche « DSAR status cannot be moved backwards. The audit trail must be append-only. »
- Lorsque vous prolongez le délai, vous devez saisir le motif. Sinon, le message « Extension reason is required when extending the deadline. » s'affiche.
- Pour clore comme refusée, la justification est requise. À défaut, le message « Refusal justification is required before closing as refused. » s'affiche.

- **Generate Portability Export** n'apparaît que sur les demandes d'accès et de portabilité dont l'identité est vérifiée. Si vous essayez sans vérification, le message « Identity must be verified before generating a portability export. » s'affiche.
- **Retention Conflict Check** n'existe que sur les demandes d'effacement. Pour un autre type, le message « Retention conflict check only applies to erasure requests. » s'affiche.
- Une demande ne peut pas être supprimée : le message « DSAR records cannot be deleted. Archive them instead (GDPR Manager / Admin only). » s'affiche.
- Les boutons ne fonctionnent qu'avec le groupe gestionnaire RGPD ou avec un administrateur. Sinon, le message « Only GDPR Managers can perform this action. » s'affiche.
- **Load Response Template**, dans l'onglet **Response**, fait la même chose que **Draft Response** : il charge le modèle général et fait passer la demande à **Response Drafted**, même si elle est encore en **Received** ou en **In Review**. Utilisez-le une fois l'identité vérifiée.

La vérification d'effacement

Retention Conflict Check compte les factures publiées, les fiches d'employé (avec l'application Employés) et les commandes de vente (avec Ventes) du contact de la demande. Il vous permet de choisir de conserver ou d'effacer chaque groupe et, avec **Record Decision & Close DSAR**, d'inscrire votre décision dans les notes internes et de clôturer la demande : complétée si tout est effacé, avec effacement partiel si certaines données sont conservées. Le module n'efface ni n'anonymise rien : c'est à vous de le faire dans Odoo.

La fiche : groupes et onglets

Request Details	Le type, le canal, la date de réception, le délai de réponse, les jours restants et la personne assignée.
Data Subject	Le nom et le courriel de la personne concernée, le contact Odoo pour l'export de portabilité et le jeton de suivi.
Extension	**Deadline Extended**, **Extension Reason**, **Extended Deadline (3 months)** et **Extension Notification Due**, qui correspond à la même date que le délai initial : un mois à compter de la réception.
Identity Verification	La case d'identité vérifiée, la méthode, la date et la personne qui l'a vérifiée.
Response	La lettre de réponse et les fichiers de l'export de portabilité.
Refusal	La base juridique et la justification du refus.
Internal Notes	Notes de la personne en charge du dossier.

La base du refus peut être **Manifestly Unfounded (Art. 12(5)(a))**, **Manifestly Excessive (Art. 12(5)(a))**, **Legal Exemption (Art. 23)** ou **Other**. Les notes internes et la justification ne sont chiffrées que si le serveur dispose de la clé de chiffrement. Sans elle, elles sont enregistrées en clair. La configuration l'indique dans **Encryption Key Configured**.

Rappels et filtres

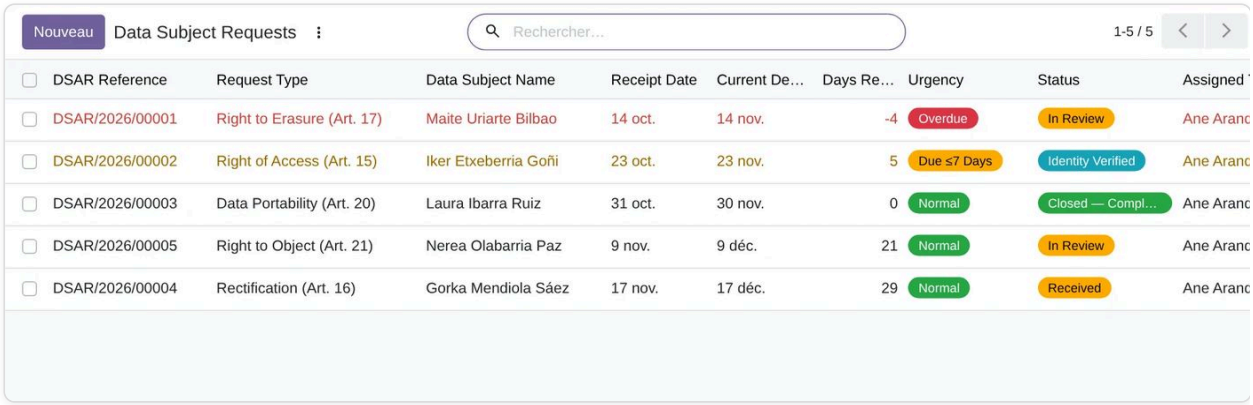
Les filtres de la liste sont **Open**, **Overdue**, celui des demandes qui arrivent à échéance dans sept jours ou moins, **Erasure Requests** et **Access Requests**, avec les regroupements **By Status** et **By Type**. Dans **GDPR Toolkit › Reports** se trouve le **DSAR History Report**.

Le seul courriel envoyé automatiquement à la personne concernée est l'accusé de réception d'une demande faite sur le portail. La lettre de réponse n'est pas envoyée depuis le module : vous la rédigez ici et l'envoyez vous-même par le canal de votre choix.

Un exemple de bout en bout

1 La demande arrive

Maite Uriarte Bilbao demande l'effacement de ses données. Odoo fixe le **Response Deadline** un mois après la **Receipt Date**.



- **Capture réelle d'Odoo 20.** La liste avec la demande d'effacement, la demande d'accès, la demande de portabilité et deux autres.

2 Le délai est dépassé

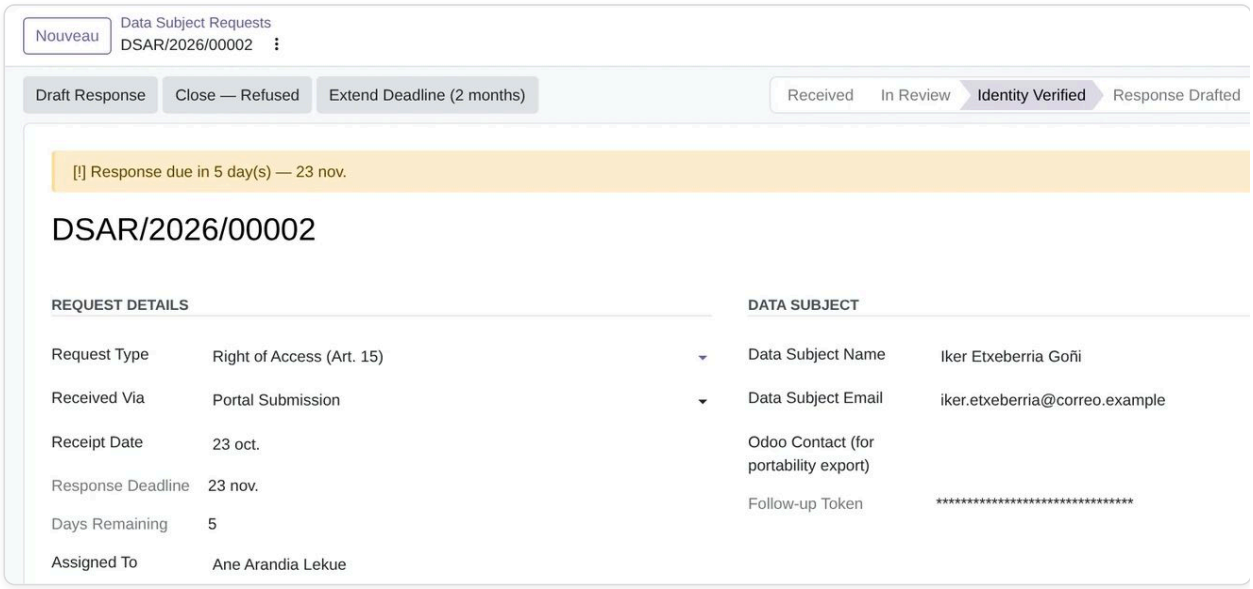
Personne ne l'a clôturée et le délai est déjà passé : **Days Remaining** affiche -4, la fiche signale qu'elle est hors délai et la demande apparaît dans **Overdue**.



- **Capture réelle d'Odoo 20.** La liste des demandes hors délai, avec une seule demande.

3 Une autre demande approche de l'échéance

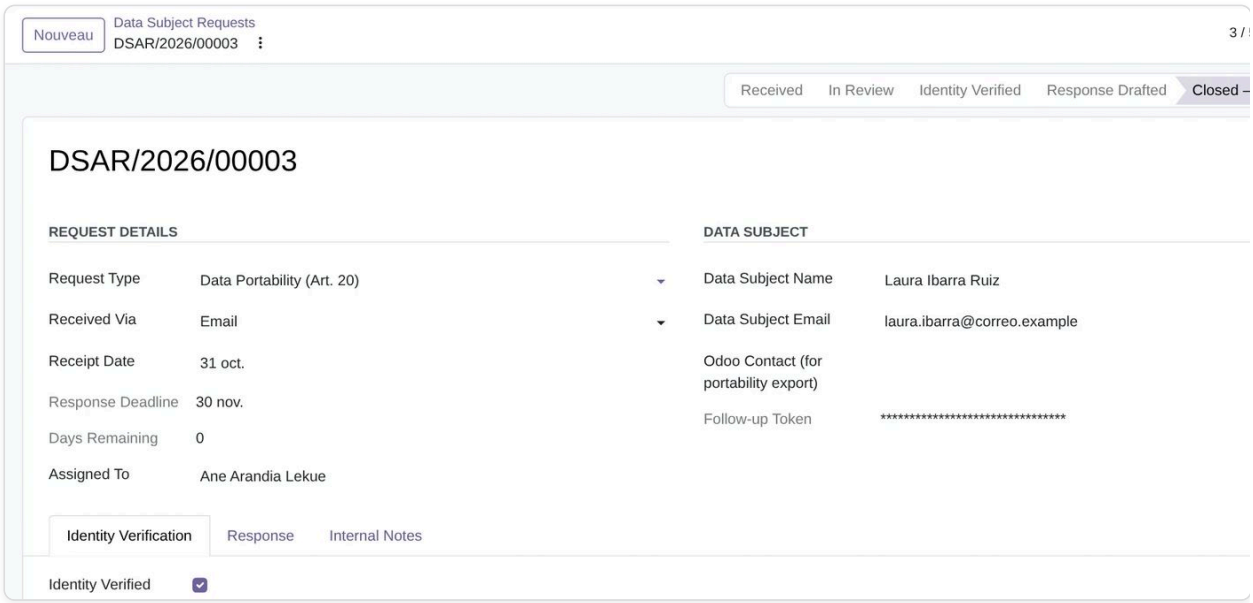
Iker Etxeberria Goñi a demandé l'accès à ses données. Il lui reste 5 jours et son identité est vérifiée : elle apparaît dans **Due This Week**.



- **Capture réelle d'Odoo 20.** Une demande échéant dans 5 jours, avec l'identité vérifiée.

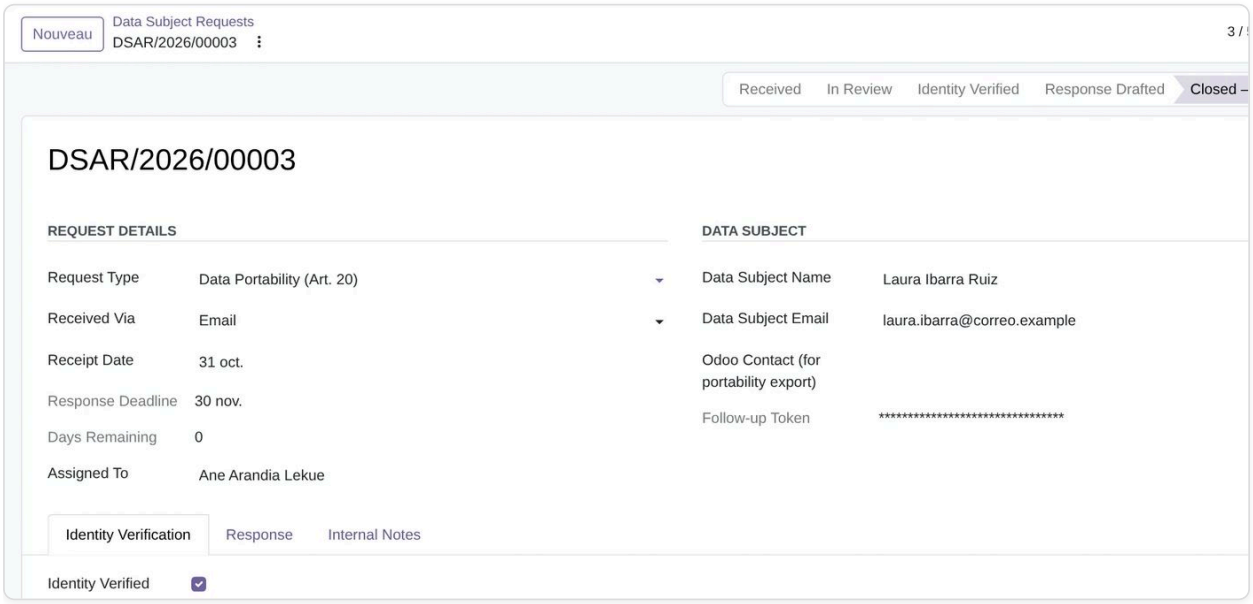
4 Elle est clôturée

La demande de portabilité de Laura Ibarra Ruiz a son identité vérifiée et est clôturée comme terminée.



- **Capture réelle d'Odoo 20.** Une demande de portabilité clôturée comme terminée.

9 Portabilité, effacement et portail de confidentialité



- **Capture réelle d'Odoo 20.** Une demande de portabilité avec l'identité vérifiée, déjà clôturée comme terminée.

Export de portabilité

L'export se génère manuellement depuis la demande, à l'aide d'un assistant. Aucune tâche planifiée ne le prépare. Deux conditions sont requises : l'identité vérifiée et un contact Odoo lié à la demande.

DSAR	La demande dont sont extraites les données. Obligatoire.
Contact Data (res.partner)	Case cochée par défaut. Inclut les données de la fiche du contact.
Order History (sale.order)	Inclut les commandes du contact. Seulement si l'application Ventes est installée.
HR Data (hr.employee)	Inclut la fiche employé. Seulement si l'application Employés est installée.
I confirm explicit HR data inclusion	Case de confirmation à cocher avec les données RH.
Export Format	Deux options : **JSON (machine-readable)** ou **CSV**.
Export File	Le fichier généré, une fois l'export prêt.
Generate Export	Crée le fichier. Le bouton disparaît une fois l'export réalisé.
Close	Ferme l'assistant.

Vérification des conflits d'effacement

Pour une demande d'effacement, **Retention Conflict Check** compte les données du contact : factures validées, fiches employé et commandes de vente, selon les applications installées. L'assistant affiche les groupes **Data Subject**, **Conflict Findings** et **Your Decision per Category**. Pour chaque catégorie, vous choisissez **Retain (legal obligation)** ou **Erase / Anonymise**. La catégorie marketing et consentement est définie par défaut sur **Erase / Anonymise**.

Record Decision & Close DSAR enregistre la décision dans les notes internes et clôture la demande : comme terminée si tout est effacé, et avec effacement partiel si une catégorie est conservée. **Cancel** quitte sans rien enregistrer.

Portail de confidentialité

Le portail se trouve à /my/privacy-rights de votre Odoo et exige une connexion : la personne concernée a donc besoin d'un compte portail. Le module n'ajoute aucun lien dans Mon compte : c'est à vous de lui communiquer l'adresse. Le formulaire demande le type de droit, un texte de 2 000 caractères maximum et jusqu'à 3 documents de 50 Mo chacun. À l'envoi, un accusé de réception est envoyé par courriel, ainsi qu'une page de suivi avec un lien dédié, qui affiche le type et le statut sans données personnelles.

> Le module n'efface ni n'anonymise aucune donnée : la vérification d'effacement se contente de compter les données et d'enregistrer votre décision. L'effacement ou l'anonymisation se font manuellement dans Odoo. Le module n'envoie pas non plus la lettre de réponse.

Ce qui se passe lors de l'export de portabilité

Le droit à la portabilité est celui de l'art. 20.1 du RGPD : recevoir les données que la personne concernée a fournies, dans un format structuré, couramment utilisé et lisible par machine. C'est pourquoi l'assistant propose JSON ou CSV.

L'assistant refuse de générer l'export dans trois cas :

- Si l'identité n'est pas vérifiée : « Identity must be verified before generating a portability export. »
- Si la demande n'a pas de contact Odoo : « No Odoo contact linked to this DSAR. Please link a res.partner record first. » Liez-le dans le champ **Odoo Contact (for portability export)** de la demande.
- Si les données du contact ont déjà été anonymisées, l'assistant indique que les données de la personne concernée ont déjà été anonymisées, qu'un traitement manuel est nécessaire et qu'il faut contacter le DPO.

Les données de contact sont cochées par défaut. Les commandes ne sont incluses que si l'application Ventes est installée : jusqu'à 500, de la société de la demande. Les données RH ne sont incluses que si l'application Employés est installée et que la case de confirmation est cochée : la fiche employé de cette personne, avec son poste, son service et ses coordonnées privées.

Fin de l'export

Une fois généré, l'assistant indique que le fichier est prêt et joint à la demande, et affiche le **Export File**. Le fichier figure aussi dans l'onglet **Response** de la demande.

Statuts de la demande et délais

Le délai de réponse est d'un mois à compter de la réception de la demande, prolongeable de deux mois si nécessaire ; la prolongation et ses motifs doivent être communiqués à la personne concernée dans ce premier mois (art. 12.3). Le module n'envoie pas cet avis : c'est à vous de le faire, avant la **Extension Notification Due**.

Extend Deadline (2 months) exige un motif et ne modifie pas le statut de la demande : seul le **Current Deadline** passe à la date prolongée. Aucun bouton ne permet d'aller directement à l'état « clôturée avec délai prolongé ».

Règles de la vérification d'effacement

L'assistant ne s'ouvre que pour les demandes d'effacement et examine le contact Odoo lié à la demande ; sans contact, il n'a rien à compter. Il compte les factures validées, les fiches employé et les commandes de vente de ce contact. Les deux derniers groupes dépendent des applications Employés et Ventes. Chaque groupe a sa propre case d'alerte : **Pending / Recent Invoices Found**, **Active HR Records Found** et **Active Orders Found**. Le **Conflict Summary** présente le décompte sous forme de texte.

Les décisions se prennent par groupe : **Invoice Data Decision**, **HR Data Decision**, **Order Data Decision** et **Marketing / Consent Data Decision**. Pour les trois premiers, vous choisissez entre **Retain (legal obligation)** et **Erase / Anonymise** ; pour le marketing, entre **Retain** et **Erase / Anonymise**.

Lors de l'enregistrement de la décision, la demande est clôturée comme terminée si tout est effacé, et avec effacement partiel si un groupe est conservé. Le module se contente d'inscrire la décision dans les notes internes. Le résumé de l'assistant est en anglais et cite des durées de conservation issues du droit espagnol : vérifiez-les avec votre DPO, car elles ne valent pas pour tous les pays.

Le portail et ses limites

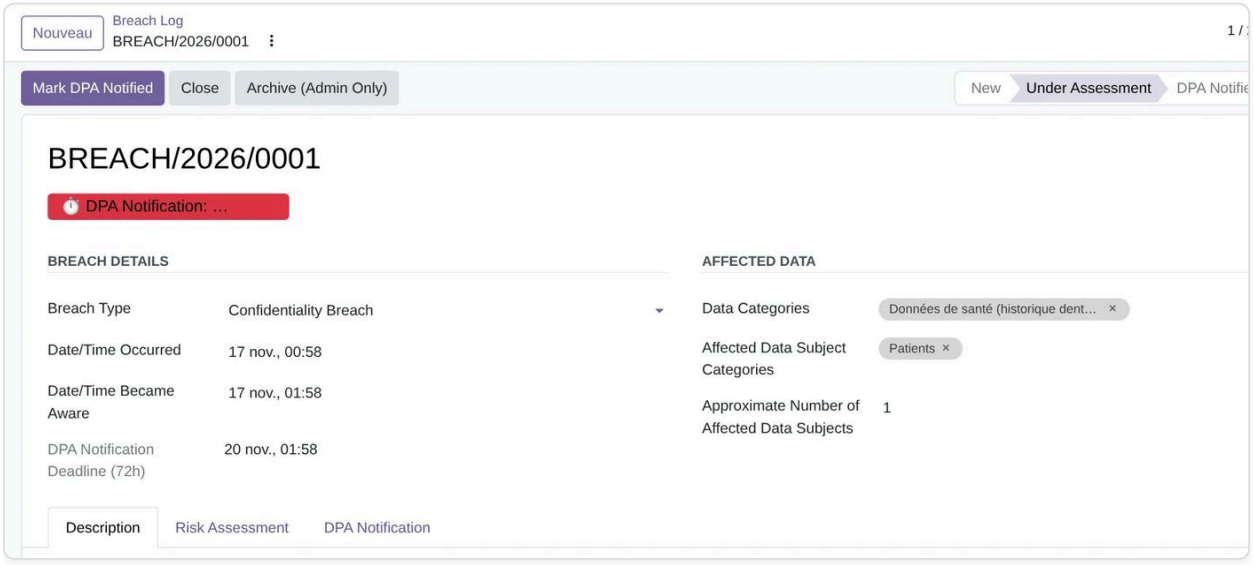
Le portail impose deux limites par personne. Après 3 demandes dans une journée, il n'accepte plus d'envoi avant le lendemain. Après 5 demandes en sept jours, il n'en accepte plus, ajoute un marqueur de révision dans les notes du contact et invite la personne à contacter votre entreprise. Décider si une demande est manifestement infondée ou excessive relève du responsable de traitement (art. 12.5).

La personne qui ouvre le lien de suivi ne voit que le type et le statut de sa demande, sans données personnelles. Le seul courriel envoyé automatiquement à la personne concernée est l'accusé de réception d'une demande faite sur le portail ; la lettre de réponse est rédigée et envoyée par vous.

Un exemple de bout en bout

Laura Ibarra Ruiz a demandé la portabilité de ses données. Sa demande a son identité vérifiée et son contact Odoo lié. Vous ouvrez l'assistant, laissez cochées les données de contact, choisissez JSON et cliquez sur **Generate Export** : le fichier apparaît dans **Export File** et est joint à la demande. Vous lui envoyez ensuite la réponse par votre canal habituel et clôturez la demande comme terminée.

10 Le registre des violations et les 72 heures



- **Capture réelle d'Odoo 20.** Une violation en cours d'évaluation, avec le compte à rebours du délai et le bouton **Mark DPA Notified**.

Les violations se trouvent dans **GDPR Toolkit › Breach Log › All Breaches**. Cliquez sur **Nouveau** pour en ouvrir une. La **Breach Reference** est attribuée par Odoo à la création et ne peut pas être modifiée. Les données se saisissent dans le formulaire. Aucune donnée n'arrive de l'extérieur.

Quoi renseigner

Breach Type	Obligatoire : **Confidentiality Breach**, **Integrity Breach**, **Availability Breach** ou **Multiple Types**.
Date/Time Occurred	Quand la violation s'est produite.
Date/Time Became Aware	Obligatoire. Le délai de notification court à partir de ce moment.
DPA Notification Deadline (72h)	Calculé par Odoo à partir de la date de prise de connaissance.
Breach Description et **Likely Consequences**	Texte libre, dans l'onglet **Description**.
Impact Score et **Likelihood Score**	Dans l'onglet **Risk Assessment**, vous choisissez chacun, de 1 à 5.

Le délai de 72 heures

L'art. 33.1 du RGPD impose de notifier la violation à l'autorité de contrôle dans les meilleurs délais et, si possible, au plus tard 72 heures après en avoir pris connaissance. Le module fixe ce délai de 72 heures à partir de la **Date/Time Became Aware**. À l'ouverture du formulaire, vous voyez le temps restant en heures et minutes ; une fois le délai dépassé, il affiche « EXPIRED ». Le compte à rebours est calculé à l'ouverture et ne se met pas à jour seul à l'écran. La tâche **GDPR: Breach Countdown Alert** s'exécute chaque heure et, dans les 6 dernières heures du délai, envoie un courriel tant que la violation n'est pas marquée comme notifiée : aux **Breach Alert Recipients** ou, à défaut, aux responsables RGPD.

Risque et communication aux personnes concernées

À partir de l'impact et de la probabilité, Odoo calcule le **Risk Score** et le **Risk Level** : faible jusqu'à 4, moyen jusqu'à 9, élevé jusqu'à 19 et critique à partir de 20. Cette matrice est propre au module, et non imposée par le RGPD. Pour un risque élevé ou critique, **Art. 34 Data Subject Notification Required** est marqué. La décision finale appartient au responsable de traitement ou à son DPO, et vous pouvez la consigner dans **DPO Final Art. 34 Determination**.

Statuts et boutons

Start Assessment	Fait passer la violation de **New** à **Under Assessment**.
Mark DPA Notified	Visible uniquement en **Under Assessment**. Passe le statut à **DPA Notified** et enregistre la date et l'heure. Le module ne notifie rien : le moyen, le numéro de référence et les justificatifs se saisissent vous-même dans l'onglet **DPA Notification**.
Mark Data Subjects Notified	Visible uniquement en **DPA Notified** et si la communication de l'art. 34 est obligatoire. Passe en **Data Subjects Notified** et enregistre la date. La communication se fait hors d'Odoo ; le justificatif se joint dans l'onglet **Art. 34 Notification**.
Close	Masqué en **New** et en **Closed**. Avant de clôturer, remplissez l'onglet **Post-Breach Review** : cause racine, actions correctives, mesures préventives, personne qui approuve et date.
Archive (Admin Only)	Visible uniquement par un administrateur Odoo. Ouvre un assistant qui demande le **Archive Reason**.

Les statuts sont **New**, **Under Assessment**, **DPA Notified**, **Data Subjects Notified** et **Closed**.

1. **Créer la violation**
   Cliquez sur **Nouveau**, choisissez le **Breach Type** et renseignez le moment de prise de connaissance.
2. **Évaluer**
   Cliquez sur **Start Assessment** et notez l'impact et la probabilité.
3. **Notifier vous-même et consigner**
   Si cela est approprié, notifiez l'autorité de votre côté puis cliquez sur **Mark DPA Notified**.
4. **Communiquer et clôturer**
   Si c'est obligatoire, informez les personnes concernées de votre côté puis cliquez sur **Mark Data Subjects Notified**. Terminez par la revue post-violation et **Close**.

> Une violation ne peut pas être supprimée : Odoo répond « Breach records are append-only and cannot be deleted. Only an Odoo Administrator can archive a breach record with a written reason. » Seul un administrateur peut l'archiver, et sans motif, le message « Archive reason is required. » s'affiche.

Les statuts, un à un

New	La violation vient d'être enregistrée. Seule l'évaluation peut être lancée.
Under Assessment	L'impact et la probabilité sont notés. Depuis cet écran, la violation peut être marquée comme notifiée à l'autorité.

DPA Notified	Quelqu'un confirme que l'autorité a été notifiée en dehors d'Odoo. Si le niveau de risque impose la communication de l'art. 34, elle peut être marquée comme communiquée aux personnes concernées.
Data Subjects Notified	Il est noté que les personnes concernées ont été informées.
Closed	La violation est terminée et ne peut plus être clôturée à nouveau.

Règles et conditions

- **Start Assessment** n'apparaît que sur **New**.
- **Mark DPA Notified** n'apparaît que sur **Under Assessment**.
- **Mark Data Subjects Notified** n'apparaît que sur **DPA Notified** et seulement si la communication de l'art. 34 est obligatoire.
- **Close** n'apparaît ni sur **New** ni sur **Closed**.
- Les boutons de workflow sont réservés au groupe des gestionnaires du module ; **Archive (Admin Only)** est réservé aux administrateurs Odoo.
- Si un utilisateur sans cette autorisation tente d'archiver, le message « Only Odoo Administrators can archive breach records. » s'affiche.
- L'assistant d'archivage exige le **Archive Reason** ; sans lui, le message « Archive reason is required. » s'affiche.
- L'art. 33.1 demande de notifier dans les 72 heures si possible. Si la notification n'a pas lieu dans ce délai, elle doit être accompagnée des motifs du retard.

Le module change seulement le statut et enregistre la date. Il ne notifie pas l'autorité et n'informe personne : vous le faites vous-même, et ici vous consignez ce que vous avez fait.

La description et les conséquences ne sont enregistrées chiffrées que si le serveur dispose de la clé de chiffrement. Sans elle, elles sont enregistrées non chiffrées, et la configuration l'indique dans **Encryption Key Configured**.

Champs et onglets de l'enregistrement

Breach Details	Type, date de survenance, date de prise de connaissance et délai de notification à l'autorité.
Affected Data	**Categories of Data**, **Affected Data Subject Categories** et **Approximate Number of Affected Data Subjects**.
Description	Description, conséquences et **Measures Taken / Proposed**.
Risk Assessment	Impact, probabilité, score et niveau de risque.
DPA Notification	**DPA Notification Date/Time**, **Notification Method**, **DPA Reference Number** et pièces jointes.
Art. 34 Notification	Si elle a été envoyée, la date et les pièces jointes.
Post-Breach Review	Cause racine, actions correctives, mesures préventives, validateur et date.

Dans la liste, les filtres **High/Critical Risk** et **DPA Notification Pending** permettent de voir ce qui manque. Le menu **Active Incidents** ouvre les violations non clôturées.

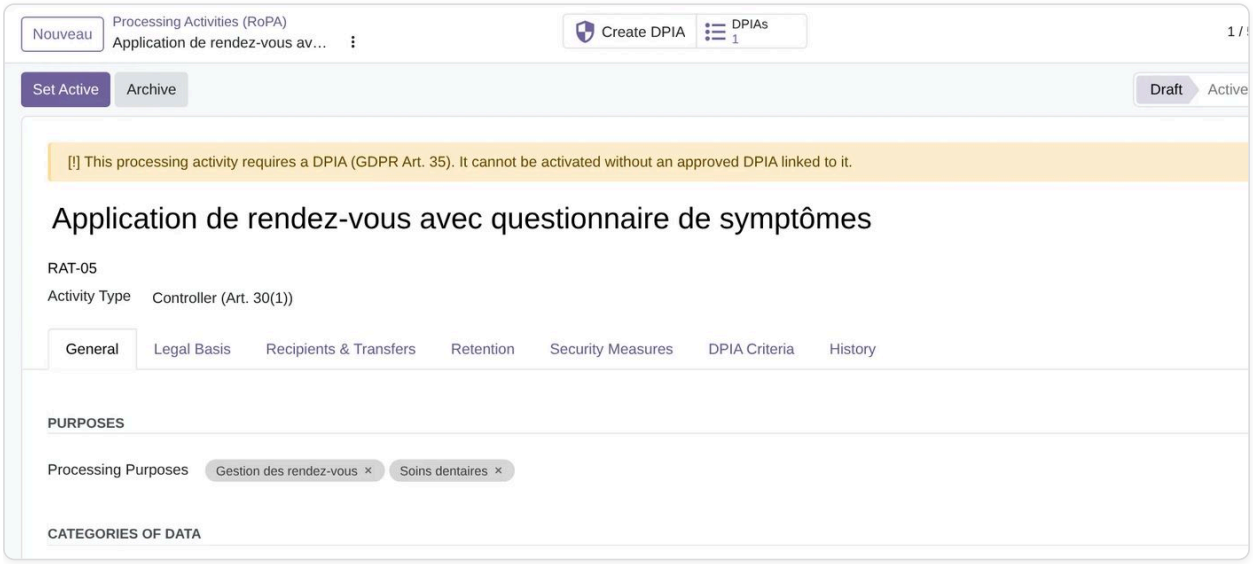
Un exemple de bout en bout

La première violation des écrans est une **Confidentiality Breach** : une radiographie envoyée par courrier au mauvais patient. Elle a été connue une heure après les faits, Odoo a fixé le délai à 72 heures à partir de là et, à l'ouverture, il restait environ 42 heures. Elle concerne des données de santé de patients, a un niveau de risque **Medium**, est **Under Assessment** et affiche le bouton **Mark DPA Notified**. La seconde, une **Availability Breach** due au vol de l'ordinateur portable de l'accueil, avec disque chiffré, a un niveau **Low** et est **Closed** : sur une violation clôturée, seul le bouton **Archive (Admin Only)** reste disponible.

GUIDE DU MODULE · GDPR COMPLIANCE

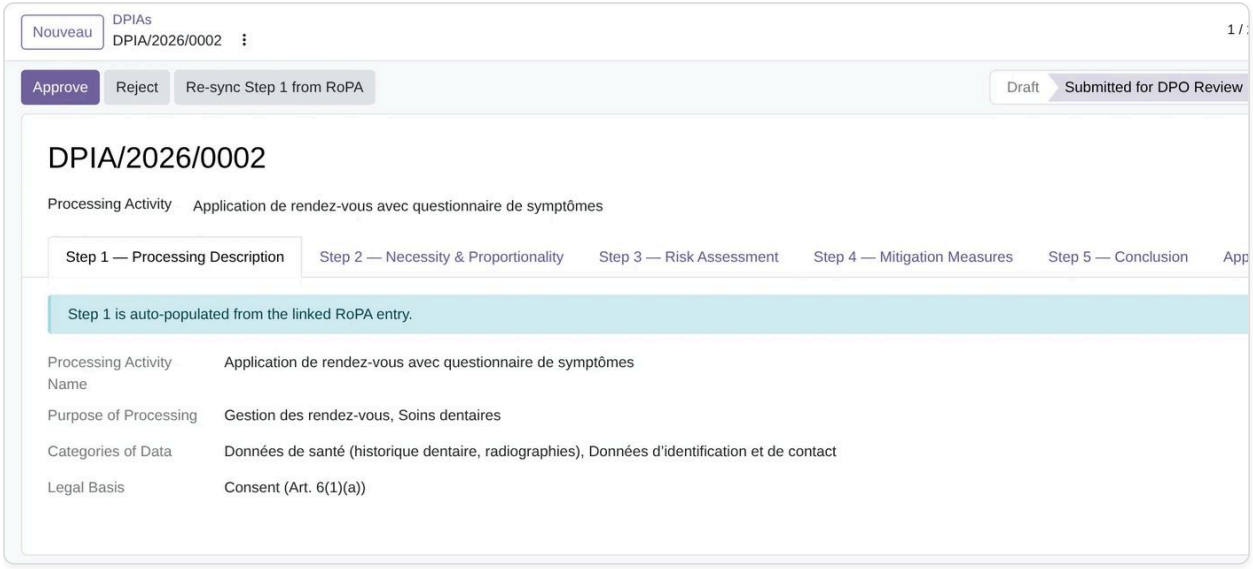
11 Les analyses d'impact (AIPD)

Dans l'onglet **DPIA Criteria** de chaque activité, il y a neuf cases, une par critère des lignes directrices WP248 rev.01. Avec deux critères ou plus cochés, ou avec la marque manuelle, l'activité apparaît avec **DPIA Required**. C'est une règle générale de ces lignes directrices, pas une obligation légale en soi. Les activités marquées se consultent dans **GDPR Toolkit › Processing Activities (RoPA) › DPIA Required**.



- **Capture réelle d'Odoo 20.** Une activité en **Draft** avec l'avertissement qu'elle nécessite une AIPD.

L'évaluation s'ouvre depuis la fiche de l'activité ou depuis **GDPR Toolkit › DPIA › All DPIAs**. La référence est attribuée automatiquement par Odoo à la création de l'enregistrement.



- **Capture réelle d'Odoo 20.** Une AIPD envoyée en revue, avec les onglets des cinq étapes et **Approval**.

Les cinq étapes et l'onglet de validation

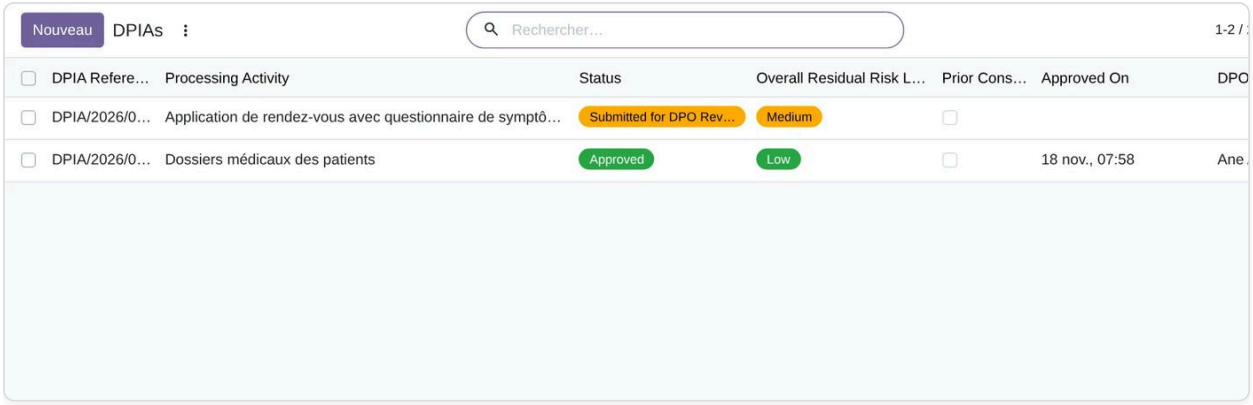
- Étape 1, la description du traitement : le nom, la finalité, les catégories de données et la base juridique de l'art. 6 sont remplis automatiquement à partir de l'activité du RoPA.
- Étape 2, nécessité et proportionnalité : la limitation de la finalité, la minimisation des données, la justification de la durée de conservation et les mesures pour les droits des personnes concernées.
- Étape 3, l'évaluation des risques : la liste des risques identifiés.
- Étape 4, les mesures d'atténuation, en texte libre.
- Étape 5, la conclusion et le risque résiduel.
- L'onglet **Approval** : qui l'a envoyée, qui l'a revue, quand et ses commentaires.

Chaque risque comporte son impact et sa probabilité avant mesures, puis les mêmes deux valeurs résiduelles après application des mesures. Chaque couple donne un score et un niveau : jusqu'à 4 faible, jusqu'à 9 moyen, jusqu'à 19 élevé et à partir de 20 critique. Cette matrice est celle du module, et non du RGPD ni des lignes directrices du Comité européen. Avec un risque résiduel élevé ou critique, **Prior Consultation Required (Art. 36)** est coché automatiquement. Si vous présentez la consultation préalable, consignez ici ce que vous avez fait dans **Prior Consultation Submitted** et **Prior Consultation Notes**. Le module ne la présente pas à l'autorité.

Boutons de l'enregistrement

Submit for DPO Review	Fait passer l'AIPD de **Draft** à **Submitted for DPO Review**. N'apparaît que sur **Draft**.
Approve	Valide l'AIPD. N'apparaît que sur **Submitted for DPO Review**.
Reject	Rejette l'AIPD. N'apparaît que sur **Submitted for DPO Review** et demande les commentaires du DPO.
Reset to Draft	Si une AIPD est en **Rejected**, vous la renvoyez en **Draft**.
Re-sync Step 1 from RoPA	Recopie l'étape 1 depuis l'activité du RoPA.

Les statuts sont **Draft**, **Submitted for DPO Review**, **Approved** et **Rejected**. Les AIPD en attente de revue se trouvent dans **GDPR Toolkit › DPIA › Awaiting DPO Review**.



- **Capture réelle d'Odoo 20.** La liste des AIPD avec leur statut et leur niveau global de risque résiduel.

> Envoyer, valider et rejeter ne peuvent être faits que par les gestionnaires RGPD. La décision finale appartient au responsable de traitement ou à son DPO. Le module ne présente pas la consultation préalable à l'autorité et ne constitue pas un avis juridique.

> Une activité nécessitant une AIPD ne s'active pas sans AIPD validée liée : la fiche de l'activité le signale à l'écran.

Statuts de l'AIPD

STATUT	SIGNIFICATION
Draft	C'est le statut initial : les étapes se remplissent et le bouton **Submit for DPO Review** est visible.
Submitted for DPO Review	L'AIPD attend la décision du DPO. Dans ce statut, les boutons **Approve** et **Reject** sont visibles.
Approved	Le DPO l'a validée, et sa date figure dans **Approved On**.
Rejected	Le DPO l'a rejetée avec ses commentaires. Le bouton **Reset to Draft** la remet en **Draft**.

Quand le module ne laisse pas faire

- Seuls les gestionnaires RGPD peuvent soumettre, approuver et rejeter. Si vous n'en êtes pas un, un de ces messages s'affiche, selon le bouton : « Only GDPR Managers can submit a DPIA for review. », « Only GDPR Managers (acting as DPO) can approve a DPIA. » ou « Only GDPR Managers (acting as DPO) can reject a DPIA. ».
- Rejeter sans rien saisir dans **DPO Comments** affiche le message « DPO comments are required when rejecting a DPIA. ».
- **Reset to Draft** n'apparaît que lorsque l'AIPD est **Rejected**.

Champs et onglets de l'enregistrement

DPIA Reference	Odoo la génère à la création de l'enregistrement, et elle ne peut pas être modifiée.
Processing Activity	L'activité du RoPA à laquelle l'AIPD se rattache. Obligatoire.
Overall Residual Risk Level	Odoo le calcule : c'est le plus élevé des risques résiduels de la liste.

Submitted By et **Submitted On**	Qui a envoyé l'AIPD en revue et quand.
DPO Reviewer et **DPO Review Date**	Qui l'a revue et quand.
DPO Comments	Le texte de la revue. Obligatoire pour un rejet.
Prior Consultation Submitted et **Prior Consultation Notes**	Ce que vous consignez si vous avez présenté la consultation préalable de l'art. 36. Le module ne la présente pas.

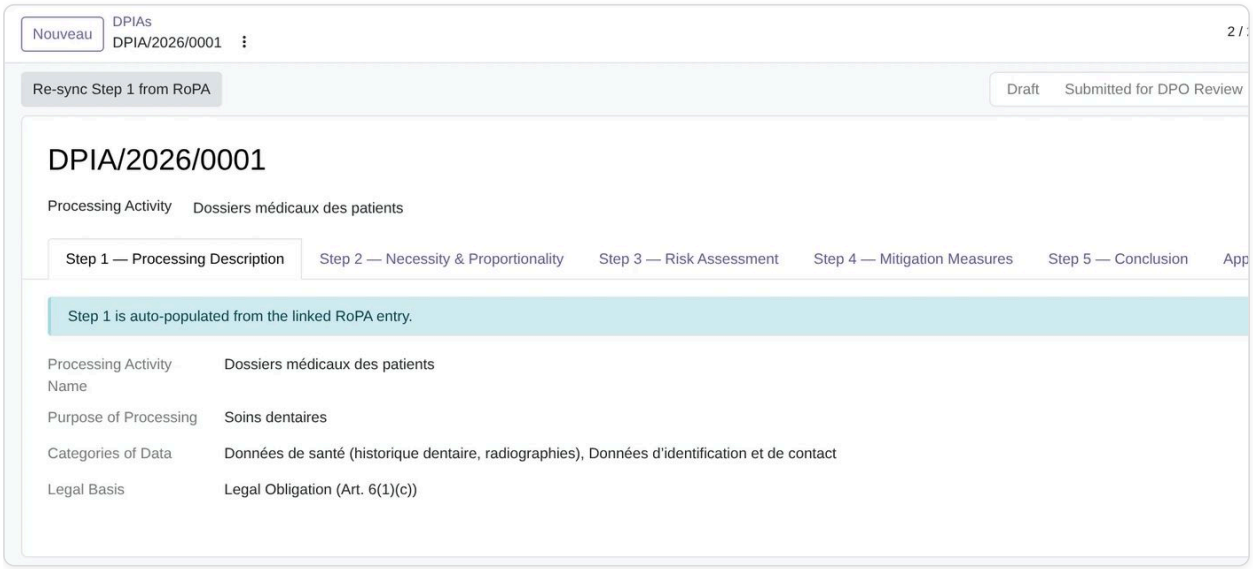
La vue comporte six onglets : les cinq étapes et **Approval**. Chaque étape contient ses textes, et **Re-sync Step 1 from RoPA** sert à mettre à jour l'étape 1 si vous modifiez l'activité. Les filtres sont **Awaiting DPO Review**, **Approved** et **High/Critical Residual Risk**, avec les regroupements **By Status** et **By Risk Level**.

Comment le risque est calculé

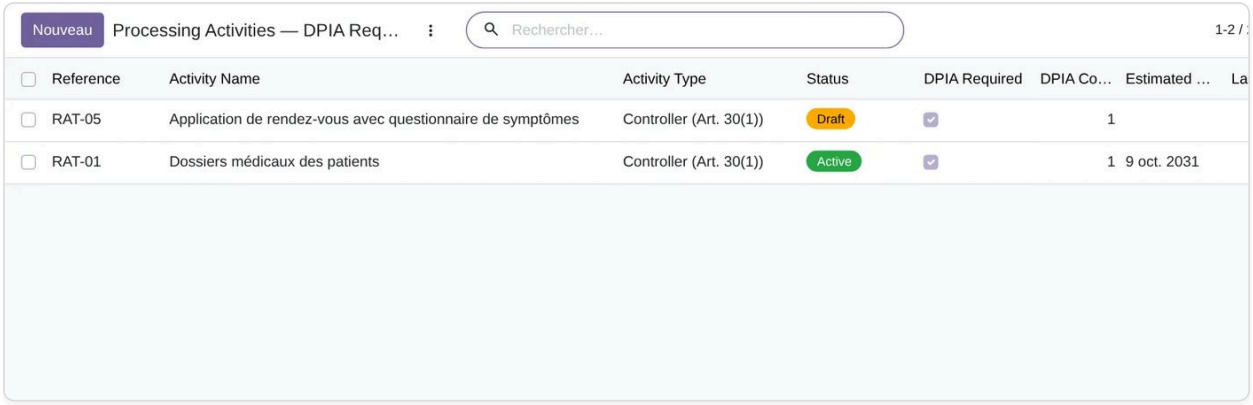
Chaque risque note son impact de insignifiant (1) à catastrophique (5) et sa probabilité de très faible (1) à très élevée (5). Les deux valeurs sont multipliées et donnent un score de 1 à 25. Jusqu'à 4 c'est **Low**, jusqu'à 9 c'est **Medium**, jusqu'à 19 c'est **High** et à partir de 20 c'est **Critical**. Après mesures, le calcul est répété avec l'impact résiduel et la probabilité résiduelle. Ces seuils sont ceux du module. Avec un risque résiduel élevé ou critique, la consultation préalable de l'art. 36.1 est signalée : elle demande de consulter l'autorité avant le traitement lorsque l'évaluation montre qu'il présenterait un risque élevé en l'absence de mesures d'atténuation.

Un exemple de bout en bout

Dans l'exemple des écrans, l'activité RAT-05, l'application de prise de rendez-vous en ligne avec questionnaire de symptômes, est en **Draft** et porte la mention **DPIA Required**. Sa fiche indique qu'elle ne peut pas être activée sans AIPD validée. Depuis là, l'AIPD est créée sous le numéro DPIA/2026/0002, et l'étape 1 reprend déjà la finalité, les catégories de données et la base juridique de l'activité. Après avoir rempli les autres étapes, elle est envoyée en revue et apparaît dans la liste en **Submitted for DPO Review** avec un risque résiduel **Medium**. Le DPO la verra dans **Awaiting DPO Review** et l'approuvera ou la rejettera avec ses commentaires. Tant qu'elle n'est pas validée, l'activité reste en **Draft**.



- **Capture réelle d'Odoo 20.** L'AIPD du dossier médical des patients, avec le statut **Approved**.

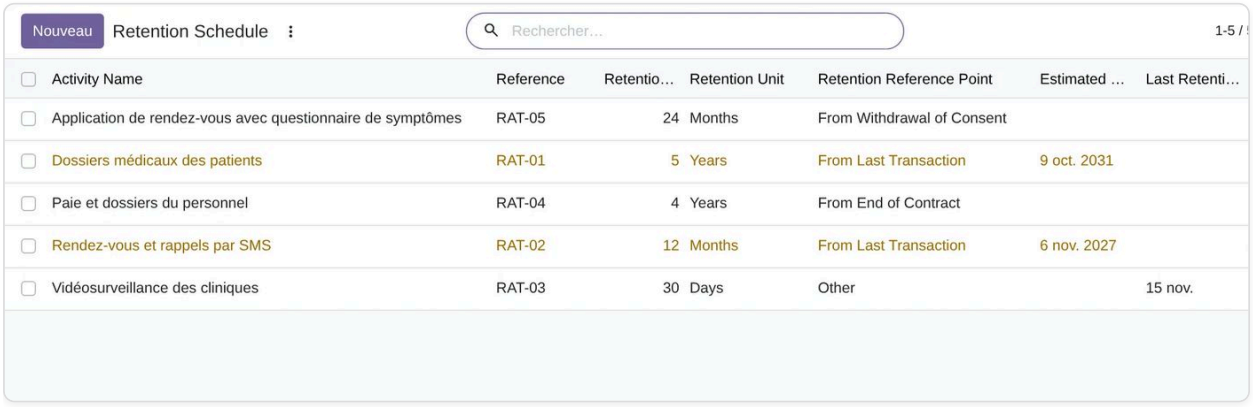


- **Capture réelle d'Odoo 20.** Les activités avec **DPIA Required** et leur numéro d'AIPD.

> Ce que ce module ne fait pas : il ne présente pas la consultation préalable à l'autorité et ne décide pas à votre place si l'évaluation est acceptable. La décision finale appartient au responsable de traitement ou à son DPO, et ceci n'est pas un avis juridique.

GUIDE DU MODULE · GDPR COMPLIANCE

12 La conservation et ses révisions



- **Capture réelle d'Odoo 20.** Le **Retention Schedule** avec les cinq activités du registre.

La durée de chaque activité (durée, unité et point de départ du calcul) se renseigne dans l'onglet **Retention** de l'activité, dans **GDPR Toolkit › Processing Activities (RoPA) › All Activities**. Odoo calcule l'**Estimated Retention End Date** uniquement lorsque le point de départ du calcul est **Fixed Date** ou **From Last Transaction** et que cette date est renseignée. Avec **From End of Contract**, **From Withdrawal of Consent** ou **Other**, le champ reste vide et cette activité ne reçoit aucun rappel. Le **Retention Schedule** affiche les activités dont la durée est renseignée, leur date estimée et leur **Last Retention Review**, qui se met à jour automatiquement à chaque révision que vous enregistrez.

Le rappel est envoyé par la tâche planifiée **GDPR: Retention Expiry Check**, chaque jour. Pour chaque activité active dont la date estimée tombe dans les jours de **Retention Advance Warning (days)** et qui n'a pas été révisée au cours des 30 derniers jours, elle crée une activité de rappel sur la fiche et envoie un e-mail aux destinataires des alertes définis dans la configuration ou, à défaut, aux gestionnaires RGPD. Une autre tâche, **GDPR: Annual RoPA Review Reminder**, rappelle une fois par an qu'il faut relire le registre des activités.

Où enregistrer une révision

Les révisions se consultent dans **GDPR Toolkit › Retention Management › Review History**, qui ouvre la liste **Retention Review History**. Chaque révision se crée avec **Nouveau** et comporte les champs suivants :

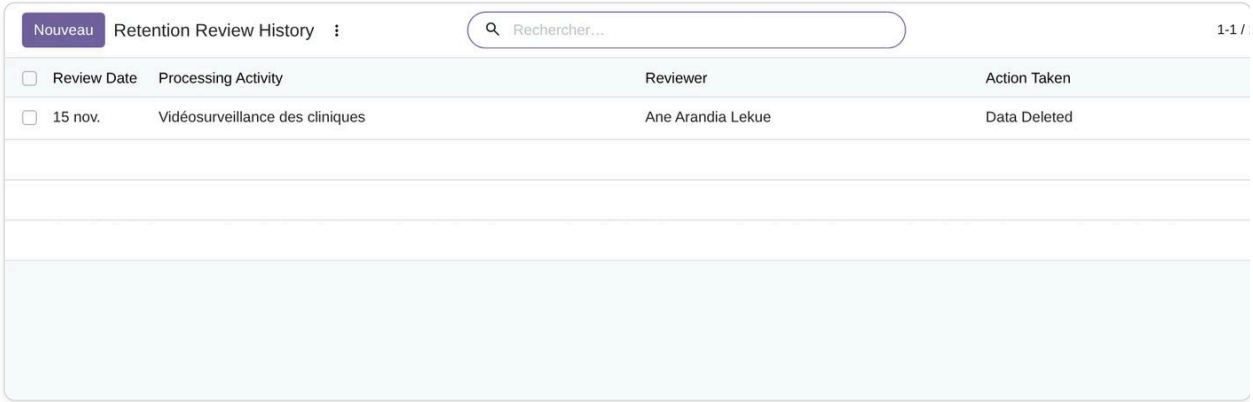
Processing Activity	L'activité que vous révisez. Champ obligatoire.
Review Date	Pré-remplie avec la date du jour. Champ obligatoire.
Reviewer	Pré-rempli avec votre utilisateur. Champ obligatoire.
Action Taken	Ce que vous avez fait à la suite de la révision. Champ obligatoire. Quatre options : **Data Deleted**, **Data Anonymised**, **Retention Extended** et celle de révisé sans action requise.
Extension Justification	Le motif de la prolongation de la conservation.
New Retention End Date	La date jusqu'à laquelle vous prolongez la conservation.
Notes	Texte libre.

L'enregistrement de révision n'a ni boutons ni statuts propres. Les options de **Action Taken** sont ce que vous consignez, et non un statut de l'enregistrement.

Comment enregistrer une révision

1 Ouvrir l'historique

Accédez à **GDPR Toolkit › Retention Management › Review History** et cliquez sur **Nouveau**.



- **Capture réelle d'Odoo 20.** La **Retention Review History** avec une révision déjà enregistrée.

2 Choisir l'activité

Renseignez **Processing Activity**. La date du jour et votre utilisateur sont déjà renseignés.

3 Indiquer l'action

Choisissez dans **Action Taken** ce que vous avez fait des données.

4 Si vous prolongez la conservation

Avec **Retention Extended**, renseignez **Extension Justification** et **New Retention End Date**.

5 Enregistrer

À l'enregistrement, la **Last Retention Review** de l'activité devient la date de cette révision.

> Le module ne supprime ni n'anonymise aucune donnée. Les options **Data Deleted** et **Data Anonymised** se contentent de consigner ce que vous avez fait en dehors de cet écran. Avec **Retention Extended**, Odoo ne vous laisse pas enregistrer s'il manque la justification (« Extension justification is required when extending retention. ») ou la nouvelle date (« New retention end date is required when extending retention. »). La **New Retention End Date** est conservée dans la révision, mais ne modifie pas la date estimée de l'activité : pour la déplacer, changez le délai ou sa date de référence dans l'onglet **Retention**.

Ce que conserve une révision

Chaque révision relie une activité de traitement à la date à laquelle vous l'avez révisée, à la personne qui l'a fait et à la décision prise. La société est copiée automatiquement depuis l'activité. Elle ne garde que ce que vous avez décidé et fait : le module ne supprime ni ne modifie aucune donnée.

Les quatre actions possibles

Data Deleted	Vous consignez qu'après révision, les données ont été supprimées. La suppression se fait par vos soins en dehors du module.
Data Anonymised	Vous consignez que les données ont été anonymisées. L'anonymisation se fait par vos soins en dehors du module.
Retention Extended	Vous décidez de continuer à conserver les données. Une justification et une nouvelle date limite sont requises ; cette date reste dans la révision et la date estimée de l'activité ne change pas.
L'option de révisé sans action	Vous avez révisé l'activité et aucune action n'est nécessaire. C'est la quatrième option de la liste **Action Taken**.

Règles et conditions

- Avec **Retention Extended** et sans **Extension Justification**, Odoo n'enregistre pas et affiche « Extension justification is required when extending retention. ».
- Avec **Retention Extended** et sans **New Retention End Date**, Odoo n'enregistre pas et affiche « New retention end date is required when extending retention. ».
- Avec les trois autres actions, ces deux champs ne sont pas exigés.
- **Processing Activity**, **Review Date**, **Reviewer** et **Action Taken** sont obligatoires.

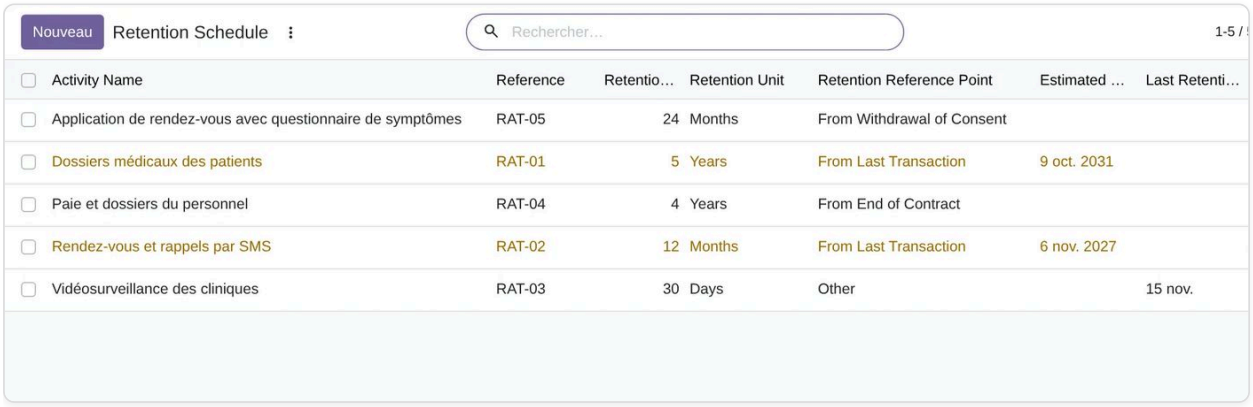
Chaque révision enregistrée met à jour la **Last Retention Review** de l'activité avec la **Review Date** de cette révision. Elle apparaît dans les colonnes du **Retention Schedule** et dans la liste des **Processing Activities (RoPA)**.

Les rappels

La tâche **GDPR: Retention Expiry Check** s'exécute chaque jour. Elle signale les activités actives dont la date estimée de fin tombe dans les jours de **Retention Advance Warning (days)** (30 par défaut) et qui n'ont pas été révisées au cours des 30 derniers jours : elle crée une activité de rappel sur la fiche et envoie un e-mail. Une activité sans date estimée ne reçoit aucun rappel. La tâche **GDPR: Annual RoPA Review Reminder** rappelle une fois par an qu'il faut réviser le registre des activités.

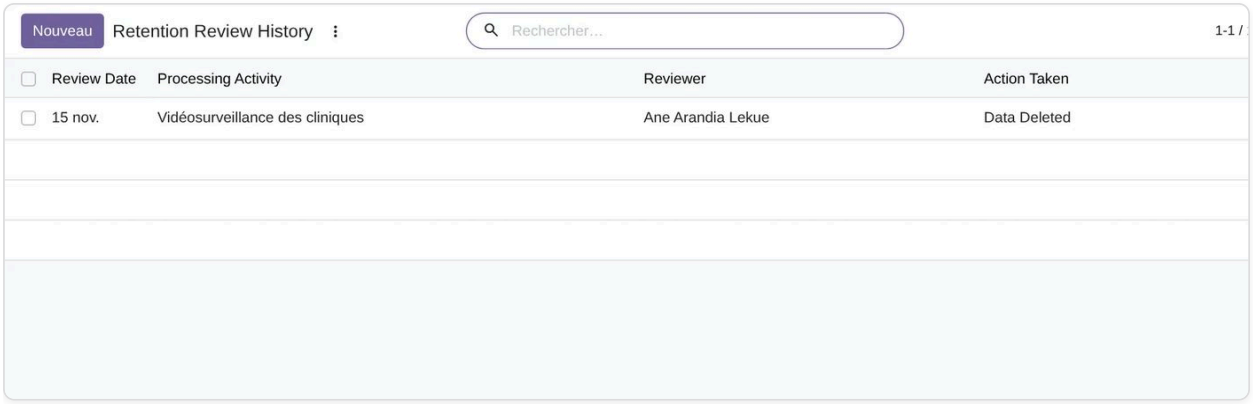
Un exemple de bout en bout

Le **Retention Schedule** de l'exemple comporte cinq activités. Le dossier médical des patients est conservé 5 ans à compter de la dernière transaction, et les rendez-vous et rappels SMS 12 mois : ces deux activités ont une date estimée de fin. La vidéosurveillance des cliniques (30 jours, avec un point de départ **Other**), les bulletins de paie (4 ans à compter de la fin du contrat) et l'application de prise de rendez-vous en ligne (24 mois à compter du retrait du consentement) n'en ont pas, car leur point de départ n'est pas une date qu'Odoo connaît.



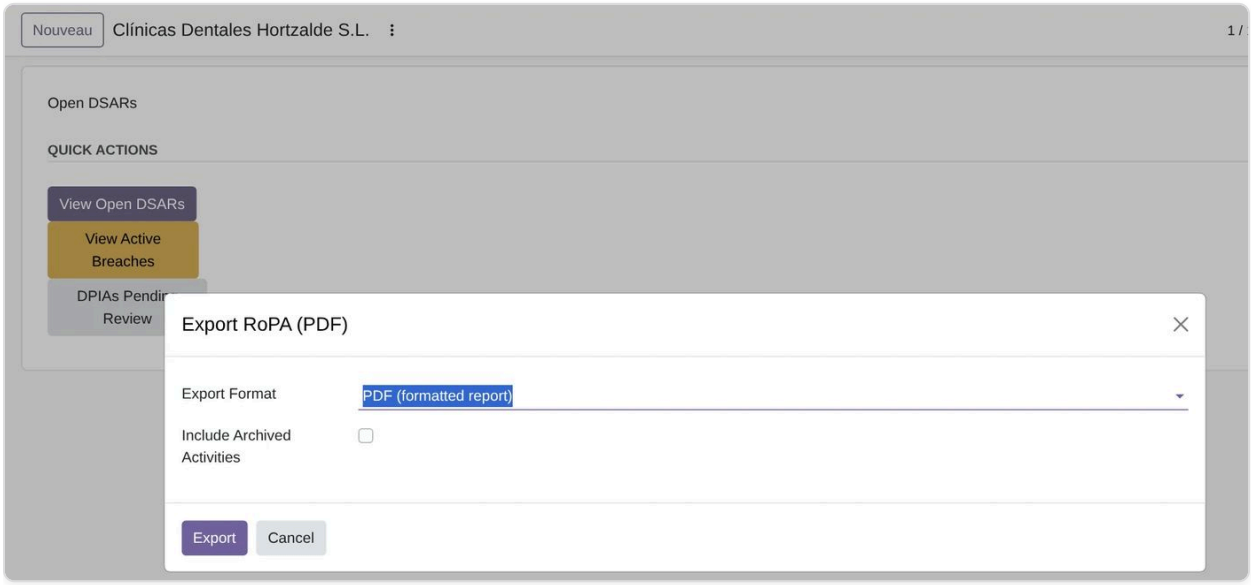
- **Capture réelle d'Odoo 20.** Le **Retention Schedule** avec les cinq activités et leurs dates estimées.

Dans la **Retention Review History** figure une révision de la vidéosurveillance des cliniques, faite par Ane Arandia Lekue, avec l'action **Data Deleted**. Elle ne comporte pas de nouvelle date limite, car cette action n'en demande pas. Dans le calendrier, cette date devient la dernière révision de l'activité.



- **Capture réelle d'Odoo 20.** La **Retention Review History** avec la révision de la vidéosurveillance.

13 Rapports, exports et journal d'audit



- **Capture réelle d'Odoo 20.** L'assistant d'export du RoPA, avec le format et la case des activités archivées.

Exporter le RoPA

1. **Ouvrir le menu d'export**
   Accédez à **GDPR Toolkit › Reports › Export RoPA (PDF)** ou à **GDPR Toolkit › Reports › Export RoPA (Excel)**. Les deux ouvrent le même assistant.

2. **Choisir le format**
   Dans **Export Format**, choisissez **PDF (formatted report)** ou **Excel (.xlsx)**. Le format du menu utilisé est présélectionné.

3. **Décider pour les archivées**
   Cochez **Include Archived Activities** si vous les voulez dans le rapport. Sans cette case, les activités archivées ne figurent pas.

4. **Cliquer sur Export**
   Le fichier est généré. **Cancel** ferme l'assistant sans rien générer.

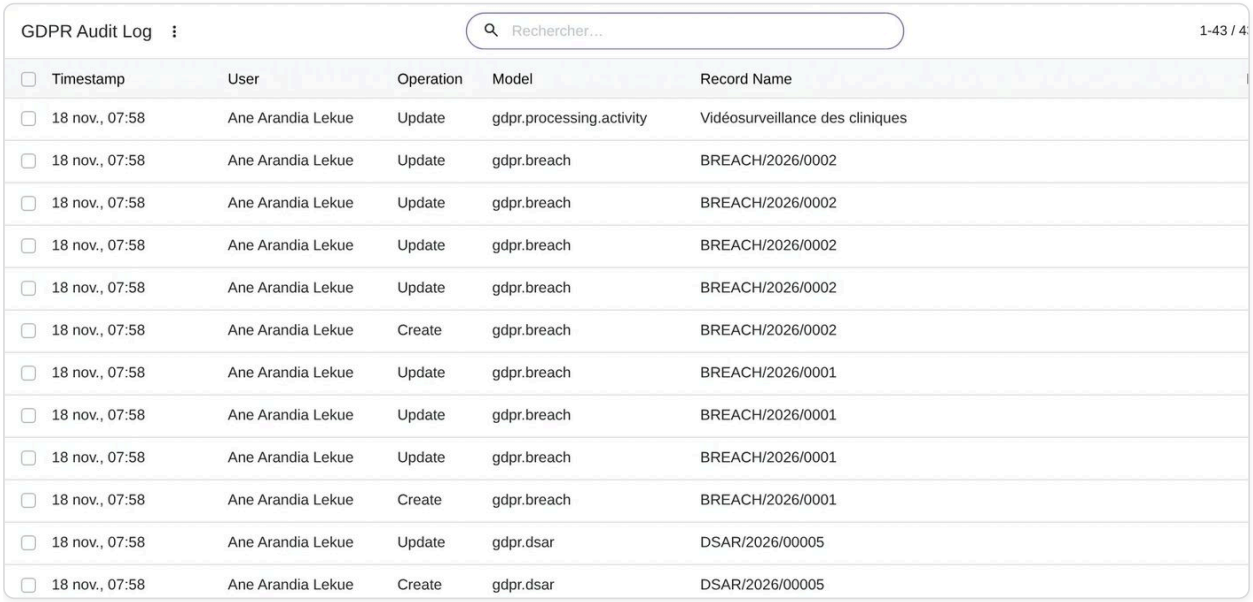
Le fichier Excel comporte une ligne par activité. Les en-têtes de colonnes sont en anglais dans toutes les langues.

- Si votre société n'a aucune activité de traitement, l'assistant le signale avec « No processing activities found for this company. ».
- Si la bibliothèque Excel est absente du serveur, il le signale avec « openpyxl is not installed. Please install it via pip to use Excel export. ». Elle doit être installée sur le serveur.

Autres rapports

Dans le même menu **Reports**, **DSAR History Report** ouvre la liste de toutes les demandes, **Breach Log Report** celle des violations et **DPIA Status Report** celle des AIPD, pour les filtrer, les regrouper ou les exporter. Chaque demande, violation, AIPD et activité s'imprime en PDF depuis sa fiche.

Journal d'audit



- **Capture réelle d'Odoo 20.** Le **GDPR Audit Log** affiche la date et l'heure, l'utilisateur, l'opération, le modèle, le nom de l'enregistrement et l'adresse IP.

Chaque entrée enregistre qui a fait la modification, quand, sur quel enregistrement et depuis quelle adresse IP. Le résumé des modifications masque les champs contenant des données personnelles. Les opérations consignées sont **Create**, **Update**, **Archive**, **Export** et **Portal Submission**.

Create Operations	Filtre qui ne conserve que les créations.
Updates	Filtre qui ne conserve que les modifications.
Exports	Filtre qui ne conserve que les exports.
By User	Regroupe les entrées par utilisateur.
By Model	Regroupe les entrées par modèle.
Change Summary	Sur la fiche de chaque entrée : les champs modifiés, les données personnelles étant barrées.

> Personne ne peut modifier ni supprimer d'entrées du journal d'audit, pas même un administrateur. Odoo le signale avec « You do not have access rights to modify GDPR Audit Log records. Audit log entries are immutable compliance records. » ou avec « You do not have access rights to delete GDPR Audit Log records. They are permanent compliance records per Art. 5(2) GDPR accountability principle. ».

Options de l'assistant d'export

PDF (formatted report)	Rapport mis en forme, prêt à être lu ou imprimé. Présélectionné si vous passez par **Export RoPA (PDF)**.
Excel (.xlsx)	Feuille de calcul avec une ligne par activité, à filtrer et trier à votre convenance.
Include Archived Activities	Case décochée par défaut. Cochée, les activités archivées entrent dans le rapport.

Les deux menus d'export ouvrent le même assistant.

Cas où l'export est refusé

- Sans activités de traitement dans votre société, l'assistant le signale avec « No processing activities found for this company. » et ne génère rien.
- Sans la bibliothèque Excel sur le serveur, l'export Excel échoue avec « openpyxl is not installed. Please install it via pip to use Excel export. ».

Opérations du journal d'audit

OPÉRATION	CE QUI EST ENREGISTRÉ
Create	Une création d'enregistrement.
Update	Une modification d'un enregistrement existant.
Archive	L'archivage d'un enregistrement.
Exporter	L'export du RoPA en Excel ou celui de la portabilité.
Portal Submission	Une demande envoyée depuis le portail de confidentialité.

Champs de l'entrée

Timestamp	Quand l'action a été effectuée. Ce champ se remplit automatiquement.
User	Qui l'a effectuée.
Operation	L'une des cinq opérations ci-dessus.
Model et **Record Name**	Le type d'enregistrement modifié et son nom.
Record ID	Identifiant numérique de l'enregistrement modifié.
L'adresse IP	D'où l'action a été effectuée.
Change Summary	Noms des champs modifiés et leurs valeurs. Les champs contenant des données personnelles sont masqués.
Company	La société à laquelle appartient l'entrée.

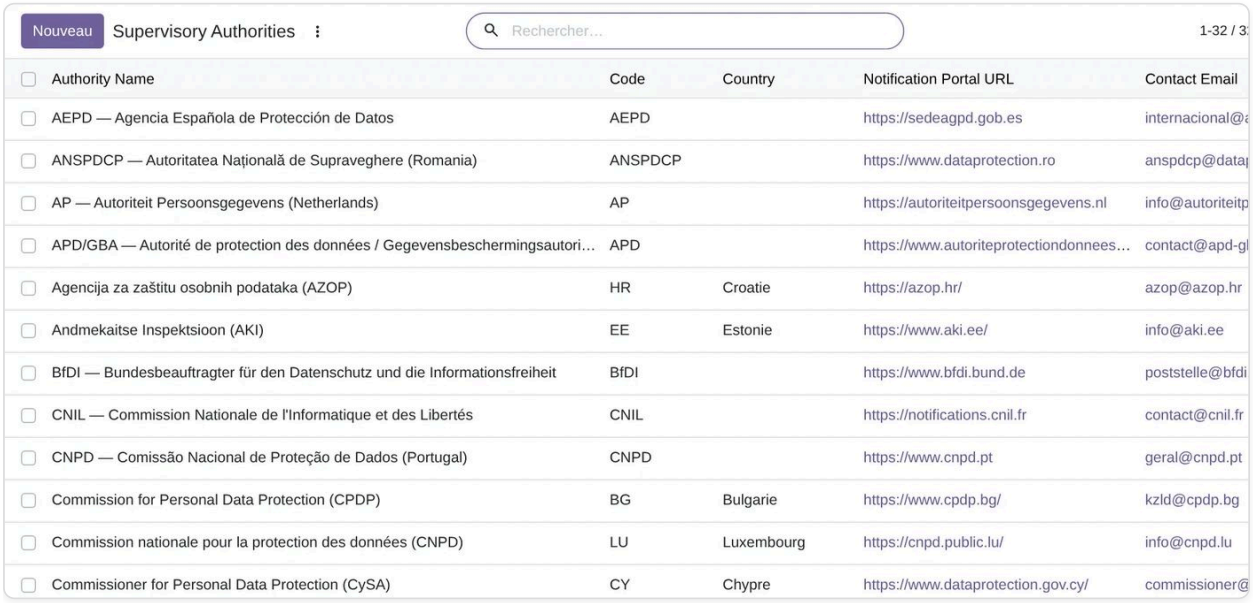
Ce qui n'est pas possible

Les entrées ne peuvent être que créées. Toute tentative de les modifier ou de les supprimer, quel que soit l'utilisateur, aboutit à un message d'erreur. Ce message cite l'art. 5(2) du RGPD, le principe de responsabilité, comme raison de leur conservation.

Un exemple de bout en bout

Vous accédez à **GDPR Toolkit › Reports › Export RoPA (Excel)**, laissez **Include Archived Activities** décochée et cliquez sur **Export**. Vous recevez le fichier avec une ligne par activité. Ensuite, vous ouvrez **GDPR Toolkit › Configuration › Audit Log** et filtrez par **Exports** : vous y voyez l'export avec votre utilisateur et la date et l'heure. Dans la même liste apparaissent les créations et modifications de vos activités et incidents, avec le nom de chaque enregistrement.

14 Autorités de contrôle et bases juridiques



Nouveau | Supervisory Authorities | Rechercher... | 1-32 / 3

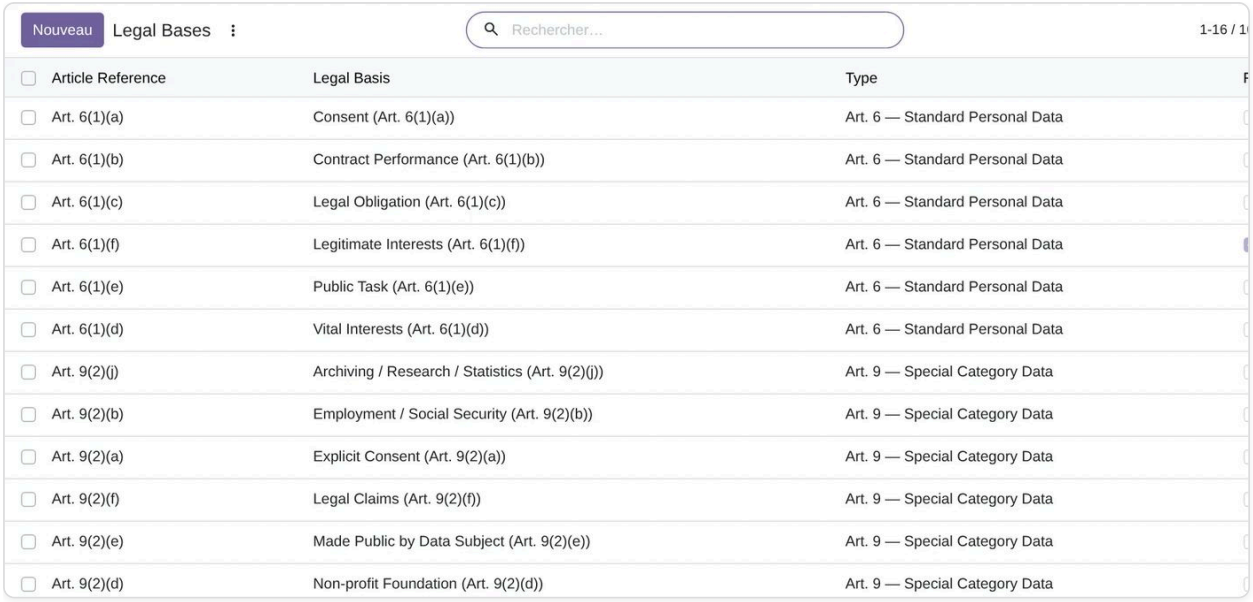
Authority Name	Code	Country	Notification Portal URL	Contact Email
AEPD — Agencia Española de Protección de Datos	AEPD		https://sedeagpd.gob.es	internacional@
ANSPDCP — Autoritatea Națională de Supraveghere (Romania)	ANSPDCP		https://www.dataprotection.ro	anspdcp@data
AP — Autoriteit Persoonsgegevens (Netherlands)	AP		https://autoriteitpersoonsgegevens.nl	info@autoriteitp
APD/GBA — Autorité de protection des données / Gegevensbeschermingsautori…	APD		https://www.autoriteprotectiondonnees…	contact@apd-gl
Agencija za zaštitu osobnih podataka (AZOP)	HR	Croatie	https://azop.hr/	azop@azop.hr
Andmekaitse Inspektsioon (AKI)	EE	Estonie	https://www.aki.ee/	info@aki.ee
BfDI — Bundesbeauftragter für den Datenschutz und die Informationsfreiheit	BfDI		https://www.bfdi.bund.de	poststelle@bfdi
CNIL — Commission Nationale de l'Informatique et des Libertés	CNIL		https://notifications.cnil.fr	contact@cnil.fr
CNPD — Comissão Nacional de Proteção de Dados (Portugal)	CNPD		https://www.cnpd.pt	geral@cnpd.pt
Commission for Personal Data Protection (CPDP)	BG	Bulgarie	https://www.cpdp.bg/	kzld@cpdp.bg
Commission nationale pour la protection des données (CNPD)	LU	Luxembourg	https://cnpd.public.lu/	info@cnpd.lu
Commissioner for Personal Data Protection (CySA)	CY	Chypre	https://www.dataprotection.gov.cy/	commissioner@

- **Capture réelle d'Odoo 20.** La liste **Supervisory Authorities** avec ses 32 enregistrements.

Le module contient 32 autorités de contrôle. Vous les trouvez dans **GDPR Toolkit › Configuration › Supervisory Authorities**. Elles sont chargées une seule fois, à l'installation. Il n'existe ni tâche planifiée ni bouton pour les mettre à jour, et seul un administrateur Odoo peut les modifier.

Authority Name	Nom complet de l'autorité. Champ obligatoire.
Country	Pays auquel appartient l'autorité.
Code	Sigle de l'autorité, par exemple AEPD, CNIL ou BfDI.
Notification Portal URL	Adresse du portail où se font les notifications.
Contact Email	Courriel de contact de l'autorité.
Breach Notification Form URL	Adresse du formulaire de notification d'une violation.
Active	Case indiquant si l'autorité est utilisée. Elle est cochée par défaut.

L'autorité principale se choisit dans **GDPR Toolkit › Configuration › DPO & Settings**.



- **Capture réelle d'Odoo 20.** La liste **Legal Bases** avec ses 16 enregistrements.

Les bases juridiques se trouvent dans **GDPR Toolkit › Configuration › Legal Bases**. Elles sont au nombre de 16 et sont chargées à l'installation : celles de l'article 6 et celles de l'article 9.

Legal Basis	Nom de la base. Champ obligatoire.
Article Reference	Référence de l'article, par exemple art. 6(1)(a).
Type	Indique s'il s'agit d'une base de l'article 6, pour les données personnelles ordinaires, ou de l'article 9, pour les catégories particulières de données.
Requires Legitimate Interests Balancing Test	Case marquant les bases qui exigent cette mise en balance.

> Ces listes n'ont ni statuts ni workflow. Elles sont toutes deux chargées à l'installation du module, et seul un administrateur Odoo peut les modifier.

Contenu de chaque liste et identification

Chaque autorité est identifiée par trois données : son **Authority Name**, son **Country** et son **Code**. Le code est un texte libre et l'aide du champ donne comme exemples AEPD, CNIL et BfDI. Les trois autres données (le portail de notification, le courriel de contact et le formulaire de violation) sont des adresses et un courriel que vous pouvez consulter depuis la fiche.

Active ou non active

Chaque autorité porte la case **Active**, cochée par défaut. C'est la seule information du registre indiquant si une autorité est considérée comme utilisée. Les bases juridiques ont elles aussi un champ d'activation, mais il n'apparaît dans aucun écran du module : vous ne pouvez ni le voir ni le modifier depuis l'interface.

Les deux types de base juridique

TYPE	CONTENU
Base de l'article 6	Les bases pour traiter des données personnelles ordinaires.

TYPE	CONTENU
Base de l'article 9	Les bases pour traiter des catégories particulières de données.

La mise en balance

La case **Requires Legitimate Interests Balancing Test** marque les bases qui exigent cette mise en balance. Apparaît par exemple **Legitimate Interests (Art. 6(1)(f))**, avec la référence de l'article dans sa colonne. La description de chaque base existe dans le modèle, mais n'apparaît dans aucun écran.

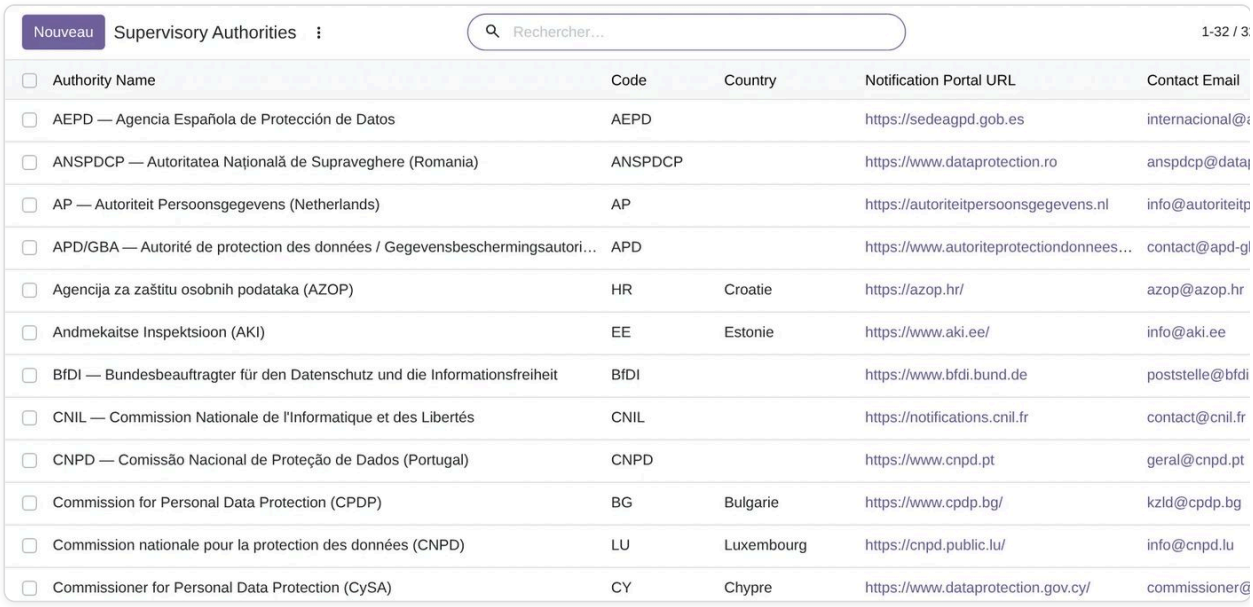
Règles et limites

- Le nom de l'autorité et le nom de la base juridique sont obligatoires.
- Le type de la base est obligatoire et, si vous ne le modifiez pas, il est défini comme base de l'article 6.
- Les listes sont chargées à l'installation. Le module ne les recharge ni ne les met à jour automatiquement.
- Le module n'envoie aucune notification à l'autorité. Le portail et le formulaire sont des adresses qui vous permettent de notifier vous-même depuis l'extérieur, puis d'en consigner ici le résultat.

Exemple de bout en bout

1 Consulter les autorités

Accédez à **GDPR Toolkit › Configuration › Supervisory Authorities**. La liste affiche 32 enregistrements, dont la AEPD : son code est AEPD.

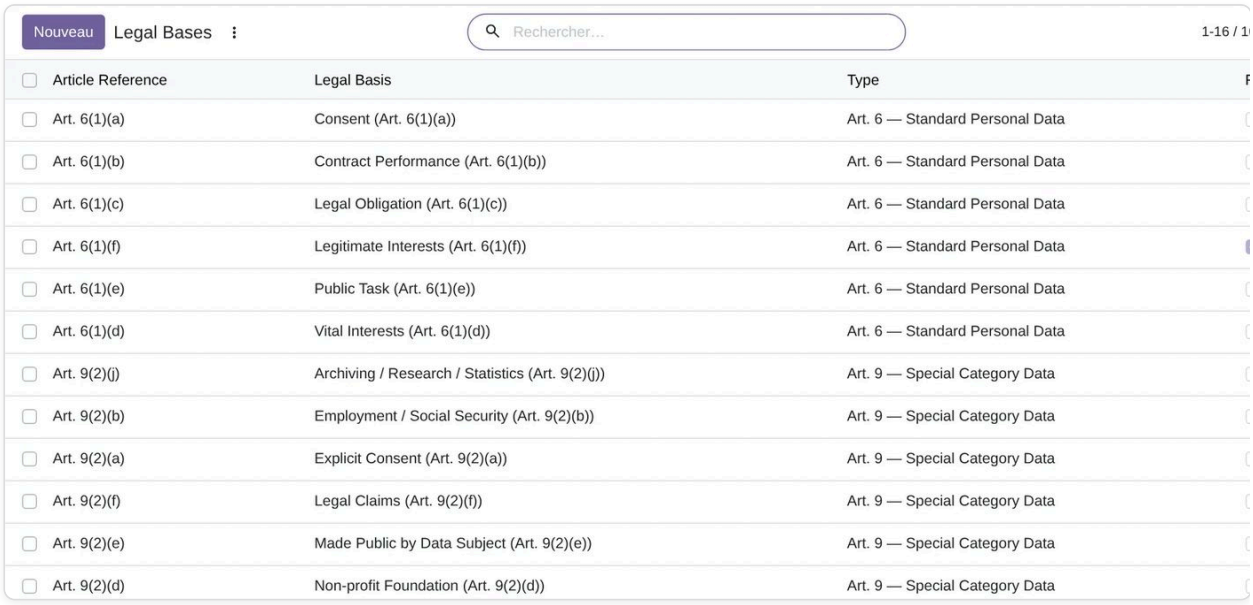


Authority Name	Code	Country	Notification Portal URL	Contact Email
AEPD — Agencia Española de Protección de Datos	AEPD		https://sedeagpd.gob.es	internacional@a
ANSPDCP — Autoritatea Națională de Supraveghere (Romania)	ANSPDCP		https://www.dataprotection.ro	anspdcp@datap
AP — Autoriteit Persoonsgegevens (Netherlands)	AP		https://autoriteitpersoonsgegevens.nl	info@autoriteitp
APD/GBA — Autorité de protection des données / Gegevensbeschermingsautori…	APD		https://www.autoriteprotectiondonnees…	contact@apd-gb
Agencija za zaštitu osobnih podataka (AZOP)	HR	Croatie	https://azop.hr/	azop@azop.hr
Andmekaitse Inspektsioon (AKI)	EE	Estonie	https://www.aki.ee/	info@aki.ee
BfDI — Bundesbeauftragter für den Datenschutz und die Informationsfreiheit	BfDI		https://www.bfdi.bund.de	poststelle@bfdi
CNIL — Commission Nationale de l'Informatique et des Libertés	CNIL		https://notifications.cnil.fr	contact@cnil.fr
CNPD — Comissão Nacional de Proteção de Dados (Portugal)	CNPD		https://www.cnpd.pt	geral@cnpd.pt
Commission for Personal Data Protection (CPDP)	BG	Bulgarie	https://www.cpdp.bg/	kzld@cpdp.bg
Commission nationale pour la protection des données (CNPD)	LU	Luxembourg	https://cnpd.public.lu/	info@cnpd.lu
Commissioner for Personal Data Protection (CySA)	CY	Chypre	https://www.dataprotection.gov.cy/	commissioner@

- **Capture réelle d'Odoo 20.** La liste affiche le nom, le code, le pays, le portail et le courriel de chaque autorité.

2 Consulter les bases juridiques

Accédez à **GDPR Toolkit › Configuration › Legal Bases**. La liste affiche 16 enregistrements. Recherchez **Consent (Art. 6(1)(a))** et **Legitimate Interests (Art. 6(1)(f))**, qui porte la case de mise en balance cochée.



- **Capture réelle d'Odoo 20.** La liste affiche la référence de l'article, la base juridique et son type.

GUIDE DU MODULE · GDPR COMPLIANCE

15 Ce qui part vers FlexigoTech Cloud et ce qui revient

DONNÉE	DIRECTION	QUAND
L'identification de la base : son identifiant, son adresse et son code public, la version d'Odoo et les noms de ses modules	De votre Odoo vers FlexigoTech Cloud	Lors de la connexion de la base au service
L'acceptation des conditions et du contrat de sous-traitance, avec le courriel de la personne qui accepte	De votre Odoo vers FlexigoTech Cloud	Lorsque vous cliquez sur **Connecter et démarrer l'essai** après avoir confirmé avoir lu la liste
La demande d'autorisation du service pour le module	De votre Odoo vers FlexigoTech Cloud	Les modules la demandent automatiquement ; **Vérifier maintenant** la demande immédiatement
Les demandes d'avis de veille	De votre Odoo vers FlexigoTech Cloud	Toutes les 6 heures, lorsque la base demande les nouveaux avis
Les avis de veille	De FlexigoTech Cloud vers votre Odoo	Lors de la demande suivante après qu'une source a changé

Ce que surveille le service

FlexigoTech Cloud contrôle chaque jour six sources officielles et signale tout changement. Il s'agit des actes de l'Union européenne qui modifient le RGPD, publiés à l'Office des publications ; de la procédure 2025/0360(COD), dite omnibus numérique, sur l'Observatoire législatif du Parlement européen ; de la LOPDGDD consolidée, au BOE ; de la page des décisions d'adéquation de la Commission européenne ; et des pages de guides et d'outils de l'AEPD.

Les avis apparaissent dans **Paramètres › FlexigoTech Cloud** et arrivent également dans un courriel quotidien.

Ce qui reste dans votre Odoo

Le registre des activités de traitement, les demandes des personnes concernées, les violations, les analyses d'impact et le journal d'audit restent dans votre base de données. Le module n'envoie rien de tout cela à FlexigoTech ni à aucun service externe. L'écran de connexion le rappelle : vos clients, commandes, factures et produits ne sont pas transmis à FlexigoTech Cloud par cette connexion.

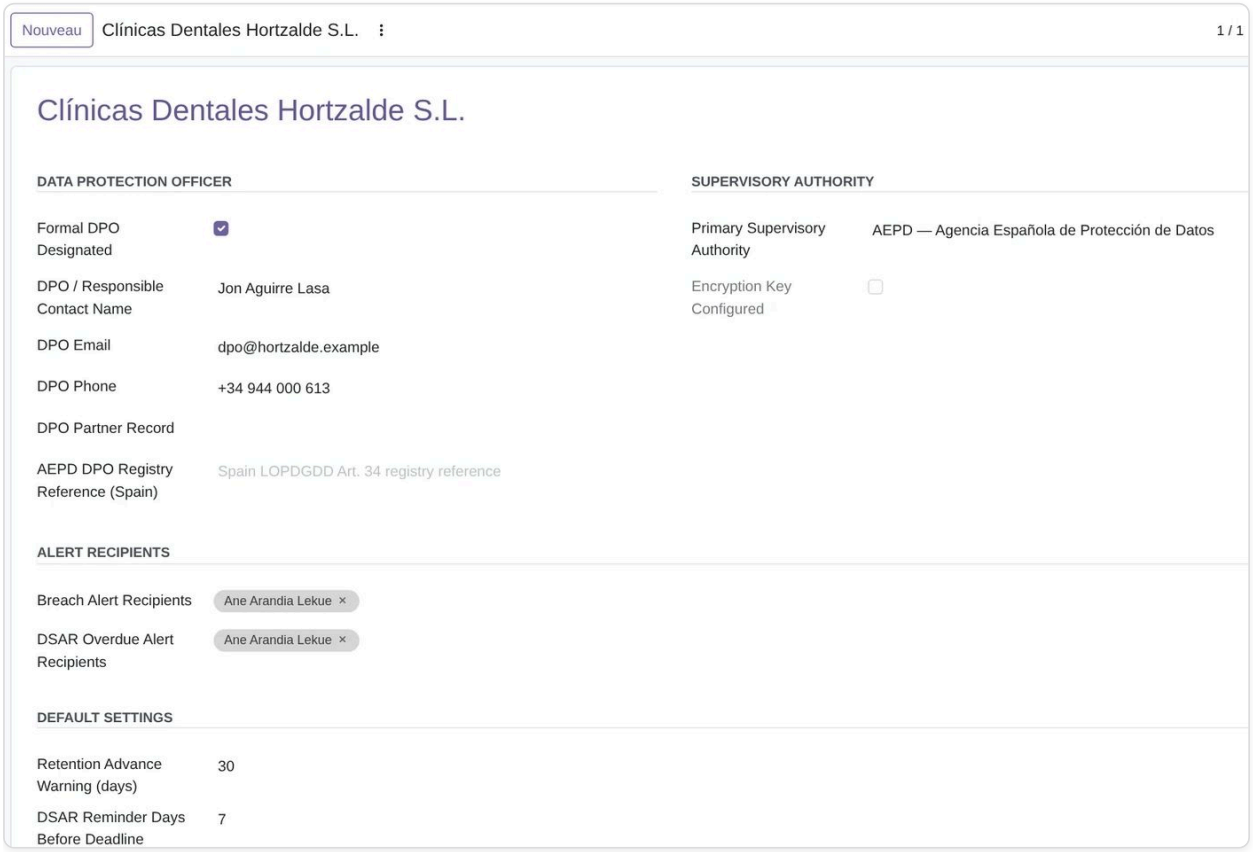
GUIDE DU MODULE · GDPR COMPLIANCE

16 Ce qui se passe automatiquement

TÂCHE	FRÉQUENCE	FONCTION
GDPR: DSAR Deadline Reminder	Tous les jours	Envoie un courriel lorsqu'une demande ouverte approche de l'échéance, selon le nombre de jours défini dans **DSAR Reminder Days Before Deadline** : à la personne assignée ou, si elle n'a pas d'adresse courriel, aux responsables RGPD.
GDPR: Breach Countdown Alert	Toutes les heures	Dans les 6 dernières heures du délai d'une violation ouverte qui n'est pas marquée comme notifiée, envoie un e-mail aux **Breach Alert Recipients** ou aux gestionnaires RGPD.
GDPR: Retention Expiry Check	Tous les jours	Crée une activité d'alerte et envoie un e-mail pour chaque activité active dont la fin de conservation approche et qui n'a pas été révisée au cours des 30 derniers jours.
GDPR: DSAR Overdue Escalation	Toutes les semaines	Envoie le récapitulatif des demandes hors délai aux **DSAR Overdue Alert Recipients** ou aux gestionnaires RGPD.
GDPR: Annual RoPA Review Reminder	Tous les 12 mois	Rappelle par e-mail qu'il est temps de réviser le registre des activités de traitement.

Les alertes sont envoyées par e-mail aux utilisateurs disposant d'une adresse e-mail, dans la langue de chacun. Les fréquences se modifient dans **Paramètres › Technique › Automatisation › Actions planifiées**, avec le mode développeur activé.

17 Les options du module et leurs valeurs par défaut



- **Capture réelle d'Odoo 20.** Les options de la configuration RGPD : le DPO, l'autorité de contrôle, les destinataires des alertes et les jours de préavis.

OPTION	VALEUR PAR DÉFAUT	FONCTION
DPO Partner Record, **DPO / Responsible Contact Name**, **DPO Email** et **DPO Phone**	Vides	Coordonnées de la personne qui fait office de délégué à la protection des données ou de contact.
Formal DPO Designated	Activée	Indique si un DPO est formellement désigné.
AEPD DPO Registry Reference (Spain)	Vide	Conserve la référence sous laquelle le DPO est inscrit auprès de l'AEPD.
Primary Supervisory Authority	Vide	Se choisit parmi les autorités de contrôle chargées dans le module.
Breach Alert Recipients	Vide	Utilisateurs qui reçoivent les alertes de violation. Si vous n'en choisissez aucun, elles sont reçues par le groupe **GDPR Toolkit / Manager** de la société.
DSAR Overdue Alert Recipients	Vide	Utilisateurs qui reçoivent l'alerte des demandes hors délai. Si vous n'en choisissez aucun, elle est reçue par le groupe **GDPR Toolkit / Manager** de la société.
Retention Advance Warning (days)	30	Nombre de jours de préavis avant la fin du délai de conservation.

OPTION	VALEUR PAR DÉFAUT	FONCTION
DSAR Reminder Days Before Deadline	7	Nombre de jours avant l'échéance d'une demande auquel le rappel est envoyé.
Art. 30(5) SME Exception Note Acknowledged	Désactivée	Vous consignez que vous avez lu la note sur l'exception de l'art. 30.5 pour les entreprises de moins de 250 personnes.
Encryption Key Configured	Selon le serveur	En lecture seule. Indique si le serveur a une clé de chiffrement configurée.

Il n'y a qu'une seule configuration par société. Si vous essayez d'en créer une seconde, Odoo affiche « Only one GDPR configuration record per company is allowed. A configuration already exists for company .... »

Les délais légaux ne sont pas modifiables (un mois pour répondre à une demande et deux mois de prolongation supplémentaires, art. 12.3 ; 72 heures pour notifier une violation, art. 33.1), ni la matrice de risque (impact par probabilité), qui relève du module.

Ce qui se fait manuellement

ÉCRAN	BOUTONS
Activité du RoPA	**Set Active** fait passer l'activité de brouillon à active ; c'est impossible si elle nécessite une AIPD et qu'aucune AIPD approuvée n'y est liée. **Archive** l'archive. **Set to Draft** la remet en brouillon. Le bouton de création de l'AIPD ouvre une évaluation pour cette activité.
Demande de droits	**Verify Identity** consigne la vérification. **Draft Response** fait passer la demande à l'état réponse rédigée. **Extend Deadline (2 months)** ajoute deux mois de prolongation (art. 12.3). **Close — Refused** et **Close — Partial Erasure** clôturent la demande selon votre décision.
Violation	**Mark DPA Notified** indique que la notification a été faite par vos soins. **Close** clôture la violation. **Archive (Admin Only)** l'archive.
AIPD	**Approve** et **Reject** enregistrent la décision du relecteur. **Re-sync Step 1 from RoPA** remplit de nouveau l'étape 1 avec les données de l'activité liée.
Assistants	**Export RoPA (PDF)** ouvre un assistant avec **Export Format** et **Include Archived Activities** ; **Export** génère le rapport et **Cancel** le ferme.

Les boutons des demandes, des violations et des AIPD ne sont visibles que pour **GDPR Toolkit / Manager**. Ceux de l'activité du RoPA sont visibles de tous, mais seul un gestionnaire peut les utiliser, car **GDPR Toolkit / User** a l'enregistrement en lecture seule. Seul un administrateur d'Odoo peut archiver une violation.

18 Sécurité et données personnelles

- Le groupe **GDPR Toolkit / User** voit le RoPA en lecture seule, peut enregistrer des demandes et voit celles qui sont à l'état **Received** ou qui lui sont assignées ; les modifier et utiliser leurs boutons relève de **GDPR Toolkit / Manager**.
- Le groupe **GDPR Toolkit / Manager** voit tout et est le seul à disposer des boutons de traitement : vérifier l'identité, rédiger la réponse, clôturer, approuver une AIPD, marquer une violation comme notifiée, entre autres.
- **Archive (Admin Only)**, sur les violations, n'est visible que pour l'administrateur d'Odoo.
- Chaque société ne voit que ses propres enregistrements.
- Les demandes, les violations et les activités ne sont pas supprimées : elles sont archivées ou clôturées.
- L'historique du RoPA et le journal d'audit ne sont pas modifiables.
- Le résumé d'audit masque les données personnelles.
- Les notes internes et la justification d'un refus (demandes), ainsi que la description et les conséquences (violations), ne sont stockées chiffrées que si le serveur dispose de la variable d'environnement GDPR_FERNET_KEY. Sans elle, elles sont stockées en clair, le journal du serveur le signale et la configuration l'affiche dans **Encryption Key Configured**.
- Aucune demande, violation, AIPD ni activité de traitement n'est envoyée à FlexigoTech Cloud. Les données de votre Odoo restent dans votre Odoo. Le service payant surveille six sources officielles et prévient lorsqu'une d'elles change.

19 Plusieurs sociétés

Chaque société Odoo a sa propre configuration du RGPD. Si personne n'a ouvert le menu de configuration, le module la crée avec les valeurs par défaut la première fois qu'il en a besoin. Le menu **Dashboard** ouvre la configuration de la société active et la crée si elle n'existe pas.

Chaque enregistrement (activité, demande, violation, AIPD) porte sa société, et chaque utilisateur voit ceux des sociétés auxquelles il a accès. Les tâches planifiées parcourent chaque société avec sa configuration. Les alertes vont aux destinataires indiqués par cette configuration et, s'il n'y en a aucun, aux gestionnaires RGPD de cette société.

Le portail de confidentialité crée la demande dans la société active au moment où la personne concernée l'envoie.

Le plan Standard coûte 29 € par mois ou 290 € par an, et le Pro 58 € par mois ou 580 € par an (prix hors TVA). Chaque module a son propre abonnement, pour la base de données de production ; ses copies de test sont incluses.

20 En cas de problème

Une activité de traitement ne s'active pas et l'avertissement indique qu'une AIPD approuvée est requise.	Complétez et approuvez une AIPD liée à l'activité. Une fois approuvée, cliquez de nouveau sur **Set Active**.
Une demande d'exercice de droits ne revient pas à un état antérieur.	L'état ne fait qu'avancer. Si vous vous êtes trompé, notez-le dans les notes internes et poursuivez à partir de l'état actuel.
L'export de portabilité ne se génère pas.	Vérifiez d'abord l'identité de la demande et liez un contact Odoo dans le champ **Odoo Contact (for portability export)**.
Vous ne pouvez pas clôturer une demande comme refusée.	Rédigez d'abord la justification du refus. Elle est obligatoire.
Vous ne pouvez pas prolonger le délai d'une demande.	Renseignez le motif de la prolongation. Sans motif, le module ne permet pas de prolonger.
Vous ne pouvez pas rejeter une AIPD.	Rédigez les commentaires du DPO. Ils sont obligatoires en cas de rejet.
Vous ne pouvez pas supprimer une violation, une demande ni une activité de traitement.	Elles font partie de la piste d'audit. Archivez-les. Pour les violations, seul un administrateur d'Odoo peut archiver, avec un motif écrit.
Les notes internes sont stockées en clair.	La clé de chiffrement est absente du serveur. Dans la configuration, **Encryption Key Configured** indique si elle est définie.

Les avertissements d'Odoo indiquent ce qui manque. Le plus souvent, il suffit de le compléter et de répéter l'action.

Autres avertissements possibles

« Only GDPR Managers can submit a DPIA for review. »	Demandez à un gestionnaire RGPD de la soumettre pour relecture.
« Only GDPR Managers (acting as DPO) can approve a DPIA. »	L'approbation est faite par un gestionnaire RGPD, qui agit en tant que DPO. Demandez-la à une personne disposant de cette autorisation.
« Only GDPR Managers can perform this action. »	L'action est réservée aux gestionnaires RGPD ou aux administrateurs d'Odoo. Demandez-la à l'un d'eux.
« Only Odoo Administrators can archive breach records. »	Demandez à un administrateur d'archiver la violation. Il doit indiquer un motif.
« Archive reason is required. »	Rédigez le motif de l'archivage et confirmez de nouveau.
« Extension justification is required when extending retention. »	Dans la revue de conservation, rédigez la justification avant d'enregistrer la prolongation.

« New retention end date is required when extending retention. »	Indiquez la nouvelle date limite dans la révision avant de l'enregistrer.
« No Odoo contact linked to this DSAR. Please link a res.partner record first. »	Associez le contact à la demande et relancez l'export.
L'avertissement indiquant que les données de la personne concernée ont déjà été anonymisées et qu'une gestion manuelle avec votre DPO est nécessaire.	Le contact est déjà anonymisé dans Odoo et il n'y a pas de données à exporter. Consultez votre DPO pour savoir comment répondre.
« No processing activities found for this company. »	Lors de l'export du RAT, vérifiez que l'entreprise active possède des activités.

GUIDE DU MODULE · GDPR COMPLIANCE

21 Autres façons de procéder

MÉTHODE	CE QUE CELA IMPLIQUE
Manuellement	Des feuilles de calcul pour le registre des activités, les demandes et les violations. Les délais se calculent à la main et personne n'est alerté lorsqu'ils approchent.
Odoo seul	Odoo 17, 18, 19 et 20 incluent d'origine, dans Community, la recherche de confidentialité, dans le menu technique des Paramètres (avec le mode développeur). Elle permet de retrouver les enregistrements d'une personne par nom ou courriel, d'archiver ou de supprimer ces enregistrements et de tenir un registre de confidentialité. Elle ne comporte ni registre des activités, ni suivi des demandes de droits, ni registre des violations, ni AIPD.
Ce module	Il ajoute le registre des activités de traitement, les demandes des personnes concernées avec leur délai d'un mois à compter de la réception et la prolongation de deux mois supplémentaires (art. 12.3), le registre des violations avec le compte à rebours de 72 heures à compter du moment où la violation est connue (art. 33.1), ainsi que les AIPD.

Pour effacer ou anonymiser les données d'une personne, la recherche de confidentialité d'Odoo s'utilise en complément de ce module. Le module assure le suivi de la demande et enregistre votre décision ; l'effacement ou l'anonymisation se fait par vos soins dans Odoo.

22 Formules et tarifs

9 €

Licence par version d'Odoo.

+ FlexigoTech Cloud

STANDARD

29 €/mois

ou 290 € par an

- Première réponse sous 1 jour ouvré

PRO

58 €/mois

ou 580 € par an

- Première réponse sous 4 heures ouvrées
- Visioconférence si besoin

14 jours d'essai, sans carte

Prix hors TVA

La licence du module s'achète par version d'Odoo. FlexigoTech Cloud se paie au mois ou à l'année, et l'essai de 14 jours ne demande pas de carte bancaire.

23 Questions fréquentes

Fonctionne-t-il sans FlexigoTech Cloud ?

Non.

Que apporte l'abonnement FlexigoTech Cloud ?

La veille quotidienne de six sources officielles, avec une alerte lorsqu'une d'elles change. Les alertes apparaissent dans **Paramètres › FlexigoTech Cloud** et dans un courriel quotidien.

Combien coûte le service FlexigoTech Cloud ?

La formule Standard coûte 29 € par mois ou 290 € par an, et la formule Pro 58 € par mois ou 580 € par an, hors TVA. S'y ajoute la licence du module, 9 € par version d'Odoo.

Quelles sources le service surveille-t-il ?

Les actes de l'Union européenne qui modifient le RGPD, la procédure de l'omnibus numérique au Parlement européen, la LOPDGDD consolidée du BOE, les décisions d'adéquation de la Commission européenne et les guides et outils de l'AEPD.

Que part de mon Odoo vers FlexigoTech Cloud ?

L'identification de l'installation (identifiant, adresse, code public, version d'Odoo et noms des modules), l'acceptation des conditions avec le courriel de la personne qui accepte et la demande d'autorisation du service. Le registre des activités, les demandes, les violations, les AIPD et l'audit restent dans votre base de données.

Fonctionne-t-il sur Odoo Online ?

Non. Odoo Online ne permet pas d'installer des modules tiers.

Nécessite-t-il Odoo Enterprise ?

Non. Il ne dépend que de modules Odoo Community (base, mail et portail) et de flexigotech_cloud : il fonctionne avec Community comme avec Enterprise.

Pour quelles versions d'Odoo est-il disponible ?

Il existe une branche pour chacune des versions 17, 18, 19 et 20.

Quel délai calcule-t-il pour une demande de personne concernée et d'où vient-il ?

Un mois à compter de la réception de la demande, selon l'art. 12.3 du RGPD. La colonne **Days Remaining** décompte jusqu'au délai en vigueur.

Comment prolonger le délai ?

Avec **Extend Deadline (2 months)**, qui ajoute deux mois supplémentaires (art. 12.3) et exige d'indiquer le motif. Cela ne modifie que le **Current Deadline** ; l'état de la demande reste inchangé.

Que se passe-t-il lorsque le délai d'une demande expire ?

La demande apparaît dans la liste **Overdue**. Chaque semaine, la tâche **GDPR: DSAR Overdue Escalation** envoie le récapitulatif des demandes en retard aux destinataires de ces alertes ou, à défaut, aux gestionnaires du RGPD.

Comment sont décomptées les 72 heures d'une violation, et à qui l'alerte est-elle envoyée ?

Le décompte part de la date et de l'heure auxquelles vous consignez que la violation a été connue, conformément à l'art. 33.1. Chaque heure, la tâche **GDPR: Breach Countdown Alert** envoie un courriel lorsqu'il reste 6 heures ou moins, tant que vous ne l'avez pas marquée comme notifiée.

Notifie-t-il l'autorité de contrôle ?

Non. La notification est effectuée par vos soins et vous en consignez ici l'état, la date et l'heure, le moyen et la référence.

Communique-t-il quoi que ce soit aux personnes concernées par une violation ?

Non. Si la communication prévue à l'art. 34 est obligatoire, vous la réalisez vous-même et la consignez avec **Mark Data Subjects Notified**.

Efface-t-il ou anonymise-t-il les données lors d'une demande d'effacement ?

Non. **Retention Conflict Check** recense ce qui existe et enregistre votre décision. L'effacement ou l'anonymisation se fait par vos soins dans Odoo.

Envoie-t-il la lettre de réponse à la personne concernée ?

Non. Vous la rédigez dans l'onglet de réponse à partir d'un modèle, puis vous l'envoyez vous-même. Le seul courriel envoyé automatiquement à la personne concernée est l'accusé de réception d'une demande faite depuis le portail.

Que permet d'exporter le droit à la portabilité, et dans quels formats ?

Les coordonnées, l'historique des commandes (avec l'application Ventes) et la fiche d'employé (avec l'application Employés, avec confirmation expresse). Les formats sont JSON ou CSV.

De quoi l'export de portabilité a-t-il besoin pour être généré ?

D'une identité vérifiée et d'un contact Odoo lié à la demande. Sans cela, l'assistant refuse.

Comment une personne concernée peut-elle faire une demande via le portail, et que lui faut-il ?

Elle accède à /my/privacy-rights de votre Odoo, ce qui exige une connexion, donc un compte portail. Le module n'ajoute aucun lien dans Mon compte : c'est à vous de lui communiquer l'adresse.

Quand une AIPD est-elle marquée comme obligatoire ?

Lorsque deux critères ou plus parmi les neuf de l'onglet **DPIA Criteria** sont remplis, ou si vous la forcez manuellement. Cette règle des deux critères est une recommandation générale des lignes directrices WP248, et non une obligation légale.

Qu'est-ce que la consultation préalable ?

La consultation de l'autorité prévue à l'art. 36. Lorsque le risque résiduel est élevé ou critique, **Prior Consultation Required (Art. 36)** se coche automatiquement. Si vous la déposez, vous consignez ici ce que vous avez fait ; le module ne la dépose pas.

Puis-je supprimer une demande, une violation ou une activité ?

Non. Les activités, les demandes et les violations sont archivées ou clôturées. Seul l'administrateur Odoo peut archiver une violation, et un motif est exigé.

Que conserve le journal d'audit ?

La date et l'heure, l'utilisateur, l'opération, le modèle, le nom de l'enregistrement et, lorsqu'elle est disponible, l'adresse IP de chaque modification. Personne ne peut modifier ni supprimer ses entrées, pas même un administrateur.

Que est-il stocké chiffré ?

Les notes internes, la motivation d'un refus ainsi que la description et les conséquences des violations, uniquement si le serveur dispose de la clé de chiffrement. Sans elle, ils sont stockés en clair.

Fonctionne-t-il avec plusieurs sociétés ?

Oui. Chaque société a sa propre configuration, et chaque utilisateur ne voit que les enregistrements des sociétés auxquelles il a accès.

Dans quelles langues s'affichent les écrans ?

En espagnol, les écrans du module s'affichent en espagnol. Dans les autres langues, ils s'affichent en anglais ; les menus et boutons d'Odoo, dans la langue de chaque utilisateur.

Sert-il à une entreprise de moins de 250 personnes ?

L'art. 30.5 du RGPD exclut des obligations des paragraphes 1 et 2 les entreprises de moins de 250 personnes, sauf si le traitement peut comporter un risque pour les droits et libertés des personnes concernées, n'est pas occasionnel, ou porte sur des catégories particulières de données ou sur des données relatives à des condamnations et infractions pénales. Le module ne se prononce pas sur le fait que cela vous concerne.

Combien d'autorités de contrôle et de bases juridiques contient-il ?

32 autorités de contrôle et 16 bases juridiques, chargées à l'installation. Vous choisissez votre autorité principale dans **GDPR Toolkit › Configuration › DPO & Settings**.

Quels rapports et exports propose-t-il ?

Vous pouvez exporter le RAT en PDF ou en Excel. Il existe aussi des rapports sur l'historique des demandes de droits, le registre des violations et l'état des AIPD.

Quelles alertes envoie-t-il par courriel ?

Cinq tâches planifiées : le rappel quotidien de l'échéance des demandes, le compte à rebours horaire des violations, la vérification quotidienne de la conservation, l'escalade hebdomadaire des demandes en retard et le rappel de la révision annuelle du RAT.

À quoi sert le menu Tableau de bord ?

Trois boutons ouvrent des listes : **View Open DSARs**, **View Active Breaches** et **DPIAs Pending Review**. Il n'affiche pas de chiffres.

Décide-t-il à ma place de notifier une violation ou de réaliser une AIPD ?

Non. La décision finale revient au responsable du traitement ou à son DPO. La matrice de risque, impact multiplié par probabilité, est celle du module, et non celle de la loi.

S'agit-il de conseil juridique ?

Non.

---

24 Glossaire

RGPD	Le règlement général sur la protection des données, le règlement (UE) 2016/679. C'est la norme européenne dont découlent les délais et les obligations gérés par le module.
LOPDGDD	La loi espagnole sur la protection des données et la garantie des droits numériques. FlexigoTech Cloud surveille son texte consolidé au BOE.
AEPD	L'Agence espagnole de protection des données. C'est l'une des 32 autorités de contrôle incluses dans le module.
Autorité de contrôle	L'autorité publique qui supervise la protection des données dans chaque pays. C'est à elle que les violations sont notifiées (art. 33.1). Dans **Primary Supervisory Authority**, vous choisissez la vôtre.
DPO	Le délégué à la protection des données ou, à défaut, la personne responsable de la confidentialité. Ses coordonnées sont enregistrées dans la configuration.
Responsable du traitement	Celui qui décide des finalités et des moyens du traitement. Son registre des activités est celui de l'art. 30.1.
Sous-traitant	Celui qui traite des données pour le compte du responsable du traitement. Son registre des activités est celui de l'art. 30.2.
Personne concernée	La personne dont les données sont traitées et qui peut exercer ses droits.
RAT	Le registre des activités de traitement (art. 30) : une fiche par activité, avec son historique.
Demande de droits	La demande d'une personne concernée : accès (art. 15), rectification (art. 16), effacement (art. 17), limitation (art. 18), portabilité (art. 20) ou opposition (art. 21).
Délai en vigueur	La date jusqu'à laquelle il faut répondre à une demande : un mois à compter de la réception et, en cas de prolongation, deux mois supplémentaires (art. 12.3).
Portabilité	Le droit de recevoir les données que la personne concernée a fournies dans un format structuré, couramment utilisé et lisible par machine (art. 20.1). Le module les exporte en JSON ou en CSV.
Effacement	Le droit d'obtenir l'effacement des données (art. 17). Le module recense ce qui existe et enregistre votre décision ; l'effacement lui-même vous revient.
Violation de données	Une violation de la sécurité des données à caractère personnel. Elle est notifiée à l'autorité de contrôle dans les meilleurs délais et, si possible, dans les 72 heures après en avoir pris connaissance, sauf si la violation est peu susceptible d'engendrer un risque (art. 33.1).
AIPD	L'analyse d'impact relative à la protection des données (art. 35), en cinq étapes.
Risque résiduel	Le risque subsistant après application des mesures d'atténuation. Lorsque le risque résiduel est élevé ou critique, la consultation préalable est signalée.
Consultation préalable	La consultation de l'autorité avant le traitement lorsque l'AIPD révèle un risque élevé qui ne peut être atténué par des mesures appropriées (art. 36.1). C'est vous qui la soumettez.
Base juridique	Le motif qui autorise le traitement des données. Le module en propose 16 : 6 de l'art. 6 et 10 de l'art. 9.

Catégories particulières	Les données visées à l'art. 9, comme les données de santé. Elles ont leurs propres bases juridiques.
Transfert international	L'envoi de données vers un pays tiers. La fiche de l'activité indique le pays et la garantie qui l'encadre.
Conservation	La durée de conservation des données de chaque activité, avec sa date limite estimée et son historique de révisions.
Journal d'audit	La liste de qui a effectué quelle modification, quand et depuis quelle adresse IP. Il ne peut être ni modifié ni supprimé.
Veille	Le service de FlexigoTech Cloud qui consulte chaque jour six sources officielles et vous alerte lorsqu'une d'entre elles change.

GUIDE DU MODULE · GDPR COMPLIANCE

25 Liste de vérification et contact

- [ ] Vous disposez d'Odoo 17, 18, 19 ou 20 sur Odoo.sh ou sur votre propre serveur. Odoo Online ne permet pas d'installer de modules tiers.
- [ ] Vous avez installé le module et sa dépendance, flexigotech_cloud.
- [ ] Vous avez activé l'essai de 14 jours de FlexigoTech Cloud dans **Paramètres › FlexigoTech Cloud** et lu la liste des données envoyées.
- [ ] Vous avez ouvert **GDPR Toolkit › Configuration › DPO & Settings** et renseigné les données du DPO et la **Primary Supervisory Authority**.
- [ ] Vous avez désigné les destinataires des alertes de violation et des demandes des personnes.
- [ ] Vous avez attribué à chaque personne le groupe **GDPR Toolkit / Manager** ou **GDPR Toolkit / User**.
- [ ] Si vous souhaitez chiffrer les notes internes et la description des violations, vous avez défini la clé de chiffrement sur le serveur et **Encryption Key Configured** le confirme.
- [ ] Vous avez créé les activités du registre des traitements avec leurs critères d'AIPD et leur durée de conservation.
- [ ] Vous avez enregistré une première demande et vérifié son **Current Deadline**.
- [ ] Vous avez communiqué aux personnes concernées l'adresse /my/privacy-rights de votre Odoo.
- [ ] Si vous le souhaitez, vous avez testé le registre des violations avec une violation fictive et observé le compte à rebours de 72 heures.

Si vous souhaitez que nous le mettions en place avec vous, écrivez-nous. 2 mois de support inclus dans tout ce que vous achetez : nous vous aidons à l'installer, à le configurer et à le faire fonctionner, par e-mail et visioconférence.

E-mail

Pour l'installer, le configurer ou pour toute question.
comercial@flexigotech.com

Sur le web

La page du module, avec le guide et les prix.
flexigotech.com/fr/odoo-gdpr.html

Sur Odoo Apps

La page du module sur la boutique d'Odoo.
apps.odoo.com

GDPR Compliance est un module de FlexigoTech pour Odoo. FlexigoTech est une marque de Flexibles y Accesorios Gobe, S.L. (Barcelone, Espagne).