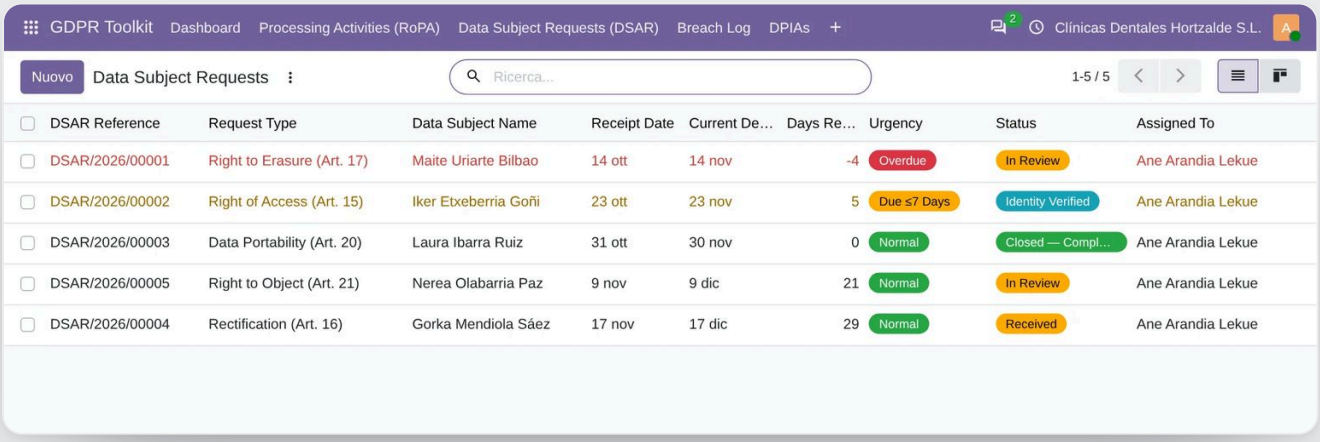
GUIDA DEL MODULO · PROTEZIONE DEI DATI

GDPR Compliance per Odoo

Il registro delle attività, le richieste con la relativa scadenza, le violazioni con le loro 72 ore e le DPIA, all'interno di Odoo.

Odoo 17 · 18 · 19 · 20 | 14 giorni di prova, senza carta | Edizione del 19-11-2026





Schermata reale di Odoo 20. La lista delle richieste con la loro scadenza e la loro urgenza, e una violazione con il conto alla rovescia di 72 ore.

Indice

A destra, la pagina in cui inizia ogni capitolo. I nomi di menu e pulsanti sono quelli di Odoo in italiano. I menu e i pulsanti del modulo sono in inglese: il modulo non è ancora tradotto in italiano.

1	Per chi è e cosa risolve	3
2	Il modulo in cifre	4
3	Dove lo vedi nel tuo Odoo	5
4	Cosa ti serve prima di iniziare	6
5	La prova di FlexigoTech Cloud	6
6	Messa in funzione passo passo	8
7	Il registro delle attività di trattamento	9
8	Le richieste degli interessati e i loro termini	13
9	Portabilità, cancellazione e portale della privacy	18
10	Il registro delle violazioni e le 72 ore	21
11	Le valutazioni d'impatto (DPIA)	24
12	La conservazione e le sue revisioni	28
13	Report, esportazioni e registro di audit	32
14	Autorità di controllo e basi giuridiche	35
15	Cosa va a FlexigoTech Cloud e cosa torna	38
16	Cosa succede da solo	39
17	Le opzioni del modulo e il loro valore iniziale	40
18	Sicurezza e dati personali	42
19	Più aziende	42
20	Se qualcosa non funziona	42
21	Altri modi di farlo	44
22	Piani e prezzo	44
23	Domande frequenti	45
24	Glossario	47
25	Checklist e contatti	49

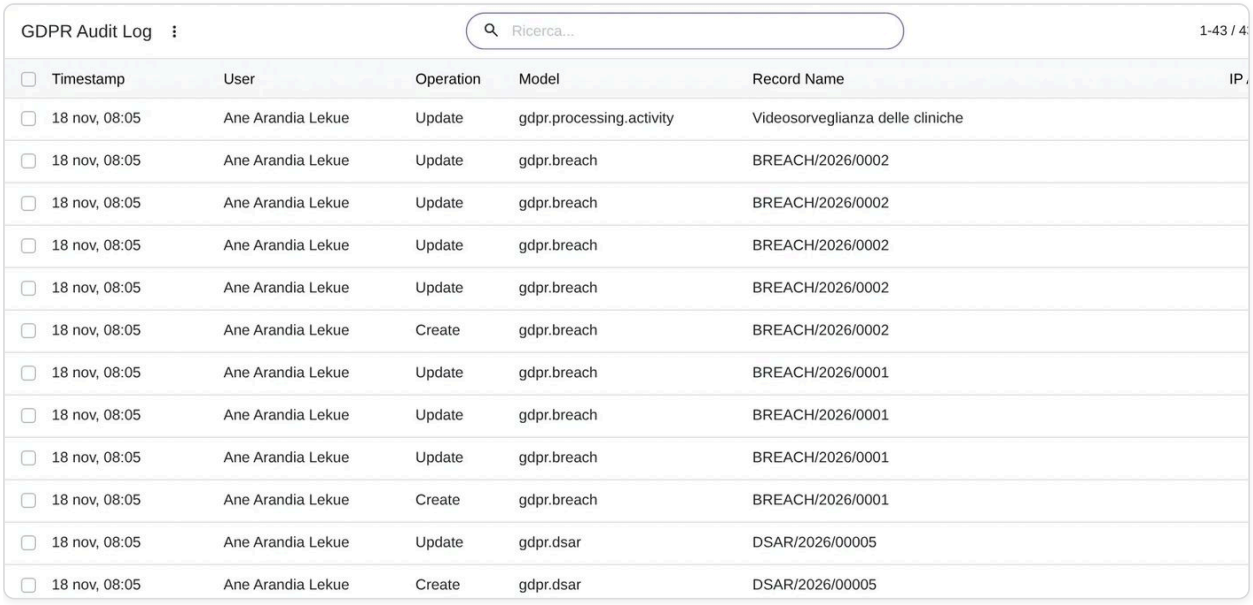
Questa guida descrive la versione 20.0.1.1.13 del modulo (branch 20.0 di Odoo, commit e15afc58d). Tutto ciò che racconta viene dal codice pubblicato, dalla documentazione ufficiale della piattaforma o da schermate reali.

Le schermate vengono da un database Odoo 20 di prova, con un'azienda e dati inventati e senza collegamento reale con FlexigoTech Cloud. Il modulo esiste anche per Odoo 17, 18 e 19.

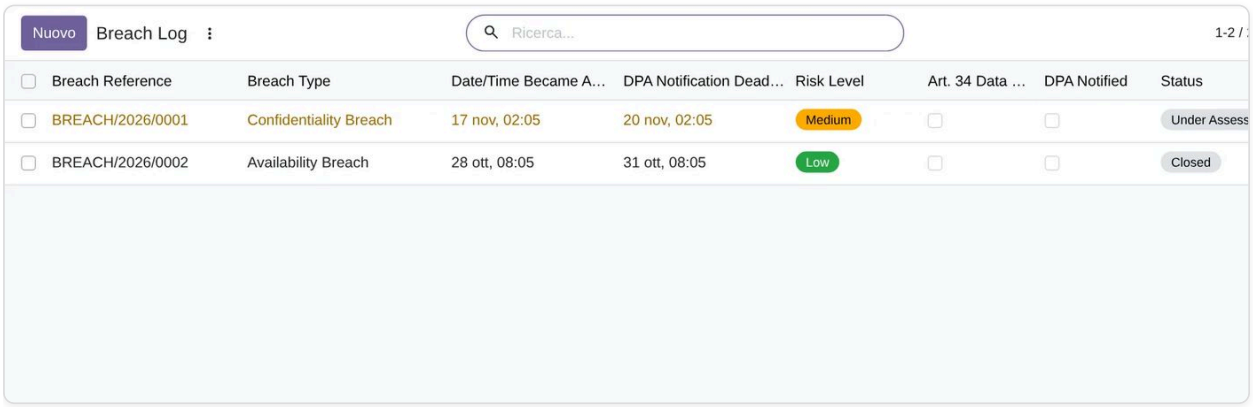
1 Per chi è e cosa risolve

Senza il modulo, il registro delle attività di solito vive in fogli di calcolo sparsi. Le scadenze delle richieste si calcolano a mano e nessuno avvisa quando si avvicinano. Non resta lo storico di chi ha cambiato cosa e quando. In una violazione, nessuno tiene il conto delle ore trascorse da quando se n'è avuta conoscenza.

Con il modulo, tutto questo sta dentro Odoo, con le scadenze in vista e un registro di controllo che non si può modificare.



- **Schermata reale di Odoo 20.** Il **GDPR Audit Log** con la data, l'utente e l'operazione di ogni modifica.



- **Schermata reale di Odoo 20.** L'elenco **Breach Log** con il termine di notifica di 72 ore di ogni violazione.

Cosa cambia nella vita quotidiana

- Ogni attività di trattamento riporta le sue finalità, basi giuridiche, categorie di dati e di interessati, destinatari e termine di conservazione, e ogni modifica viene salvata nel suo storico.
- Le richieste degli interessati hanno la loro scadenza di un mese dal ricevimento, con la proroga di altri due mesi se necessaria e motivata (art. 12.3). Ci sono elenchi di quelle fuori termine e di quelle che scadono questa settimana.
- Una violazione inizia a contare 72 ore da quando annoti quando se n'è avuta conoscenza (art. 33.1), e, nelle ultime 6 ore, il modulo avvisa via e-mail ogni ora finché non la contrassegni come notificata.
- Un'attività che soddisfa due criteri delle linee guida WP248 viene contrassegnata con **DPIA Required** e il modulo non permette di attivarla finché non ha una DPIA approvata. La DPIA (art. 35) ha cinque passaggi e

indica la consultazione preventiva quando il rischio residuo lo richiede (art. 36).

- L'interessato con account del portale invia la sua richiesta da /my/privacy-rights e riceve una ricevuta via e-mail.

Cosa non fa

- Non elimina né anonimizza dati di Odoo. Il controllo di cancellazione conta quello che c'è e annota la tua decisione; cancellare o anonimizzare lo fai tu.
- Non notifica all'autorità di controllo né comunica nulla agli interessati. Qui annoti quello che hai fatto tu: lo stato, la data e l'ora, il metodo e il riferimento.
- Non invia la lettera di risposta all'interessato. La redigi nella scheda della risposta a partire da un modello e la spedisci per conto tuo.
- Non decide al posto tuo se una violazione va notificata o se serve una DPIA. La matrice di rischio (impatto per probabilità) e le sue soglie sono del modulo, non del GDPR né delle linee guida del Comitato europeo; la decisione finale spetta al titolare o al suo DPO.
- Non è consulenza legale.

GUIDA DEL MODULO · GDPR COMPLIANCE

2 Il modulo in cifre

155
test automatici

7.013
righe di codice in Odoo Apps (ramo 20.0)

32
autorità di controllo

16
basi giuridiche

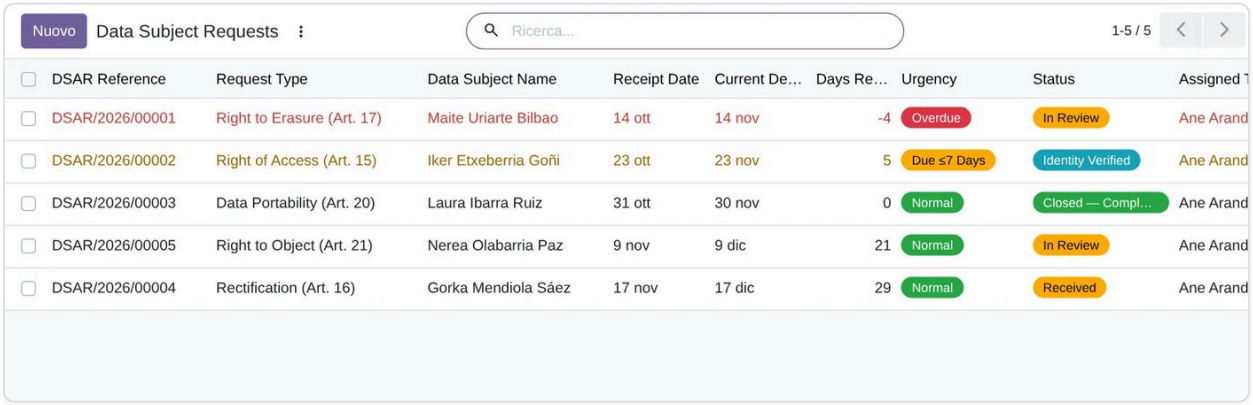
5
attività pianificate

14
giorni di prova di FlexigoTech Cloud

Dipende solo da moduli di Odoo Community (base, mail e portal) e da `flexigotech_cloud`, quindi funziona in Community e in Enterprise. Esiste una versione del modulo per Odoo 17, 18, 19 e 20.

> Come è stato testato: il modulo include 155 test automatici nella sua versione per Odoo 20. Il team di FlexigoTech lo ha testato su Odoo 17, 18, 19 e 20, su basi Community e su Odoo.sh, e ha confrontato le sue scadenze con il testo del GDPR pubblicato su EUR-Lex (articoli 12.3, 33.1, 35 e 36). Nessuna autorità ha revisionato il modulo e non è consulenza legale: la decisione finale spetta a te o al tuo DPO.

3 Dove lo vedi nel tuo Odoo



- **Schermata reale di Odoo 20.** L'elenco **Data Subject Requests** con il termine in vigore, i giorni rimanenti e l'urgenza di ogni richiesta.

Dashboard	Tre pulsanti che aprono elenchi. È spiegato più sotto.
Processing Activities (RoPA)	**All Activities** e **DPIA Required**.
Data Subject Requests	**All Requests**, **Overdue** e **Due This Week**.
Breach Log	**All Breaches** e **Active Incidents**. Lo vede solo **GDPR Toolkit / Manager**.
DPIA	**All DPIAs** e **Awaiting DPO Review**. Lo vede solo **GDPR Toolkit / Manager**.
Retention Management	**Retention Schedule** e **Review History**. Lo vede solo **GDPR Toolkit / Manager**.
Reports	**Export RoPA (PDF)**, **Export RoPA (Excel)**, **DSAR History Report**, **Breach Log Report** e **DPIA Status Report**. Lo vede solo **GDPR Toolkit / Manager**.
Configuration	**DPO & Settings**, **Supervisory Authorities**, **Categories of Data**, **Categories of Data Subjects**, **Categories of Recipients**, **Legal Bases** e **Audit Log**. Lo vede solo **GDPR Toolkit / Manager**.

Il menu **Dashboard** apre la configurazione della società con tre pulsanti: **View Open DSARs**, **View Active Breaches** e **DPIAs Pending Review**. Ogni pulsante apre un elenco. Non mostra cifre né indicatori.

Al di fuori del suo menu, il modulo aggiunge il portale privacy all'indirizzo /my/privacy-rights del tuo Odoo, per chi ha un account del portale. Il modulo non mette un link nella pagina Il mio account del portale: l'indirizzo lo fornisci tu all'interessato. Cinque attività pianificate inviano avvisi via e-mail: il promemoria giornaliero della scadenza delle richieste, l'avviso del conto alla rovescia delle violazioni, il controllo giornaliero della scadenza della conservazione, l'escalation settimanale delle richieste fuori termine e il promemoria della revisione annuale del RAT.

4 Cosa ti serve prima di iniziare

- Odoo 17, 18, 19 o 20, su Odoo.sh o sul tuo server. Non va bene Odoo Online, che non permette di installare moduli di terze parti.
- Chi farà da **GDPR Toolkit / Manager** e chi da **GDPR Toolkit / User**. Quando installi il modulo, l'amministratore è **GDPR Toolkit / Manager**.
- I dati del DPO o, se non c'è, della persona responsabile della privacy: nome, e-mail e telefono.
- L'autorità di controllo capofila. Si sceglie nella configurazione tra quelle che include il modulo.
- Se vuoi che le note interne, la motivazione di un rifiuto e la descrizione e le conseguenze delle violazioni vengano salvate cifrate, serve la variabile GDPR_FERNET_KEY sul server. La imposta chi lo amministra. Senza di essa questi testi vengono salvati in chiaro e **Encryption Key Configured** lo mostra.
- Per includere dati di vendita o del personale nell'esportazione per la portabilità, servono le app Vendite e Dipendenti installate.
- L'abbonamento a FlexigoTech Cloud o la sua prova di 14 giorni. Con esso, ogni giorno vengono monitorate sei fonti ufficiali e arriva un avviso quando una cambia.

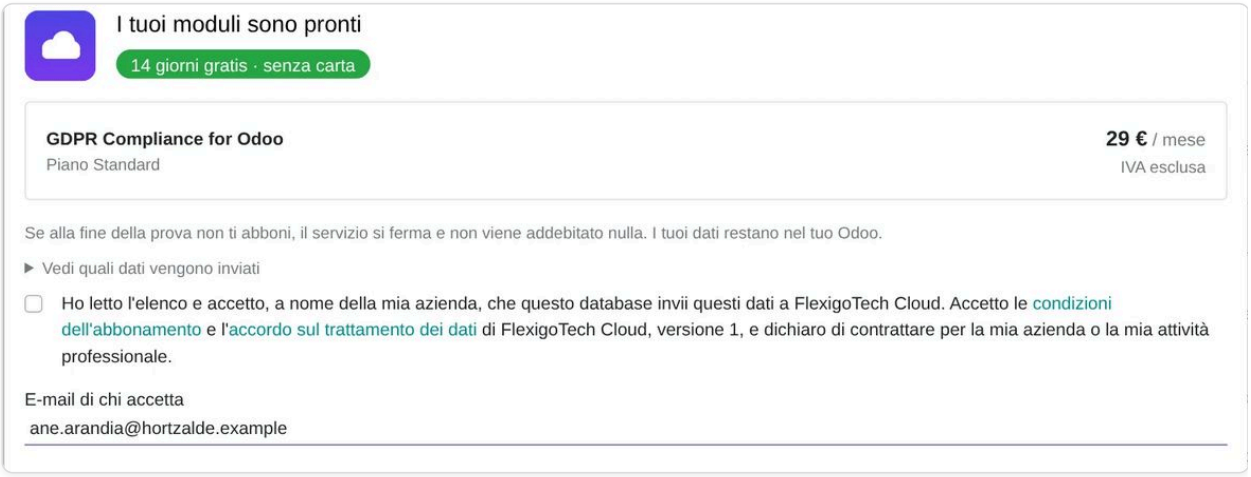
> Il modulo non elimina né anonimizza dati: il controllo di cancellazione conta quello che c'è e annota la tua decisione. Inoltre non notifica all'autorità di controllo né comunica nulla agli interessati: tu annoti qui quello che hai fatto. Non invia la lettera di risposta all'interessato. La decisione finale spetta al titolare o al suo DPO, e il modulo non è consulenza legale.

Si installa come qualsiasi modulo di Odoo di terze parti, su Odoo.sh o sul tuo server. Odoo installa insieme `flexigotech_cloud`, il collegamento con FlexigoTech Cloud, e le app di Odoo da cui dipende: Conversazioni e il portale.

5 La prova di FlexigoTech Cloud

1. **Premi Attiva nella barra in alto**

   Compare appena installi il modulo. Apre la finestra **Attiva FlexigoTech Cloud**, con il piano Standard e i suoi 14 giorni gratuiti, senza carta.



- **Schermata reale di Odoo 20.** La finestra di attivazione: leggi l'elenco dei dati, spunta la casella e inserisci la tua e-mail.

2 **Accetta e inserisci la tua e-mail**

Spunta «Ho letto l'elenco e accetto, a nome della mia azienda...» (include le condizioni dell'abbonamento e il contratto di trattamento dei dati) e scrivi l'**E-mail di chi accetta**.

3 **Premi Connetti e inizia la prova**

Odoo registra la base su FlexigoTech Cloud e avvia la prova del modulo. Se preferisci rimandare, **Più tardi** chiude la finestra.

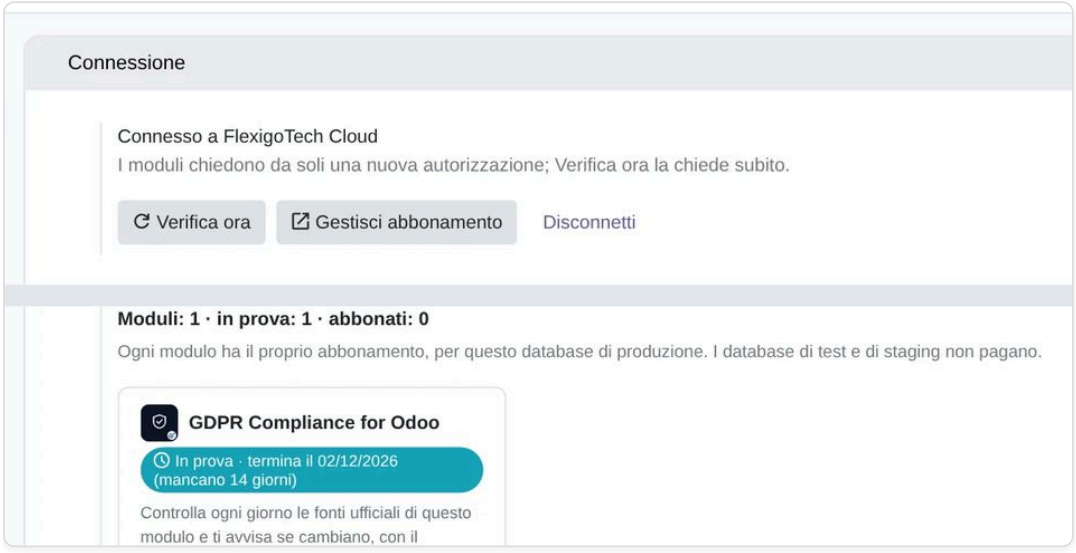
Lo stesso, dalle Impostazioni

In **Impostazioni › FlexigoTech Cloud** c'è l'elenco completo di ciò che la base invia. Spunta la casella, inserisci l'e-mail e premi **Accetta e connetti**. Se hai già un account su app.flexigotech.com, il campo **Hai un codice dal tuo account?** collega la base a quell'account (il codice vale 10 minuti).



- **Schermata reale di Odoo 20.** Impostazioni › FlexigoTech Cloud, prima di connettere: la casella spuntata, l'e-mail e **Accetta e connetti**.

Con la base connessa, il blocco **Moduli** mostra ogni modulo con il suo stato: **In prova** e la data di scadenza, **Abbonato**, ecc. Da lì si sceglie il piano (Standard o Pro, mensile o annuale) e si preme **Abbonati**: il pagamento avviene nella pagina di Stripe, fuori da Odoo.



- **Schermata reale di Odoo 20.** Impostazioni › FlexigoTech Cloud con la base connessa e il modulo in prova.

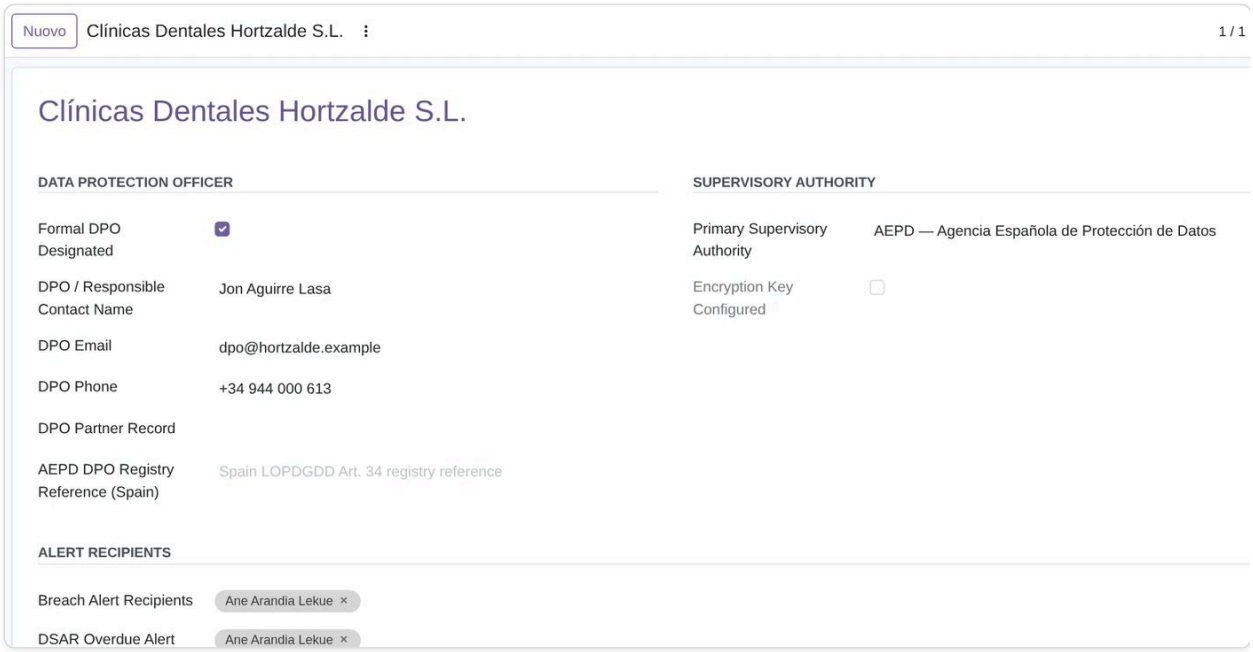
Prezzi IVA esclusa. Se al termine della prova non ti abboni, il servizio si ferma e non viene addebitato nulla; i tuoi dati restano nel tuo Odoo. **Verifica ora** richiede il permesso subito (altrimenti il modulo lo rinnova da solo ogni 6 ore).

> In una copia neutralizzata (staging) o in un database con dati dimostrativi non si può avviare una prova: Impostazioni lo segnala con «Questo database è una copia neutralizzata o ha dati dimostrativi, quindi qui non si possono avviare prove.»

6 Messa in funzione passo passo

1 Apri la configurazione

Vai a **GDPR Toolkit › Configuration › DPO & Settings**. Si apre la configurazione GDPR della tua società; se non ne ha ancora una, Odoo la crea con i valori predefiniti.



- **Schermata reale di Odoo 20.** La configurazione del GDPR dell'azienda, con i dati del DPO, l'autorità di controllo e chi riceve gli avvisi.

2 Compila i dati del DPO

Completa **DPO / Responsible Contact Name**, **DPO Email** e **DPO Phone**. Se non c'è un DPO designato, deseleziona **Formal DPO Designated**.

3 Scegli l'autorità di controllo

Seleziona la **Primary Supervisory Authority**.

4 Indica chi riceve gli avvisi

Compila **Breach Alert Recipients** e **DSAR Overdue Alert Recipients**. Se non indichi nessuno, gli avvisi arrivano a chi ha **GDPR Toolkit / Manager** in azienda.

5 Regola i giorni di anticipo

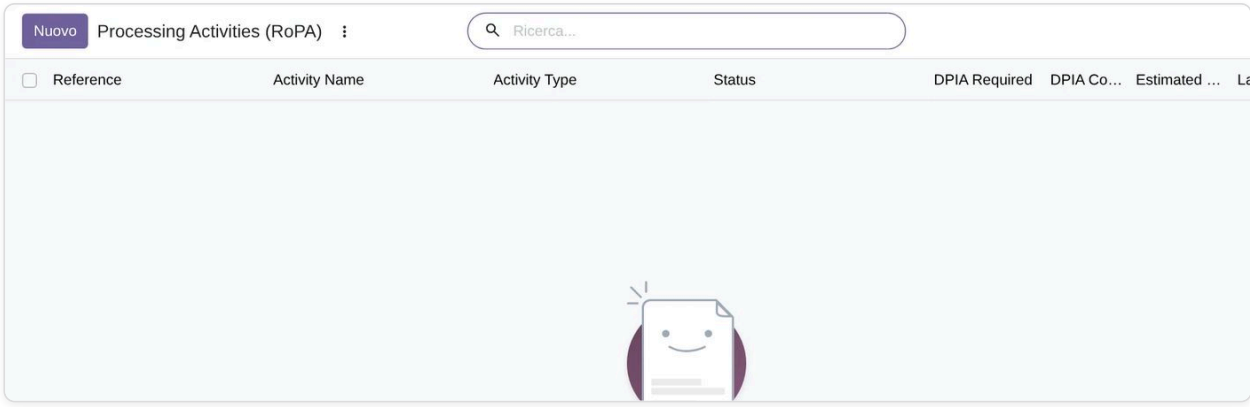
Controlla **Retention Advance Warning (days)**, che è impostato a 30, e **DSAR Reminder Days Before Deadline**, che è impostato a 7.

6 Assegna i gruppi

Assegna **GDPR Toolkit / Manager** e **GDPR Toolkit / User** a chi ne ha bisogno.

7 Crea la prima attività

Vai a **GDPR Toolkit › Processing Activities (RoPA) › All Activities**. All'inizio l'elenco è vuoto. Premi **Nuovo** e compila l'attività.



- **Schermata reale di Odoo 20.** L'elenco delle attività di trattamento, ancora senza nessuna.

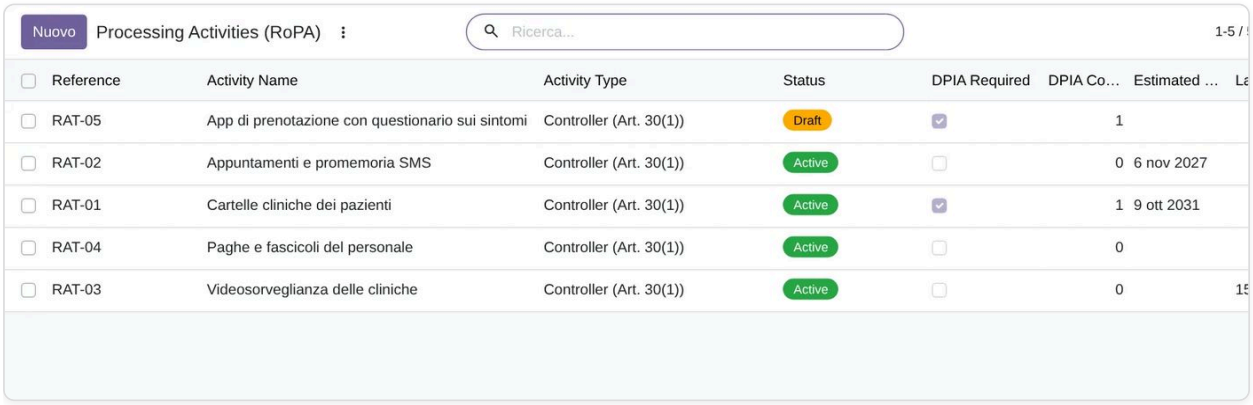
8 Fornisci l'indirizzo del portale

Se vuoi che gli interessati facciano richieste dal portale, dai a ciascuno con account del portale l'indirizzo /my/privacy-rights del tuo Odoo. Il modulo non mette un link nella pagina Il mio account.

Dopo questo, le attività pianificate lavorano da sole. Ogni giorno partono i promemoria delle richieste che scadono presto e si controlla la fine della conservazione. Ogni ora, nelle ultime 6 ore del termine di una violazione, parte il suo avviso. Ogni settimana parte il riepilogo delle richieste fuori termine e, una volta l'anno, il promemoria di rivedere il registro delle attività. Il promemoria di una richiesta va alla persona assegnata; gli altri avvisi, ai destinatari che hai indicato o, se non ci sono, ai gestori GDPR dell'azienda.

GUIDA DEL MODULO · GDPR COMPLIANCE

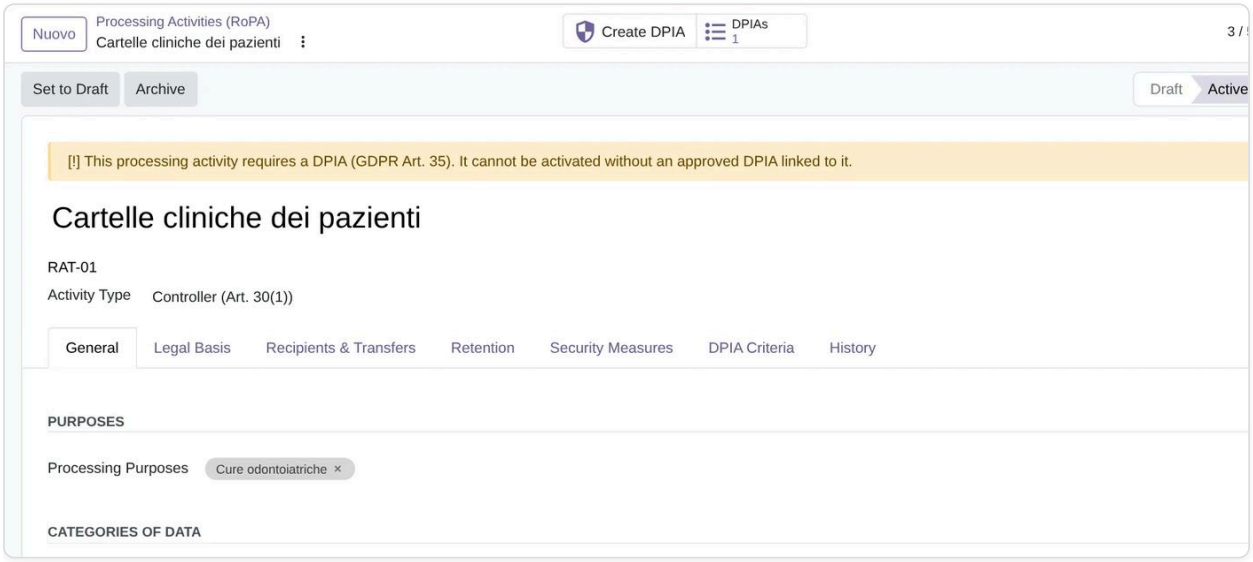
7 Il registro delle attività di trattamento



- **Schermata reale di Odoo 20.** L'elenco **Processing Activities (RoPA)** con le sue cinque attività.

Ogni scheda raccoglie ciò che richiede l'art. 30.1 se agisci come titolare o l'art. 30.2 se agisci come responsabile. Lo scegli in **Activity Type**. Compili finalità, categorie di interessati, di dati e di destinatari, la base giuridica dell'art. 6 e quella dell'art. 9, i trasferimenti verso paesi terzi con la relativa garanzia, la conservazione e le misure di sicurezza.

Le categorie di dati, di interessati e di destinatari si scelgono dagli elenchi di **GDPR Toolkit › Configuration › Categories of Data**, **GDPR Toolkit › Configuration › Categories of Data Subjects** e **GDPR Toolkit › Configuration › Categories of Recipients**. Le finalità si creano scrivendole direttamente nella scheda. Il campo **Reference** lo imposta Odoo alla creazione dell'attività e non è modificabile.



- **Schermata reale di Odoo 20.** La scheda di un'attività con le sue schede.

Set Active	Porta l'attività in **Active**. Non appare quando è già attiva.
Set to Draft	Riporta l'attività in **Draft**. Appare solo quando è attiva.
Archive	Porta l'attività in **Archived**. Non appare quando è già archiviata.

Stati

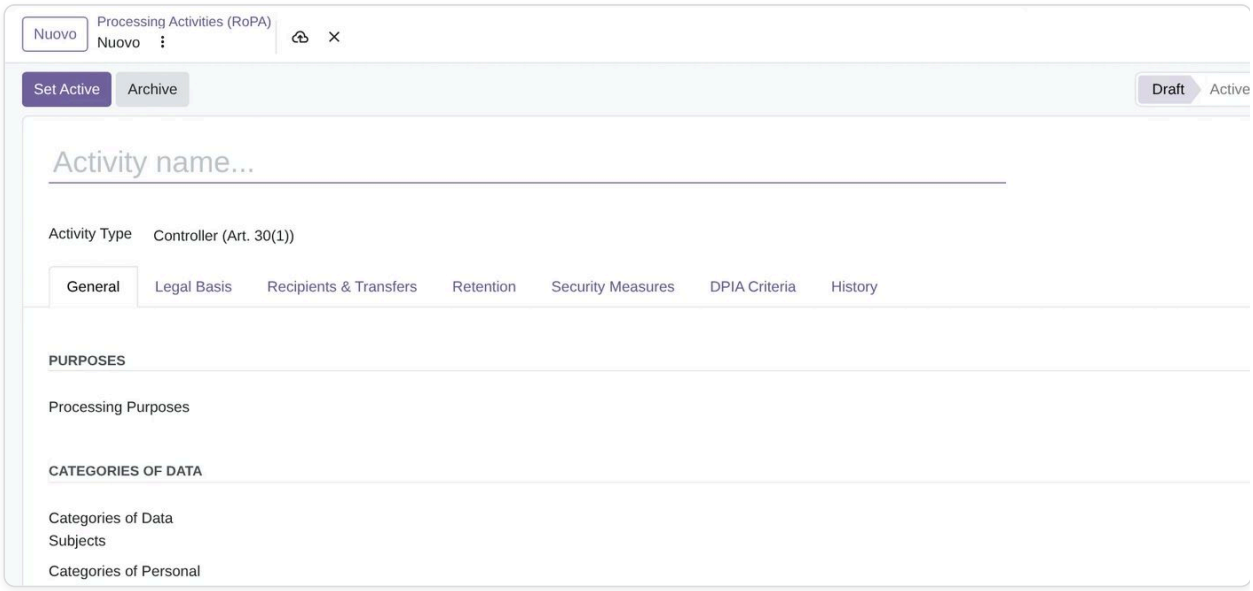
- **Draft**: lo stato con cui nasce l'attività.
- **Active**: l'attività che è in vigore.
- **Archived**: l'attività che non si usa più. Resta nel registro.

History

Ogni volta che si crea o si salva una modifica all'attività, il modulo aggiunge una voce allo storico, che si vede nella scheda **History**. Quelle voci non si possono modificare né eliminare.

Creare un'attività

1. **Crea l'attività**
   Nell'elenco **Processing Activities (RoPA)** premi **Nuovo**.



- **Schermata reale di Odoo 20.** Il modulo di una nuova attività in stato **Draft**.

2 **Compila le schede**

Completa **General**, **Legal Basis**, **Recipients & Transfers**, **Retention** e **Security Measures**.

3 **Attivala**

Premi **Set Active**.

> Un'attività non si elimina: il modulo lo impedisce per conservare la traccia di audit, e va archiviata con **Archive**. Inoltre non si può attivare un'attività che richiede una DPIA se non ha collegata una DPIA approvata.

Cosa significa ogni stato

Draft	Stato iniziale. Puoi compilare e correggere la scheda mentre la completi.
Active	L'attività è in vigore. Per arrivarci, se richiede una DPIA, deve avere collegata una DPIA approvata. Da qui, **Set to Draft** la riporta in **Draft**.
Archived	L'attività viene ritirata dall'uso, ma la sua scheda e il suo storico si conservano. È l'unico modo per toglierla, perché non si può eliminare.

Quando il modulo non ti lascia fare qualcosa

- Attivare un'attività con **DPIA Required** senza una DPIA approvata collegata: compare «Cannot activate processing activity "...": a DPIA is required but no approved DPIA is linked. Please complete and approve a DPIA first.»
- Eliminare un'attività: compare «Processing activity records cannot be deleted to preserve the audit trail. Please archive the record instead.»
- Modificare o eliminare una voce della cronologia: compaiono «History records are immutable and cannot be deleted. They are part of the GDPR audit trail.» e «History records are immutable.».

Quando la DPIA è obbligatoria

DPIA Required si segna da sola quando si verificano due o più dei criteri della scheda **DPIA Criteria**, oppure quando la si forza a mano con **DPIA Required (Manual Override)**. Quella regola dei due criteri deriva dalle linee guida WP248 rev.01 ed è una prassi generale, non un obbligo di legge. I criteri sono **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** e **Prevents exercise of rights**. **DPIA Criteria Met** mostra quanti se ne verificano e **DPIA Requirement Reason** riporta la motivazione.

Schede e campi del modulo

General	**Activity Name**, **Activity Type**, i gruppi **Purposes** e **Categories of Data** e i dati del responsabile, che vanno in un gruppo proprio, **Processor Details (Art. 30(2))**.
Legal Basis	**Legal Basis (Art. 6)** e **Special Category Legal Basis (Art. 9)**.
Recipients & Transfers	**Categories of Recipients**, **Third-Country Transfer**, **Third Countries**, **Transfer Safeguard** e **Safeguard Notes**.
Retention	**Retention Duration**, **Retention Unit** e **Retention Reference Point**, oltre a **Reference Date (fixed)**, **Last Transaction Date**, **Estimated Retention End Date** e **Last Retention Review**.
Security Measures	**Technical & Organisational Security Measures**.
History	**Version History**: una voce per ogni modifica.

Le opzioni di **Transfer Safeguard** sono **Adequacy Decision**, **Standard Contractual Clauses (SCC)**, **Binding Corporate Rules (BCR)**, **EU-US Data Privacy Framework (DPF)**, **Other Safeguard** e **No Safeguard (document justification)**. In **Safeguard Notes** si annota il riferimento delle SCC, il numero di certificazione del DPF o la motivazione. **Retention Reference Point** ammette **From End of Contract**, **From Last Transaction**, **From Withdrawal of Consent**, **Fixed Date** e **Other**.

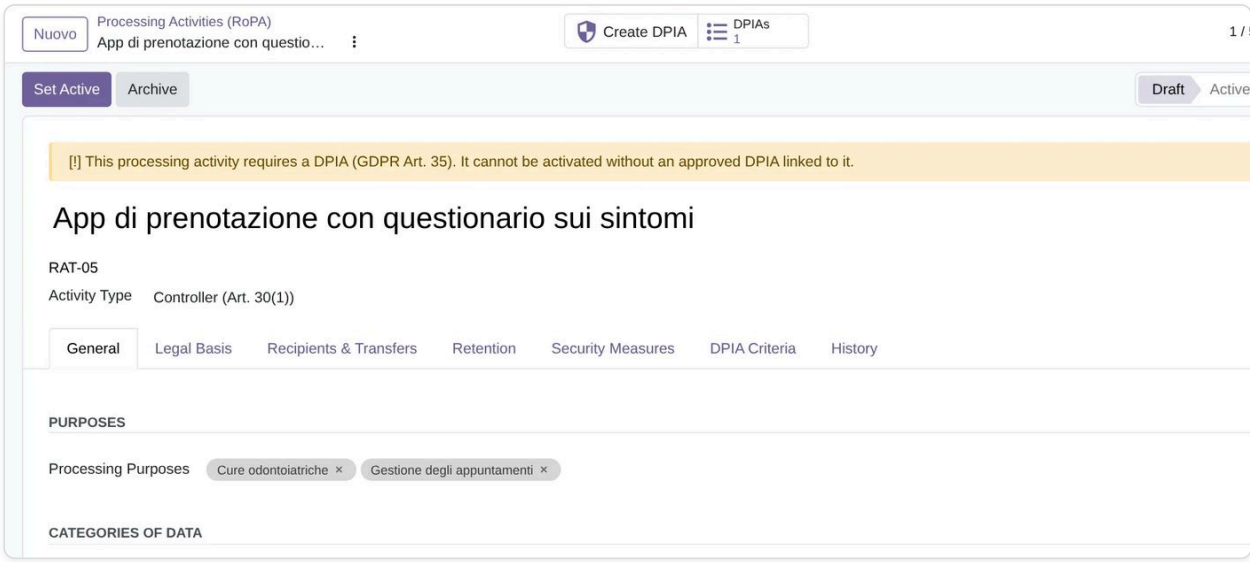
Filtri ed elenchi correlati

La ricerca ha i filtri **Active**, **Draft** e **DPIA Required**, e i raggruppamenti **By Type** e **By Status**. Il menu **GDPR Toolkit › Processing Activities (RoPA) › DPIA Required** apre le attività che la richiedono. Il menu **GDPR Toolkit › Retention Management › Retention Schedule** apre quelle con un termine di conservazione impostato.

Esempio dall'inizio alla fine

Le schermate di esempio mostrano uno studio dentistico con cinque attività. Una, la cartella clinica dei pazienti, è attiva e richiede una DPIA. Un'altra, l'app di prenotazione online con questionario sui sintomi, è ancora in **Draft** e richiede anch'essa la DPIA.

1. **Crea e compila**
   Premi **Nuovo**, scrivi il nome e compila finalità, interessati, dati, base giuridica, conservazione e misure di sicurezza.



- **Schermata reale di Odoo 20.** L'attività in **Draft**, con l'avviso che richiede una DPIA.

2 **Prova ad attivarla**

Premi **Set Active**. Finché non c'è una DPIA approvata collegata, il modulo lo impedisce e compare il messaggio di errore.

3 **Risolvi la DPIA**

Il pulsante per creare la DPIA, in alto nella scheda dell'attività, apre una DPIA nuova già collegata ad essa. Quando viene approvata, puoi attivare l'attività.

4 **Controlla lo storico**

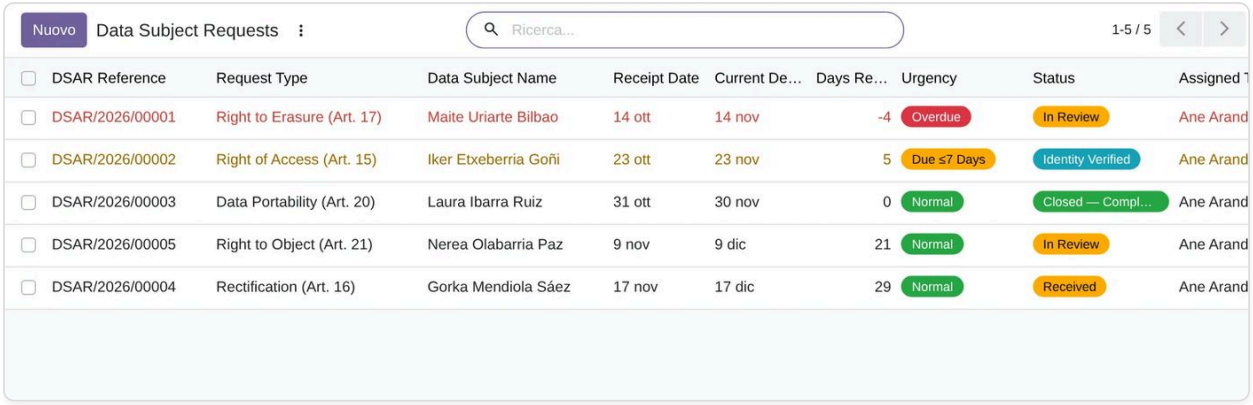
Ogni modifica resta nella scheda **History**.

GUIDA DEL MODULO · GDPR COMPLIANCE

8 Le richieste degli interessati e i loro termini

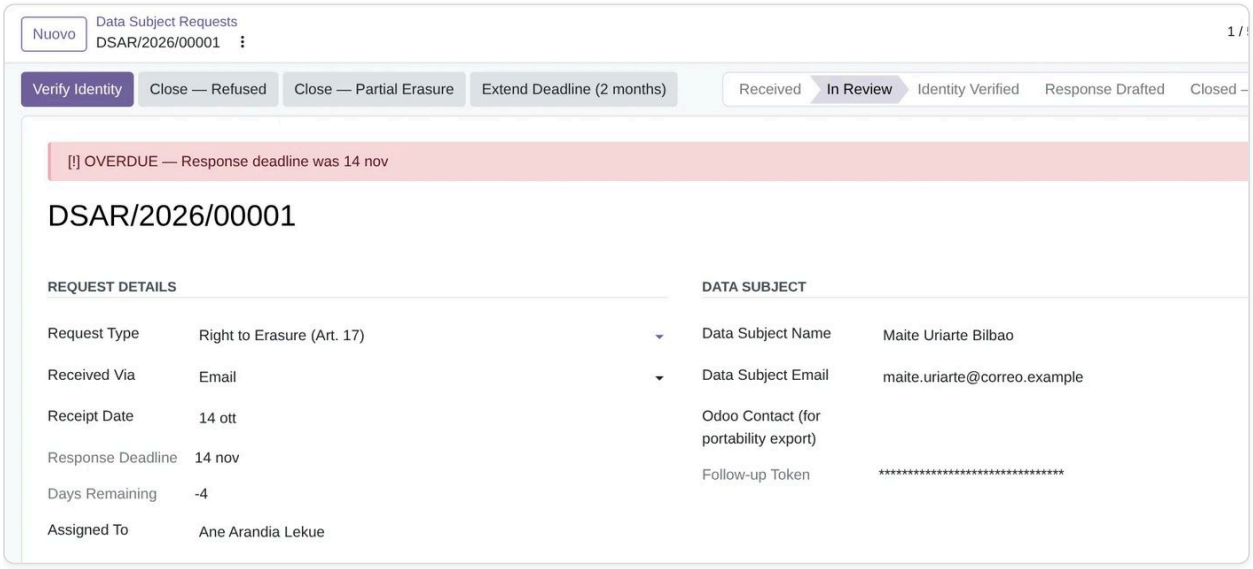
Ci sono sei tipi di richiesta: **Right of Access (Art. 15)**, **Rectification (Art. 16)**, **Right to Erasure (Art. 17)**, **Restriction of Processing (Art. 18)**, **Data Portability (Art. 20)** e **Right to Object (Art. 21)**. Il **Received Via** può essere **Portal Submission**, **Email**, **Letter**, **Phone** o **Manual Entry**.

Il **Response Deadline** è un mese dalla **Receipt Date** (art. 12.3 del GDPR). Se serve, si può prorogare di altri due mesi, sempre ai sensi dell'art. 12.3, e allora il **Current Deadline** diventa quello prorogato. La colonna **Days Remaining** conta fino a quel termine vigente.



- **Schermata reale di Odoo 20.** L'elenco delle richieste con il termine vigente, i giorni rimanenti, l'urgenza e la persona assegnata.

L'elenco **Overdue** mostra le richieste aperte il cui termine è già scaduto, e l'elenco **Due This Week** quelle che scadono entro sette giorni. La colonna **Urgency** distingue questi due casi dagli altri, che compaiono come **Normal**.



- **Schermata reale di Odoo 20.** Una richiesta con l'avviso di fuori termine e i pulsanti del suo stato.

La persona che segue ogni richiesta è indicata in **Assigned To**. La scheda **Identity Verification** registra il metodo, la data e chi l'ha verificata. Nella scheda **Response** c'è la **Response Letter**: **Load Response Template** la compila con il modello generale e, come **Draft Response**, porta la richiesta a **Response Drafted**. **Generate Refusal Letter** predispone la lettera di rifiuto senza cambiare lo stato. La lettera non viene inviata dal modulo.

Per rifiutare, la scheda **Refusal** chiede la **Refusal Legal Basis** e la **Refusal Justification**. Senza motivazione non si può chiudere come rifiutata.

Pulsanti del registro

Start Review	Porta la richiesta da **Received** a **In Review**.
Verify Identity	Porta da **In Review** a **Identity Verified**.
Draft Response	Porta da **Identity Verified** a **Response Drafted** e carica il modello.
Close — Completed	Chiude una richiesta con la risposta redatta.
Close — Refused	Si vede in revisione, con l'identità verificata o con la risposta redatta.

Close — Partial Erasure	Solo nelle richieste di cancellazione, negli stessi stati.
Extend Deadline (2 months)	Si vede finché la richiesta è aperta e non è stata prorogata. Chiede il motivo.

Stati

Gli stati sono **Received**, **In Review**, **Identity Verified** e **Response Drafted**. Una richiesta si chiude come completata, come rifiutata o con cancellazione parziale. Gli stati possono solo avanzare: non si può tornare a uno precedente.

Promemoria

L'attività pianificata **GDPR: DSAR Deadline Reminder** viene eseguita ogni giorno e invia un'email quando a una richiesta aperta mancano i giorni di **DSAR Reminder Days Before Deadline**: alla persona assegnata; se non ha un'email, ai gestori GDPR; e se nemmeno così, all'email dell'azienda. Se non arriva a nessuno, lo annota nella richiesta. L'attività pianificata **GDPR: DSAR Overdue Escalation** viene eseguita ogni settimana e invia il riepilogo delle richieste fuori termine ai **DSAR Overdue Alert Recipients** o, in mancanza, ai gestori GDPR.

> Una richiesta non si elimina: si archivia. Non si può tornare a uno stato precedente. Solo i gestori GDPR possono usare i pulsanti della richiesta.

Gli stati, uno per uno

- **Received**: la richiesta è appena arrivata. Si vede solo **Start Review**.
- **In Review**: qualcuno la sta esaminando. Si può **Verify Identity**, chiuderla come rifiutata, chiuderla con cancellazione parziale (se è di cancellazione) o prorogare il termine.
- **Identity Verified**: risulta chi è l'interessato. Si può **Draft Response**, e da qui anche chiudere come rifiutata o prorogare il termine.
- **Response Drafted**: la lettera è pronta. Si può **Close — Completed** oppure chiudere come rifiutata.
- Chiusa come completata: risposta data e chiusa.
- Chiusa come rifiutata: chiusa con la sua base e la sua motivazione.
- Chiusa con cancellazione parziale: solo nelle cancellazioni, quando qualcosa viene conservato.
- Chiusa con termine prorogato: non ha pulsante. Prorogare il termine lascia la richiesta nel suo stato e cambia il **Current Deadline**.

Regole e condizioni

- Lo stato non torna indietro. Se ci provi, Odoo dice «DSAR status cannot be moved backwards. The audit trail must be append-only.»
- Quando prolunghi il termine devi scrivere il motivo. Altrimenti compare «Extension reason is required when extending the deadline.»
- Per chiudere come rifiutata serve la motivazione. Se manca, compare «Refusal justification is required before closing as refused.»
- **Generate Portability Export** compare solo nelle richieste di accesso e di portabilità con l'identità verificata. Se si prova senza verifica, compare «Identity must be verified before generating a portability export.»
- **Retention Conflict Check** esiste solo nelle richieste di cancellazione. In un altro tipo compare «Retention conflict check only applies to erasure requests.»

- Una richiesta non si può eliminare: compare «DSAR records cannot be deleted. Archive them instead (GDPR Manager / Admin only).»
- I pulsanti funzionano solo con il gruppo di gestore GDPR o con un amministratore. Altrimenti compare «Only GDPR Managers can perform this action.»
- **Load Response Template**, nella scheda **Response**, fa la stessa cosa di **Draft Response**: carica il modello generale e porta la richiesta a **Response Drafted**, anche se è ancora in **Received** o in **In Review**. Usalo quando hai già verificato l'identità.

Il controllo per la cancellazione

Retention Conflict Check conta le fatture pubblicate, le schede dipendente (con l'app Dipendenti) e gli ordini di vendita (con Vendite) del contatto della richiesta. Ti permette di scegliere se conservare o cancellare ogni gruppo e, con **Record Decision & Close DSAR**, annota la tua decisione nelle note interne e chiude la richiesta: completata se tutto è da cancellare, con cancellazione parziale se qualcosa viene conservato. Il modulo non cancella né anonimizza nulla: quello lo fai tu in Odoo.

La scheda: gruppi e schede

Request Details	Il tipo, il canale, la data di ricezione, il termine di risposta, i giorni rimanenti e la persona assegnata.
Data Subject	Il nome e l'email dell'interessato, il contatto di Odoo per l'esportazione di portabilità e il token di tracciamento.
Extension	**Deadline Extended**, **Extension Reason**, **Extended Deadline (3 months)** ed **Extension Notification Due**, che è la stessa data del termine iniziale: un mese dalla ricezione.
Identity Verification	La casella di identità verificata, il metodo, la data e chi l'ha verificata.
Response	La lettera di risposta e i file dell'esportazione di portabilità.
Refusal	La base giuridica e la motivazione del rifiuto.
Internal Notes	Note della persona che segue il caso.

La base del rifiuto può essere **Manifestly Unfounded (Art. 12(5)(a))**, **Manifestly Excessive (Art. 12(5)(a))**, **Legal Exemption (Art. 23)** o **Other**. Le note interne e la motivazione vengono salvate cifrate solo se il server ha la chiave di cifratura. Senza di essa vengono salvate in chiaro. La configurazione lo mostra in **Encryption Key Configured**.

Promemoria e filtri

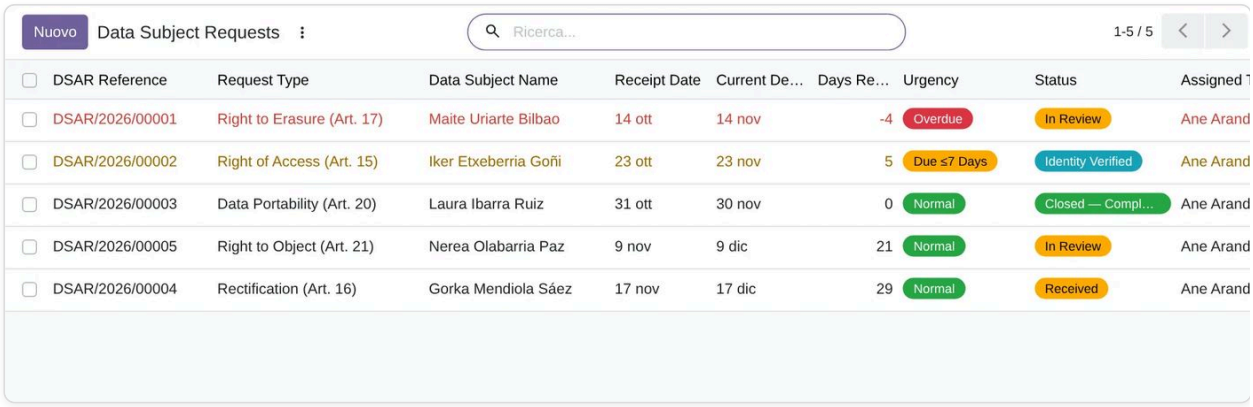
I filtri dell'elenco sono **Open**, **Overdue**, quello delle richieste in scadenza entro sette giorni o meno, **Erasure Requests** e **Access Requests**, con raggruppamenti **By Status** e **By Type**. In **GDPR Toolkit › Reports** trovi il **DSAR History Report**.

L'unica e-mail all'interessato che parte da sola è la conferma di ricezione di una richiesta fatta dal portale. La lettera di risposta non viene inviata dal modulo: la compili qui e la invii tu con il mezzo che usi.

Un esempio dall'inizio alla fine

1 Arriva la richiesta

Maite Uriarte Bilbao chiede la cancellazione dei suoi dati. Odoo imposta il **Response Deadline** un mese dopo la **Receipt Date**.



- **Schermata reale di Odoo 20.** L'elenco con la richiesta di cancellazione, quella di accesso, quella di portabilità e altre due.

2 Il termine scade

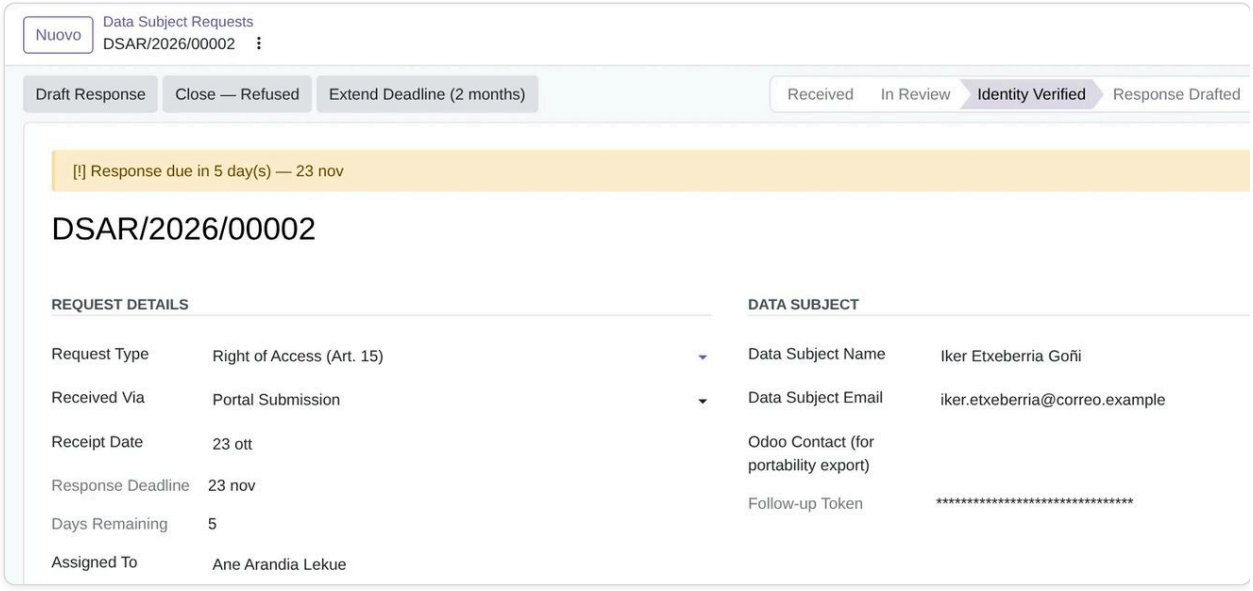
Nessuno l'ha chiusa e il termine è già passato: **Days Remaining** indica -4, la scheda segnala che è fuori termine e la richiesta compare in **Overdue**.



- **Schermata reale di Odoo 20.** L'elenco delle richieste fuori termine, con una sola richiesta.

3 Un'altra richiesta è in scadenza

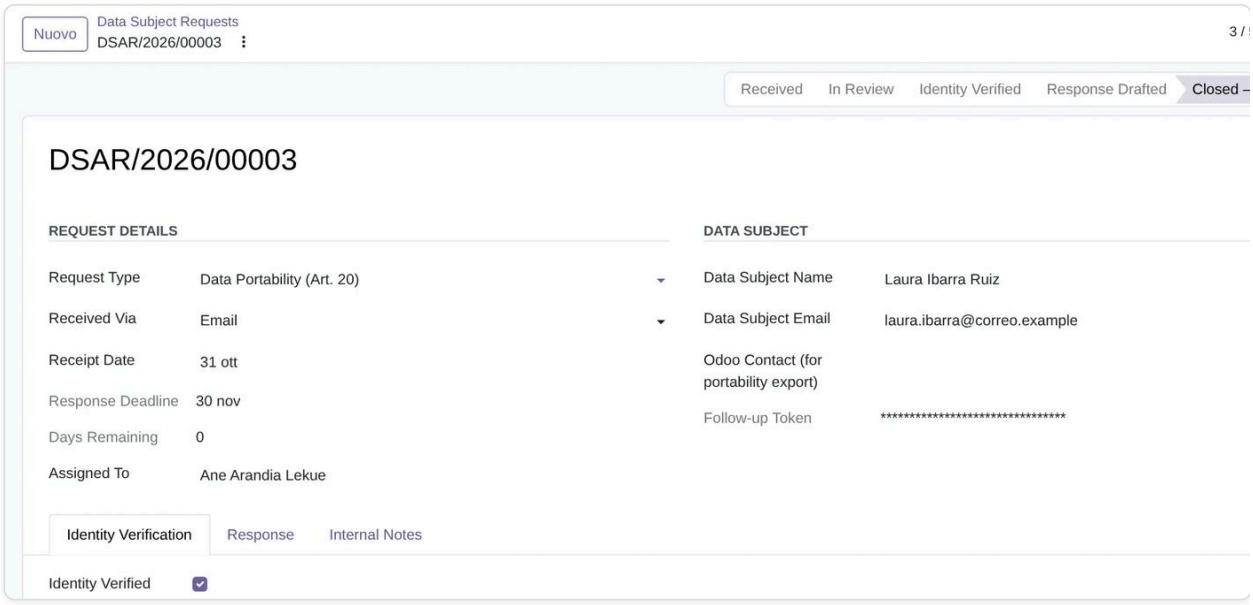
Iker Etxeberria Goñi ha chiesto l'accesso ai suoi dati. La sua richiesta ha ancora 5 giorni e ha l'identità verificata: compare in **Due This Week**.



- **Schermata reale di Odoo 20.** Una richiesta che scade tra 5 giorni, con l'identità verificata.

4 Si chiude

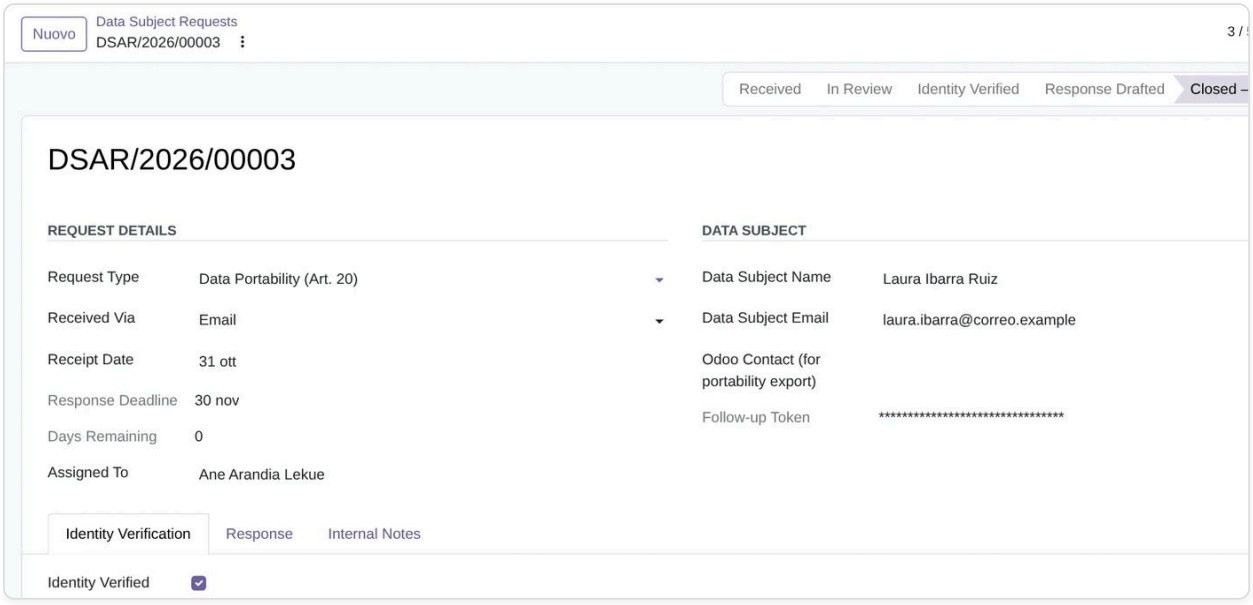
La richiesta di portabilità di Laura Ibarra Ruiz ha l'identità verificata ed è chiusa come completata.



- **Schermata reale di Odoo 20.** Una richiesta di portabilità chiusa come completata.

GUIDA DEL MODULO · GDPR COMPLIANCE

9 Portabilità, cancellazione e portale della privacy



- **Schermata reale di Odoo 20.** Una richiesta di portabilità con l'identità verificata, già chiusa come completata.

Esportazione di portabilità

L'esportazione si genera a mano dalla richiesta, con una procedura guidata. Non c'è nessuna attività pianificata che la prepari. Servono due cose: l'identità verificata e un contatto Odoo collegato alla richiesta.

DSAR	La richiesta da cui si esporta. È obbligatoria.
Contact Data (res.partner)	Casella selezionata per impostazione predefinita. Include i dati della scheda del contatto.
Order History (sale.order)	Include gli ordini del contatto. Solo con l'app Vendite installata.

HR Data (hr.employee)	Include la scheda dipendente. Solo con l'app Dipendenti installata.
I confirm explicit HR data inclusion	Casella di conferma che accompagna i dati HR.
Export Format	Due opzioni: **JSON (machine-readable)** o **CSV**.
Export File	Il file generato, quando l'esportazione è pronta.
Generate Export	Crea il file. Si nasconde quando l'esportazione è già stata fatta.
Close	Chiude la procedura guidata.

Verifica dei conflitti di cancellazione

In una richiesta di cancellazione, **Retention Conflict Check** conta ciò che esiste del contatto: fatture registrate, schede dipendente e ordini di vendita, a seconda delle app installate. La procedura guidata mostra i gruppi **Data Subject**, **Conflict Findings** e **Your Decision per Category**. Per ogni categoria scegli **Retain (legal obligation)** oppure **Erase / Anonymise**. Quella di marketing e consenso è impostata su **Erase / Anonymise** per impostazione predefinita.

Con **Record Decision & Close DSAR** la decisione viene annotata nelle note interne e la richiesta viene chiusa: come completata se tutto è da cancellare e con cancellazione parziale se qualcosa viene conservato. **Cancel** esce senza registrare nulla.

Portale della privacy

Il portale si trova in /my/privacy-rights del tuo Odoo e richiede l'accesso, quindi l'interessato ha bisogno di un account del portale. Il modulo non aggiunge un link in Il mio account: l'indirizzo lo fornisci tu. Il modulo richiede il tipo di diritto, un testo fino a 2.000 caratteri e fino a 3 documenti da 50 MB. All'invio parte la conferma di ricezione via e-mail e compare una pagina di stato con un link proprio, che mostra il tipo e lo stato senza dati personali.

> Il modulo non cancella né anonimizza dati: la verifica di cancellazione conta solo ciò che esiste e annota la tua decisione. Cancellare o anonimizzare lo fai tu in Odoo. Non invia nemmeno la lettera di risposta.

Cosa succede nell'esportazione di portabilità

Il diritto alla portabilità è quello dell'art. 20.1 del GDPR: ricevere i dati forniti dall'interessato in un formato strutturato, di uso comune e leggibile da dispositivo automatico. Per questo la procedura guidata offre JSON o CSV.

La procedura guidata si rifiuta di generare l'esportazione in tre casi:

- Se l'identità non è verificata: «Identity must be verified before generating a portability export.»
- Se la richiesta non ha un contatto Odoo: «No Odoo contact linked to this DSAR. Please link a res.partner record first.» Collegalo nel campo **Odoo Contact (for portability export)** della richiesta.
- Se i dati del contatto sono già stati anonimizzati, la procedura guidata avvisa che i dati dell'interessato sono già stati anonimizzati, che serve una gestione manuale e che bisogna contattare il DPO.

I dati di contatto sono selezionati. Gli ordini entrano solo con l'app Vendite installata: fino a 500, della società della richiesta. I dati HR entrano solo con l'app Dipendenti installata e la casella di conferma selezionata: la scheda dipendente di quella persona, con la sua mansione, il suo reparto e i suoi dati privati di contatto.

Quando l'esportazione termina

Al generarlo, l'assistente avvisa che il file è pronto e allegato alla richiesta e mostra l'**Export File**. Il file resta anche nella scheda **Response** della richiesta.

Stati della richiesta e scadenze

Il termine per rispondere è di un mese dal ricevimento della richiesta e, se necessario, può essere prorogato di altri due mesi; la proroga e i suoi motivi vanno comunicati all'interessato entro quel primo mese (art. 12.3). Il modulo non invia questo avviso: lo invii tu, prima della **Extension Notification Due**.

Extend Deadline (2 months) richiede il motivo e non cambia lo stato della richiesta: cambia solo la **Current Deadline**, portandola alla data prorogata. Nessun pulsante porta allo stato di chiusa con scadenza prorogata.

Regole del controllo di cancellazione

L'assistente si apre solo sulle richieste di cancellazione e guarda il contatto di Odoo collegato alla richiesta; senza contatto non trova nulla da contare. Conta fatture pubblicate, schede dipendente e ordini di vendita di quel contatto. Gli ultimi due gruppi dipendono dalla presenza delle app Dipendenti e Vendite. Ogni gruppo ha la sua casella di avviso: **Pending / Recent Invoices Found**, **Active HR Records Found** e **Active Orders Found**. Il **Conflict Summary** riporta il conteggio in forma di testo.

Le decisioni si prendono per gruppo: **Invoice Data Decision**, **HR Data Decision**, **Order Data Decision** e **Marketing / Consent Data Decision**. Nei primi tre scegli tra **Retain (legal obligation)** e **Erase / Anonymise**; in quello di marketing, tra **Retain** e **Erase / Anonymise**.

Quando registri la decisione, la richiesta si chiude come completata se tutto va cancellato, e con cancellazione parziale se qualche gruppo viene conservato. Il modulo annota la decisione solo nelle note interne. Il riepilogo dell'assistente è in inglese e cita termini di conservazione della legge spagnola: rivedili con il tuo DPO, perché non valgono per tutti i paesi.

Il portale e i suoi limiti

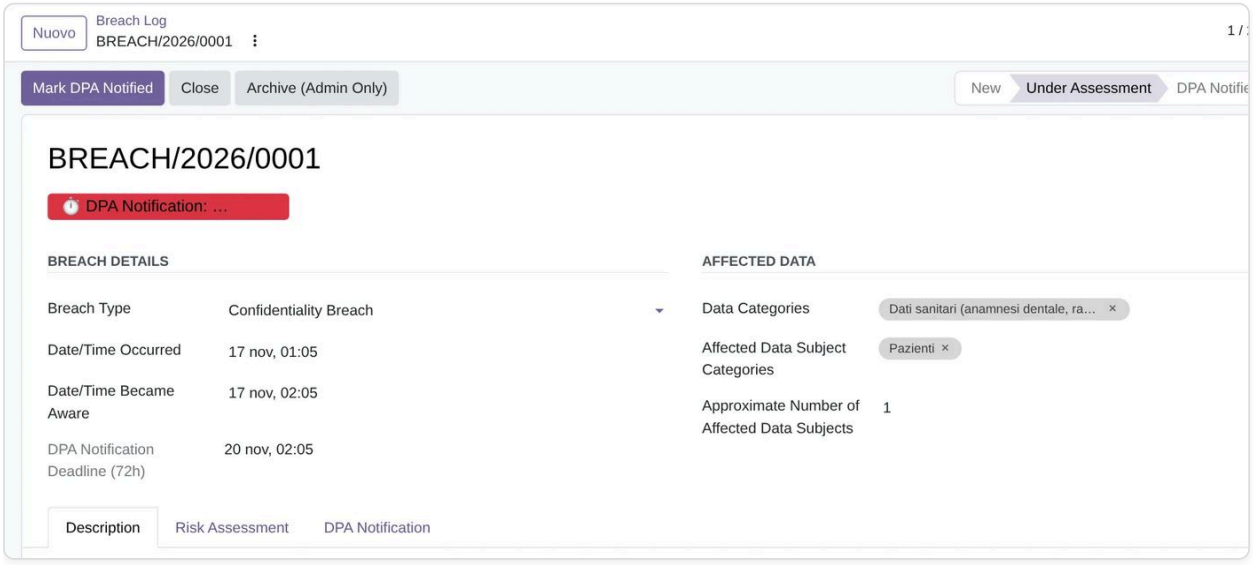
Il portale pone due limiti per persona. Con 3 richieste in un giorno non consente di inviarne altre fino al giorno successivo. Con 5 in sette giorni smette di accettarle, annota un segnale di revisione nelle note del contatto e gli chiede di contattare la tua azienda. Decidere se una richiesta è manifestamente infondata o eccessiva spetta al titolare del trattamento (art. 12.5).

Chi apre il link di stato vede solo il tipo e lo stato della propria richiesta, senza dati personali. L'unica email che parte da sola verso l'interessato è la conferma di ricezione di una richiesta fatta dal portale; la lettera di risposta la redigi e la invii tu.

Un esempio dall'inizio alla fine

Laura Ibarra Ruiz ha chiesto la portabilità dei suoi dati. La sua richiesta ha l'identità verificata e il contatto di Odoo collegato. Apri l'assistente, lasci selezionati i dati di contatto, scegli JSON e premi **Generate Export**: il file resta in **Export File** e allegato alla richiesta. Poi le invii la risposta attraverso il tuo canale abituale e chiudi la richiesta come completata.

10 Il registro delle violazioni e le 72 ore



- **Schermata reale di Odoo 20.** Una violazione in valutazione, con il conto alla rovescia della scadenza e il pulsante **Mark DPA Notified**.

Le violazioni si trovano in **GDPR Toolkit › Breach Log › All Breaches**. Premi **Nuovo** per aprirne una. Il **Breach Reference** viene assegnato da Odoo al momento della creazione e non si può modificare. I dati li inserisci tu nel modulo. Nessun dato arriva dall'esterno.

Cosa compilare

Breach Type	Obbligatorio: **Confidentiality Breach**, **Integrity Breach**, **Availability Breach** o **Multiple Types**.
Date/Time Occurred	Quando è avvenuta la violazione.
Date/Time Became Aware	Obbligatorio. Da questo momento decorre il termine di notifica.
DPA Notification Deadline (72h)	Lo calcola Odoo a partire dalla data in cui si è venuti a conoscenza della violazione.
Breach Description e **Likely Consequences**	Testo libero, nella scheda **Description**.
Impact Score e **Likelihood Score**	Nella scheda **Risk Assessment** scegli ciascuno, da 1 a 5.

Il termine di 72 ore

L'art. 33.1 del GDPR richiede di notificare la violazione all'autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui se ne è venuti a conoscenza. Il modulo imposta questo termine di 72 ore a partire dalla **Date/Time Became Aware**. Quando apri il modulo vedi quanto resta, in ore e minuti; scaduto il termine compare «EXPIRED». Il conteggio viene calcolato all'apertura e non si aggiorna da solo a schermo. L'attività **GDPR: Breach Countdown Alert** gira ogni ora e, nelle ultime 6 ore del termine, avvisa via email finché la violazione non è segnata come notificata: ai **Breach Alert Recipients** o, se non ce ne sono, ai gestori del GDPR.

Rischio e comunicazione agli interessati

Con impatto e probabilità, Odoo calcola il **Risk Score** e il **Risk Level**: basso fino a 4, medio fino a 9, alto fino a 19 e critico da 20. Questa matrice è del modulo, non del GDPR. Con rischio alto o critico si attiva **Art. 34 Data Subject Notification Required**. La decisione finale spetta al titolare del trattamento o al suo DPO, e puoi annotarla in **DPO Final Art. 34 Determination**.

Stati e pulsanti

Start Assessment	Porta la violazione da **New** a **Under Assessment**.
Mark DPA Notified	Si vede solo in **Under Assessment**. Cambia lo stato in **DPA Notified** e annota data e ora. Il modulo non notifica nulla: il mezzo, il numero di riferimento e le prove li compili tu nella scheda **DPA Notification**.
Mark Data Subjects Notified	Si vede solo in **DPA Notified** e se la comunicazione dell'art. 34 è obbligatoria. Passa a **Data Subjects Notified** e annota la data. La comunicazione la fai tu fuori da Odoo; la prova va nella scheda **Art. 34 Notification**.
Close	Non è visibile in **New** e in **Closed**. Prima di chiudere, compila la scheda **Post-Breach Review**: causa radice, azioni correttive, misure preventive, chi approva e la data.
Archive (Admin Only)	Lo vede solo un amministratore di Odoo. Apre un assistente che richiede l'**Archive Reason**.

Gli stati sono **New**, **Under Assessment**, **DPA Notified**, **Data Subjects Notified** e **Closed**.

1. **Crea la violazione**
   Premi **Nuovo**, scegli il **Breach Type** e compila quando si è venuti a conoscenza della violazione.
2. **Valuta**
   Premi **Start Assessment** e assegna i punteggi di impatto e probabilità.
3. **Notifica tu e annota**
   Se serve, notifica tu stesso l'autorità e premi **Mark DPA Notified**.
4. **Comunica e chiudi**
   Se è obbligatorio, comunica tu stesso agli interessati e premi **Mark Data Subjects Notified**. Concludi con la revisione successiva e **Close**.

> Una violazione non si può eliminare: Odoo risponde «Breach records are append-only and cannot be deleted. Only an Odoo Administrator can archive a breach record with a written reason.» Solo un amministratore la archivia, e senza motivo compare «Archive reason is required.»

Gli stati, uno per uno

New	La violazione è appena stata registrata. Si può solo avviare la valutazione.
Under Assessment	Si assegnano i punteggi di impatto e probabilità. Da qui si segna come notificata all'autorità.

DPA Notified	Qualcuno conferma che la notifica è già avvenuta fuori da Odoo. Se il livello di rischio richiede la comunicazione dell'art. 34, si può segnare come comunicata agli interessati.
Data Subjects Notified	Resta annotato che la violazione è stata comunicata agli interessati.
Closed	La violazione è conclusa e non si può chiudere di nuovo.

Regole e condizioni

- **Start Assessment** si vede solo in **New**.
- **Mark DPA Notified** si vede solo in **Under Assessment**.
- **Mark Data Subjects Notified** si vede solo in **DPA Notified** e solo se la comunicazione dell'art. 34 è obbligatoria.
- **Close** non si vede né in **New** né in **Closed**.
- I pulsanti del flusso sono per il gruppo dei gestori del modulo; **Archive (Admin Only)** è solo per gli amministratori di Odoo.
- Se un utente senza questo permesso prova ad archiviare, compare «Only Odoo Administrators can archive breach records.»
- L'assistente di archiviazione richiede l'**Archive Reason**; senza di esso compare «Archive reason is required.»
- L'art. 33.1 richiede di notificare entro 72 ore, ove possibile. Se la notifica non avviene nei termini, deve essere accompagnata dai motivi del ritardo.

Il modulo si limita a cambiare lo stato e ad annotare la data. Non notifica l'autorità né comunica nulla agli interessati: lo fai tu, e qui conservi ciò che hai fatto.

La descrizione e le conseguenze vengono salvate cifrate solo se il server dispone della chiave di cifratura. Senza di essa vengono salvate in chiaro, e la configurazione lo mostra in **Encryption Key Configured**.

Campi e schede del record

Breach Details	Tipo, quando è avvenuta, quando se ne è venuti a conoscenza e termine di notifica all'autorità.
Affected Data	**Categories of Data**, **Affected Data Subject Categories** e **Approximate Number of Affected Data Subjects**.
Description	Descrizione, conseguenze e **Measures Taken / Proposed**.
Risk Assessment	Impatto, probabilità, punteggio e livello di rischio.
DPA Notification	**DPA Notification Date/Time**, **Notification Method**, **DPA Reference Number** e allegati.
Art. 34 Notification	Se è stata inviata, quando e gli allegati.
Post-Breach Review	Causa radice, azioni correttive, misure preventive, chi approva e data.

Nell'elenco, i filtri **High/Critical Risk** e **DPA Notification Pending** aiutano a vedere cosa manca. Il menu **Active Incidents** apre le violazioni non ancora chiuse.

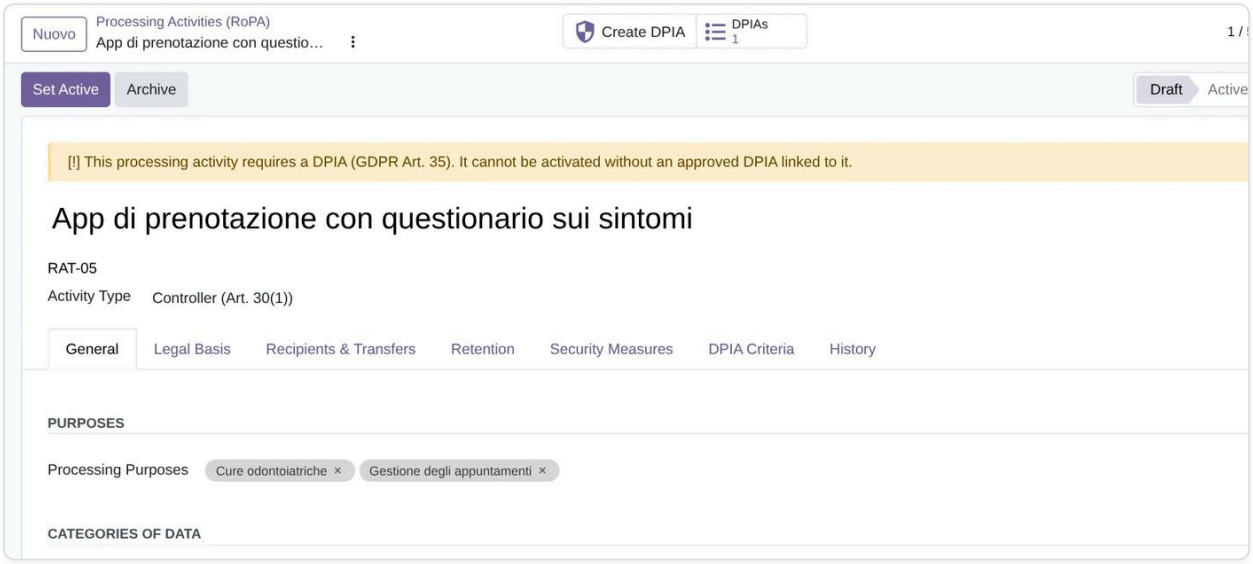
Un esempio dall'inizio alla fine

La prima violazione delle schermate è una **Confidentiality Breach**: una radiografia inviata per email al paziente sbagliato. Se ne è avuta conoscenza un'ora dopo l'accaduto, Odoo ha fissato il termine 72 ore più tardi e, all'apertura, ne restavano circa 42. Riguarda dati sanitari di pazienti, ha livello di rischio **Medium**, è **Under Assessment** e mostra il pulsante **Mark DPA Notified**. La seconda, una **Availability Breach** per il furto del portatile della reception, con il disco cifrato, ha livello **Low** ed è **Closed**: in una violazione chiusa resta solo il pulsante **Archive (Admin Only)**.

GUIDA DEL MODULO · GDPR COMPLIANCE

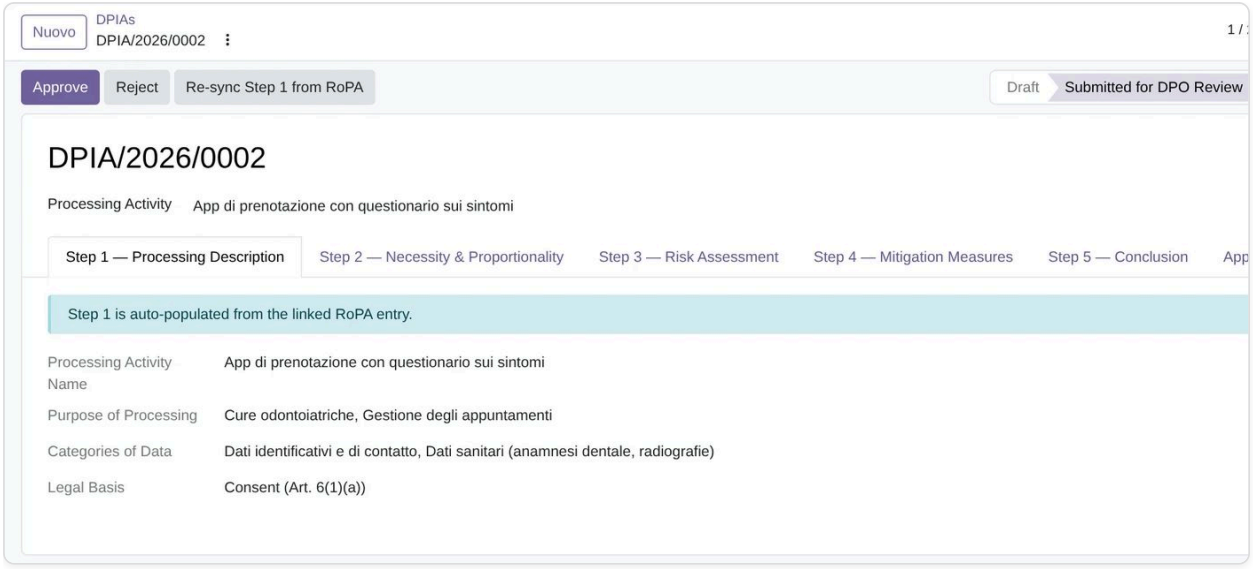
11 Le valutazioni d'impatto (DPIA)

Nella scheda **DPIA Criteria** di ogni attività ci sono nove caselle, una per criterio delle linee guida WP248 rev.01. Con due o più selezionate, o con il segnale manuale, l'attività risulta con **DPIA Required**. È una regola generale di quelle linee guida, non un obbligo di legge in sé. Le attività segnalate si vedono in **GDPR Toolkit › Processing Activities (RoPA) › DPIA Required**.



- **Schermata reale di Odoo 20.** Un'attività in **Draft** con l'avviso che richiede una DPIA.

La valutazione si apre dalla scheda dell'attività o da **GDPR Toolkit › DPIA › All DPIAs**. Il riferimento lo assegna Odoo da solo alla creazione del registro.



- **Schermata reale di Odoo 20.** Una DPIA inviata in revisione, con le schede dei cinque passi e **Approval**.

I cinque passi e la scheda di approvazione

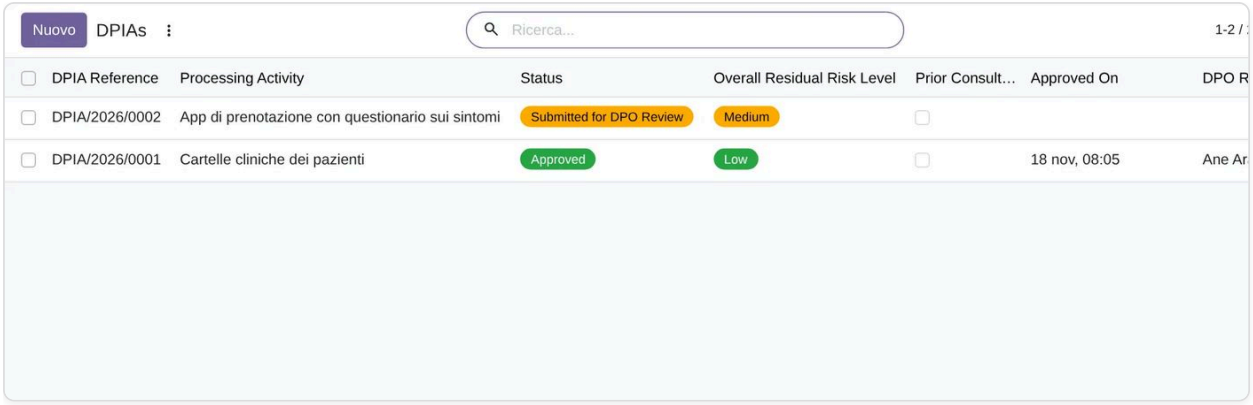
- Il passo 1, la descrizione del trattamento: il nome, la finalità, le categorie di dati e la base giuridica dell'art. 6 si compilano da soli dall'attività del RoPA.
- Il passo 2, necessità e proporzionalità: la limitazione della finalità, la minimizzazione dei dati, la giustificazione del periodo di conservazione e le misure per i diritti degli interessati.
- Il passo 3, la valutazione dei rischi: l'elenco dei rischi identificati.
- Il passo 4, le misure di mitigazione, in testo libero.
- Il passo 5, la conclusione e il rischio residuo.
- La scheda **Approval**: chi l'ha inviata, chi l'ha rivista, quando e i suoi commenti.

Ogni rischio ha il suo impatto e la sua probabilità prima delle misure, e gli stessi due valori residui dopo averle applicate. Da ogni coppia derivano un punteggio e un livello: fino a 4 basso, fino a 9 medio, fino a 19 alto e da 20 critico. Questa matrice è del modulo, non del GDPR né delle linee guida del Comitato europeo. Con rischio residuo alto o critico, **Prior Consultation Required (Art. 36)** si attiva da sola. Se presenti la consultazione, annota qui ciò che hai fatto tu in **Prior Consultation Submitted** e **Prior Consultation Notes**. Il modulo non la presenta all'autorità.

Pulsanti del registro

Submit for DPO Review	Porta la DPIA da **Draft** a **Submitted for DPO Review**. Si vede solo in **Draft**.
Approve	Approva la DPIA. Si vede solo in **Submitted for DPO Review**.
Reject	Rifiuta la DPIA. Si vede solo in **Submitted for DPO Review** e richiede i commenti del DPO.
Reset to Draft	Se una DPIA è in **Rejected**, riportala in **Draft**.
Re-sync Step 1 from RoPA	Copia di nuovo il passo 1 dall'attività del RoPA.

Gli stati sono **Draft**, **Submitted for DPO Review**, **Approved** e **Rejected**. Le DPIA in attesa di revisione si trovano in **GDPR Toolkit › DPIA › Awaiting DPO Review**.



- **Schermata reale di Odoo 20.** L'elenco delle DPIA con il loro stato e il loro livello globale di rischio residuo.

> Inviare, approvare e rifiutare possono farlo solo i gestori GDPR. La decisione finale spetta al titolare o al suo DPO. Il modulo non presenta la consultazione preventiva all'autorità e non è consulenza legale.

> Un'attività che richiede una DPIA non si attiva senza una DPIA approvata collegata: la scheda dell'attività lo segnala a schermo.

Stati della DPIA

STATO	COSA SIGNIFICA
Draft	È lo stato di partenza: si compilano i passi e compare **Submit for DPO Review**.
Submitted for DPO Review	La DPIA attende la decisione del DPO. In questo stato compaiono **Approve** e **Reject**.
Approved	Il DPO l'ha approvata e la data resta in **Approved On**.
Rejected	Il DPO l'ha rifiutata con i suoi commenti. Il pulsante **Reset to Draft** la riporta a **Draft**.

Quando non te lo consente

- Inviare, approvare e rifiutare possono farlo solo i gestori GDPR. Se non lo sei, compare il messaggio «Only GDPR Managers can submit a DPIA for review.», «Only GDPR Managers (acting as DPO) can approve a DPIA.» oppure «Only GDPR Managers (acting as DPO) can reject a DPIA.», a seconda del pulsante.
- Rifiutare senza scrivere nulla in **DPO Comments** genera il messaggio «DPO comments are required when rejecting a DPIA.».
- **Reset to Draft** si vede solo quando la DPIA è in **Rejected**.

Campi e schede del record

DPIA Reference	La assegna Odoo alla creazione del record e non è modificabile.
Processing Activity	L'attività del RoPA a cui appartiene la DPIA. È obbligatoria.
Overall Residual Risk Level	Lo calcola Odoo: è il più alto tra i rischi residui dell'elenco.
Submitted By e **Submitted On**	Chi ha inviato la DPIA in revisione e quando.

DPO Reviewer e **DPO Review Date**	Chi l'ha revisionata e quando.
DPO Comments	Testo della revisione. È obbligatorio per rifiutare.
Prior Consultation Submitted e **Prior Consultation Notes**	Ciò che annoti tu se hai presentato la consultazione preventiva dell'art. 36. Il modulo non la presenta.

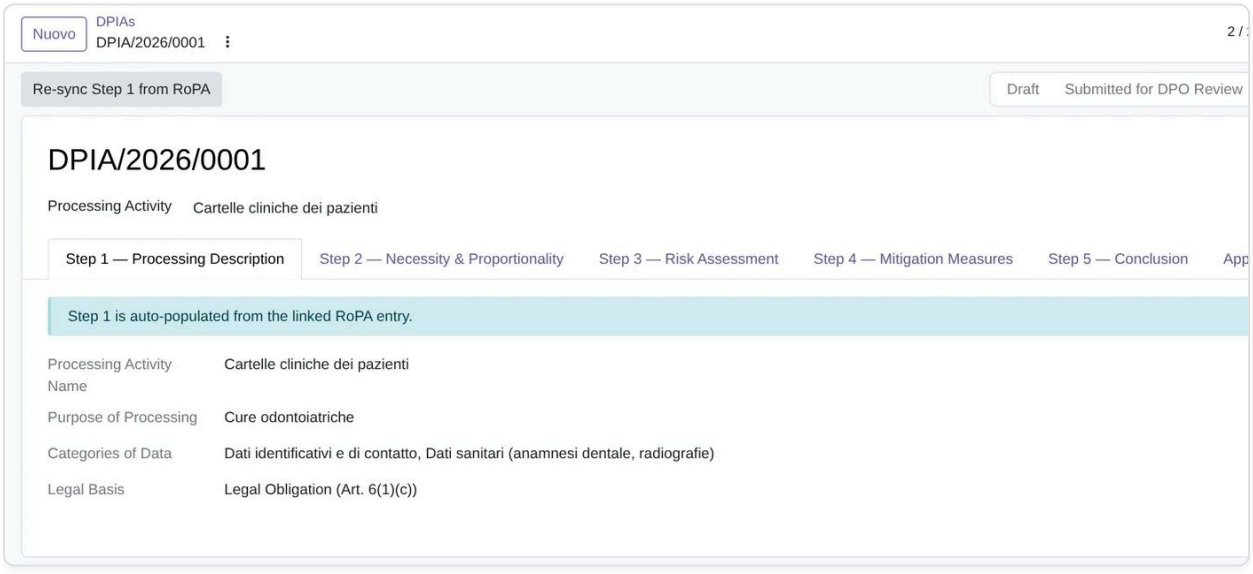
La vista ha sei schede: i cinque passi e **Approval**. Ogni passo ha i propri testi, e **Re-sync Step 1 from RoPA** serve ad aggiornare il passo 1 se cambi qualcosa nell'attività. I filtri sono **Awaiting DPO Review**, **Approved** e **High/Critical Residual Risk**, con raggruppamento **By Status** e **By Risk Level**.

Come si calcola il rischio

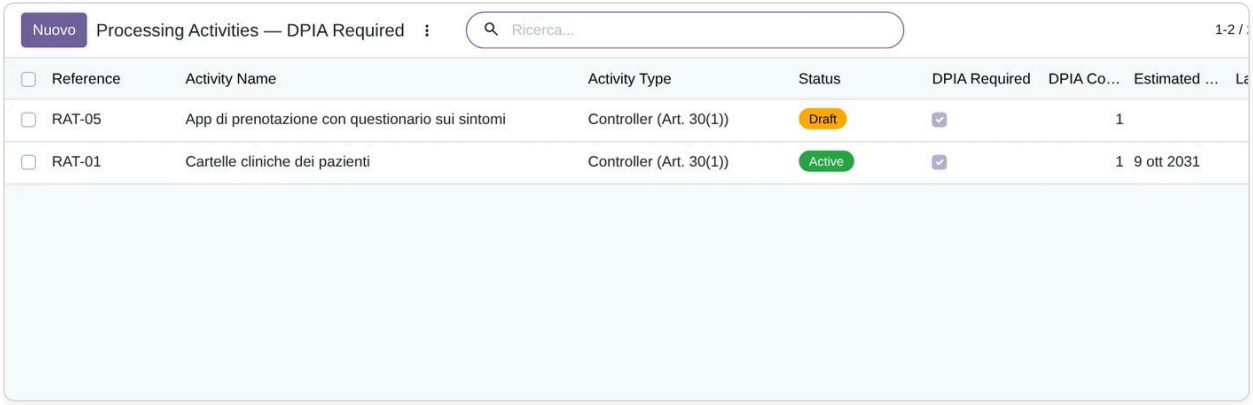
Ogni rischio valuta il proprio impatto da trascurabile (1) a catastrofico (5) e la propria probabilità da molto bassa (1) a molto alta (5). Si moltiplicano e ne risulta un punteggio da 1 a 25. Fino a 4 è **Low**, fino a 9 è **Medium**, fino a 19 è **High** e da 20 è **Critical**. Dopo le misure si ripete con l'impatto residuo e la probabilità residua. Queste soglie sono del modulo. Con rischio residuo alto o critico resta segnata la consultazione preventiva dell'art. 36.1, che richiede di consultare l'autorità prima del trattamento quando la valutazione mostra che comporterebbe un rischio elevato se non si adottano misure per attenuarlo.

Un esempio dall'inizio alla fine

Nell'esempio delle schermate, l'attività RAT-05, l'app di prenotazione online con questionario sui sintomi, è in **Draft** e ha **DPIA Required** attivo. La sua scheda avvisa che non si può attivare senza una DPIA approvata. Da lì si crea la DPIA, che esce con il numero DPIA/2026/0002, e il passo 1 contiene già la finalità, le categorie di dati e la base giuridica dell'attività. Dopo aver compilato gli altri passi si invia in revisione e nell'elenco resta in **Submitted for DPO Review** con rischio residuo **Medium**. Il DPO la vedrà in **Awaiting DPO Review** e la approverà o la rifiuterà con i suoi commenti. Finché non è approvata, l'attività resta in **Draft**.



- **Schermata reale di Odoo 20.** La DPIA della cartella clinica dei pazienti, con lo stato **Approved**.

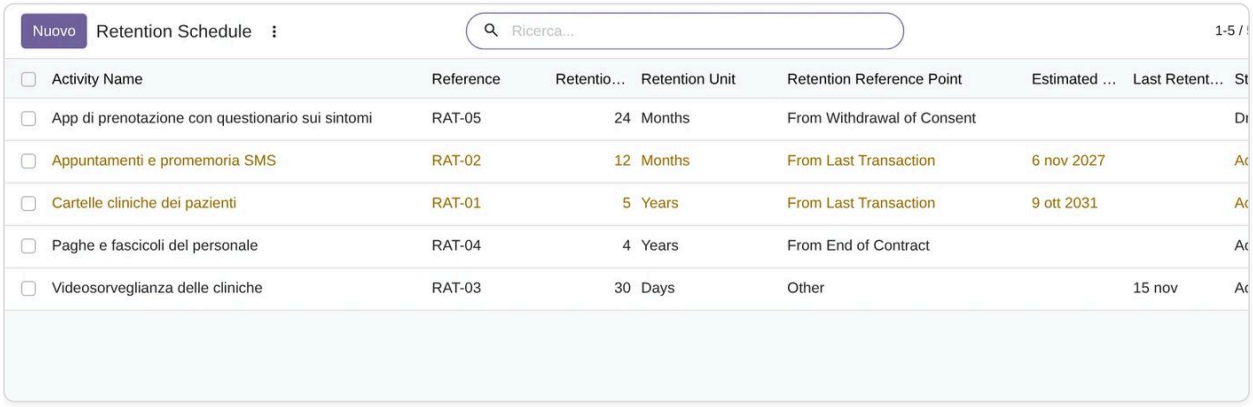


- **Schermata reale di Odoo 20.** Le attività con **DPIA Required** e il loro numero di DPIA.

> Ciò che questo modulo non fa: non presenta la consultazione preventiva all'autorità né decide al posto tuo se la valutazione è accettabile. La decisione finale spetta al titolare o al suo DPO, e non è consulenza legale.

GUIDA DEL MODULO · GDPR COMPLIANCE

12 La conservazione e le sue revisioni



- **Schermata reale di Odoo 20.** Il **Retention Schedule** con le cinque attività del registro.

La durata di ogni attività (durata, unità e inizio del computo) si compila nella scheda **Retention** dell'attività, in **GDPR Toolkit › Processing Activities (RoPA) › All Activities**. Odoo calcola la **Estimated Retention End Date** solo quando l'inizio del computo è **Fixed Date** o **From Last Transaction** e quella data è impostata. Con **From End of Contract**, **From Withdrawal of Consent** o **Other** resta vuota e quell'attività non riceve avvisi. Il **Retention Schedule** mostra le attività con una durata impostata, la loro data stimata e la loro **Last Retention Review**, che si aggiorna da sola ogni volta che salvi una revisione.

L'avviso è inviato dall'attività pianificata **GDPR: Retention Expiry Check**, ogni giorno. Per ogni attività attiva la cui data stimata rientra nei giorni di **Retention Advance Warning (days)** e che non è stata revisionata negli ultimi 30 giorni, lascia un'attività di avviso sulla scheda e invia un'email ai destinatari degli avvisi configurati o, in mancanza, ai responsabili GDPR. Un'altra attività pianificata, **GDPR: Annual RoPA Review Reminder**, ricorda una volta all'anno che è ora di rivedere il registro delle attività.

Dove registrare una revisione

Le revisioni si consultano in **GDPR Toolkit › Retention Management › Review History**, che apre l'elenco **Retention Review History**. Ogni revisione si crea con **Nuovo** e contiene questi campi:

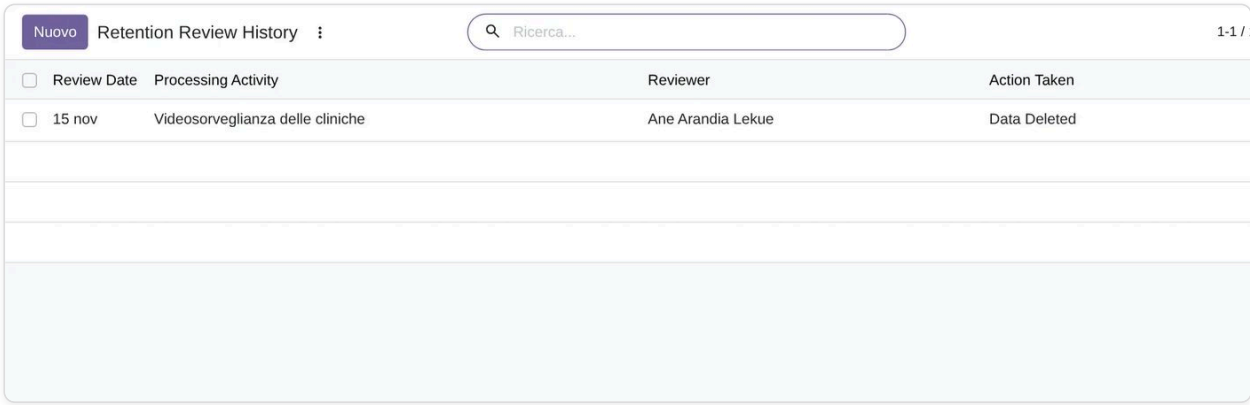
Processing Activity	L'attività che revisioni. È obbligatoria.
Review Date	Viene impostata con la data di oggi. È obbligatoria.
Reviewer	Viene impostata con il tuo utente. È obbligatorio.
Action Taken	Ciò che hai fatto dopo la revisione. È obbligatoria. Ha quattro opzioni: **Data Deleted**, **Data Anonymised**, **Retention Extended** e quella di revisionato senza necessità di azione.
Extension Justification	Il motivo per cui estendi la conservazione.
New Retention End Date	La data fino alla quale estendi la conservazione.
Notes	Testo libero.

La registrazione della revisione non ha pulsanti né stati propri. Le opzioni di **Action Taken** sono ciò che annoti tu, non uno stato del record.

Come registrare una revisione

1 Apri la cronologia

Entra in **GDPR Toolkit › Retention Management › Review History** e premi **Nuovo**.



- **Schermata reale di Odoo 20.** La **Retention Review History** con una revisione già registrata.

2 Scegli l'attività

Compila **Processing Activity**. La data di oggi e il tuo utente sono già impostati.

3 Indica l'azione

Scegli in **Action Taken** ciò che hai fatto con i dati.

4 Se estendi la conservazione

Con **Retention Extended**, compila **Extension Justification** e **New Retention End Date**.

5 Salva

Al salvataggio, la **Last Retention Review** dell'attività diventa la data di questa revisione.

> Il modulo non cancella né anonimizza dati. Le opzioni **Data Deleted** e **Data Anonymised** annotano soltanto ciò che hai fatto tu fuori da questa schermata. Con **Retention Extended**, Odoo non ti lascia salvare se manca la giustificazione («Extension justification is required when extending retention.») o la nuova data («New retention end date is required when extending retention.»). La **New Retention End Date** resta nella revisione, ma non cambia la data stimata dell'attività: per spostarla, cambia il termine o la sua data di riferimento nella scheda **Retention**.

Cosa conserva una revisione

Ogni revisione collega un'attività di trattamento alla data in cui l'hai revisionata, a chi l'ha fatta e a ciò che hai deciso. L'azienda si copia da sola dall'attività. Registra solo ciò che hai deciso e fatto: il modulo non cancella né modifica alcun dato.

Le quattro azioni possibili

Data Deleted	Registri che, dopo la revisione, i dati sono stati cancellati. La cancellazione la fai tu fuori dal modulo.
Data Anonymised	Registri che i dati sono stati anonimizzati. L'anonimizzazione la fai tu fuori dal modulo.
Retention Extended	Decidi di continuare a conservare i dati. Richiede una giustificazione e una nuova data di scadenza, che resta nella revisione: la data stimata dell'attività non cambia.
L'opzione di revisionato senza azione	Hai revisionato l'attività e non serve fare nulla. È la quarta opzione dell'elenco **Action Taken**.

Regole e condizioni

- Con **Retention Extended** e senza **Extension Justification**, Odoo non salva e mostra «Extension justification is required when extending retention.».
- Con **Retention Extended** e senza **New Retention End Date**, Odoo non salva e mostra «New retention end date is required when extending retention.».
- Con le altre tre azioni, questi due campi non sono richiesti.
- **Processing Activity**, **Review Date**, **Reviewer** e **Action Taken** sono obbligatori.

Ogni revisione che salvi aggiorna sull'attività la **Last Retention Review** con la **Review Date** di quella revisione. Si vede nelle colonne del **Retention Schedule** e nell'elenco delle **Processing Activities (RoPA)**.

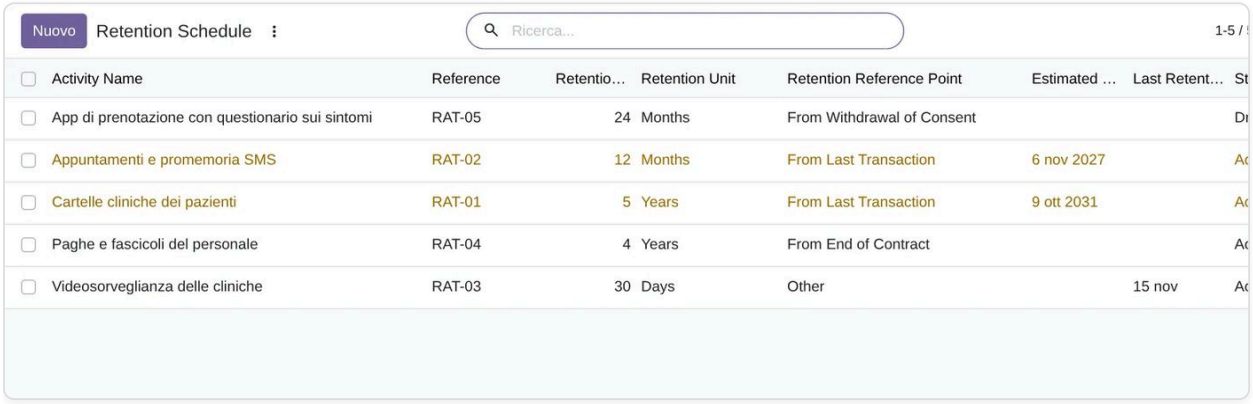
Gli avvisi

L'attività pianificata **GDPR: Retention Expiry Check** viene eseguita ogni giorno. Avvisa per le attività attive la cui data stimata di fine rientra nei giorni di **Retention Advance Warning (days)** (30 di serie) e che non sono state revisionate negli ultimi 30 giorni: lascia un'attività di avviso sulla scheda e invia un'email. Un'attività senza data stimata non riceve avvisi. L'attività pianificata **GDPR: Annual RoPA Review Reminder** ricorda una volta all'anno di rivedere il registro delle attività.

Un esempio dall'inizio alla fine

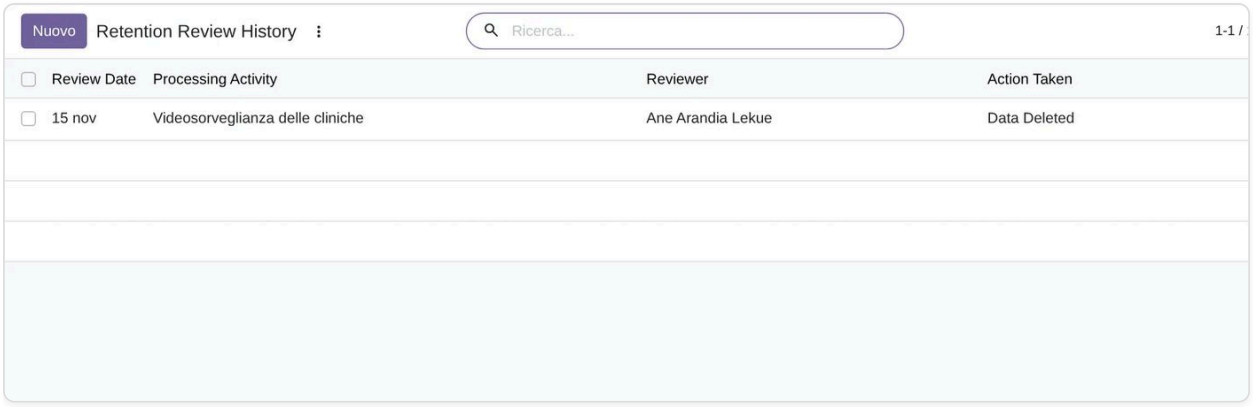
Il **Retention Schedule** delle schermate ha cinque attività. La storia clinica dei pazienti si conserva 5 anni dall'ultima transazione e gli appuntamenti e i promemoria via SMS 12 mesi: entrambe hanno una data stimata di fine. La videosorveglianza delle cliniche (30 giorni, con inizio del computo **Other**), le buste paga (4 anni dalla

fine del contratto) e l'app di prenotazione online (24 mesi dalla revoca del consenso) non ce l'hanno, perché il loro inizio del computo non è una data che Odoo conosce.



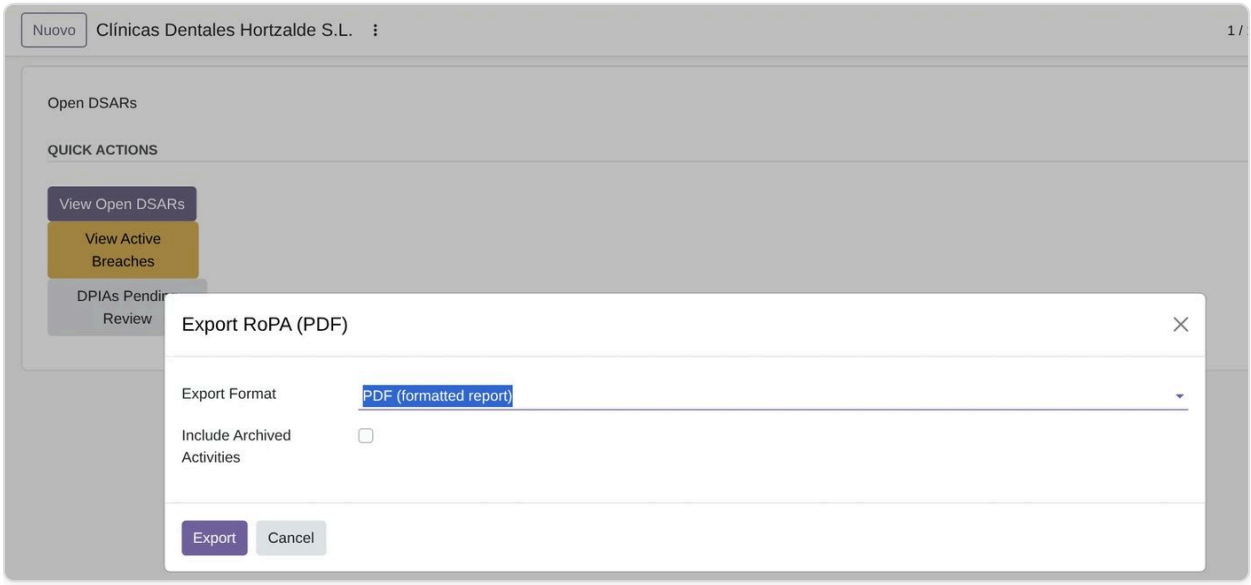
- **Schermata reale di Odoo 20.** Il **Retention Schedule** con le cinque attività e le loro date stimate.

Nella **Retention Review History** c'è una revisione della videosorveglianza delle cliniche, fatta da Ane Arandia Lekue, con l'azione **Data Deleted**. Non ha una nuova data di scadenza perché quell'azione non la richiede. Nel calendario, quella data diventa l'ultima revisione dell'attività.



- **Schermata reale di Odoo 20.** La **Retention Review History** con la revisione della videosorveglianza.

13 Report, esportazioni e registro di audit



- **Schermata reale di Odoo 20.** La procedura guidata di esportazione del RoPA, con il formato e la casella delle attività archiviate.

Esportare il RoPA

1. **Apri il menu di esportazione**
   Entra in **GDPR Toolkit › Reports › Export RoPA (PDF)** o in **GDPR Toolkit › Reports › Export RoPA (Excel)**. Entrambi aprono la stessa procedura guidata.

2. **Scegli il formato**
   In **Export Format** scegli **PDF (formatted report)** o **Excel (.xlsx)**. Viene selezionato il formato del menu da cui sei entrato.

3. **Decidi sulle archiviate**
   Spunta **Include Archived Activities** se le vuoi nel report. Senza spunta, le attività archiviate non compaiono.

4. **Premi Export**
   Il file viene generato. **Cancel** chiude la procedura guidata senza generare nulla.

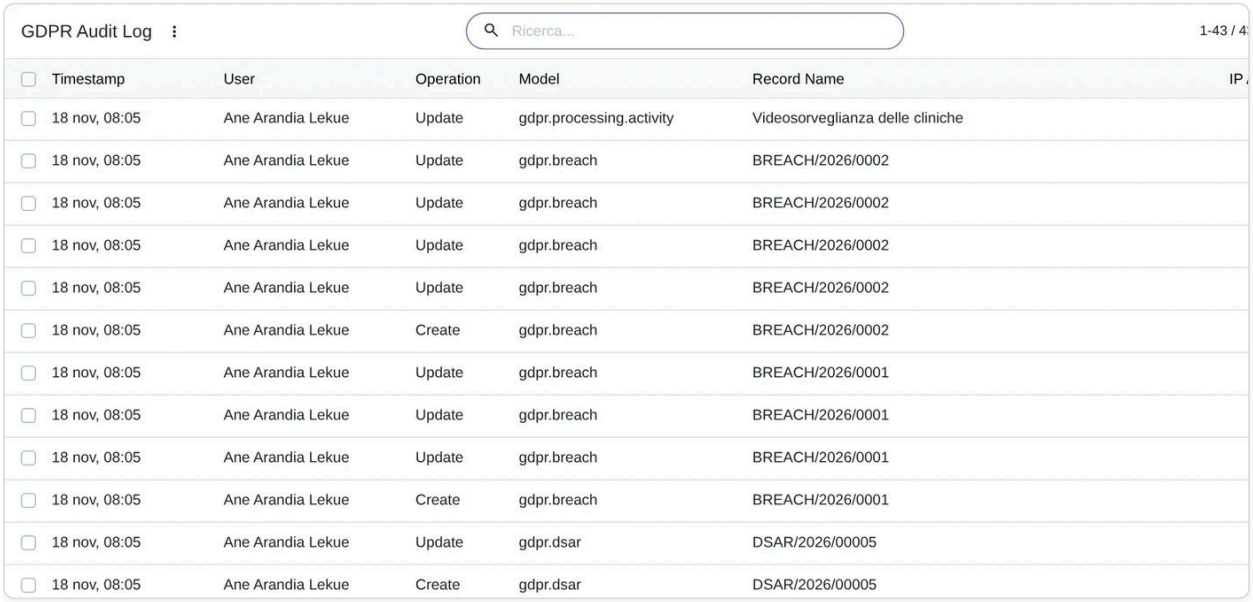
L'Excel contiene una riga per attività. Le intestazioni delle colonne compaiono in inglese in tutte le lingue.

- Se la tua azienda non ha attività di trattamento, la procedura guidata avvisa con «No processing activities found for this company.».
- Se manca la libreria di Excel sul server, avvisa con «openpyxl is not installed. Please install it via pip to use Excel export.». Va installata sul server.

Altri report

Nello stesso menu **Reports**, **DSAR History Report** apre l'elenco di tutte le richieste, **Breach Log Report** quello delle violazioni e **DPIA Status Report** quello delle DPIA, per filtrarli, raggrupparli o esportarli. Ogni richiesta, violazione, DPIA e attività si stampa in PDF dalla sua scheda.

Registro di audit



- **Schermata reale di Odoo 20.** Il **GDPR Audit Log** con data e ora, utente, operazione, modello, nome del record e indirizzo IP.

Ogni voce registra chi ha fatto la modifica, quando, su quale record e da quale indirizzo IP. Il riepilogo delle modifiche oscura i campi con dati personali. Le operazioni registrate sono **Create**, **Update**, **Archive**, **Export** e **Portal Submission**.

Create Operations	Filtro che lascia solo le creazioni.
Updates	Filtro che lascia solo le modifiche.
Exports	Filtro che lascia solo le esportazioni.
By User	Raggruppa le voci per utente.
By Model	Raggruppa le voci per modello.
Change Summary	Nella scheda di ogni voce: i campi modificati, con i dati personali oscurati.

> Nessuno può modificare né cancellare voci del registro di audit, nemmeno un amministratore. Odoo avvisa con «You do not have access rights to modify GDPR Audit Log records. Audit log entries are immutable compliance records.» oppure con «You do not have access rights to delete GDPR Audit Log records. They are permanent compliance records per Art. 5(2) GDPR accountability principle.».

Quali opzioni ha la procedura guidata di esportazione

PDF (formatted report)	Report formattato, pronto da leggere o stampare. Risulta selezionato se accedi da **Export RoPA (PDF)**.
Excel (.xlsx)	Foglio di calcolo con una riga per attività, da filtrare e ordinare a piacere.
Include Archived Activities	Casella deselezionata all'inizio. Se spuntata, le attività archiviate entrano nel report.

I due menu di esportazione portano alla stessa procedura guidata.

Quando non permette l'esportazione

- Senza attività di trattamento nella tua azienda, la procedura guidata avvisa con «No processing activities found for this company.» e non genera nulla.
- Senza la libreria di Excel sul server, l'esportazione in Excel fallisce con «openpyxl is not installed. Please install it via pip to use Excel export.».

Le operazioni del registro di audit

OPERAZIONE	COSA REGISTRA
Create	La creazione di un record.
Update	Una modifica su un record esistente.
Archive	L'archiviazione di un record.
Esporta	L'esportazione del RAT in Excel o quella della portabilità.
Portal Submission	Una richiesta inviata dal portale della privacy.

Campi del registro

Timestamp	Quando è stato fatto. Si compila da sola.
User	Chi l'ha fatto.
Operation	Una delle cinque indicate sopra.
Model e **Record Name**	Che tipo di registro è stato modificato e come si chiama.
Record ID	Identificatore numerico del registro modificato.
L'indirizzo IP	Da dove è stato fatto.
Change Summary	Nomi dei campi modificati e i loro valori. I campi con dati personali vengono mascherati.
Company	L'azienda a cui appartiene la voce.

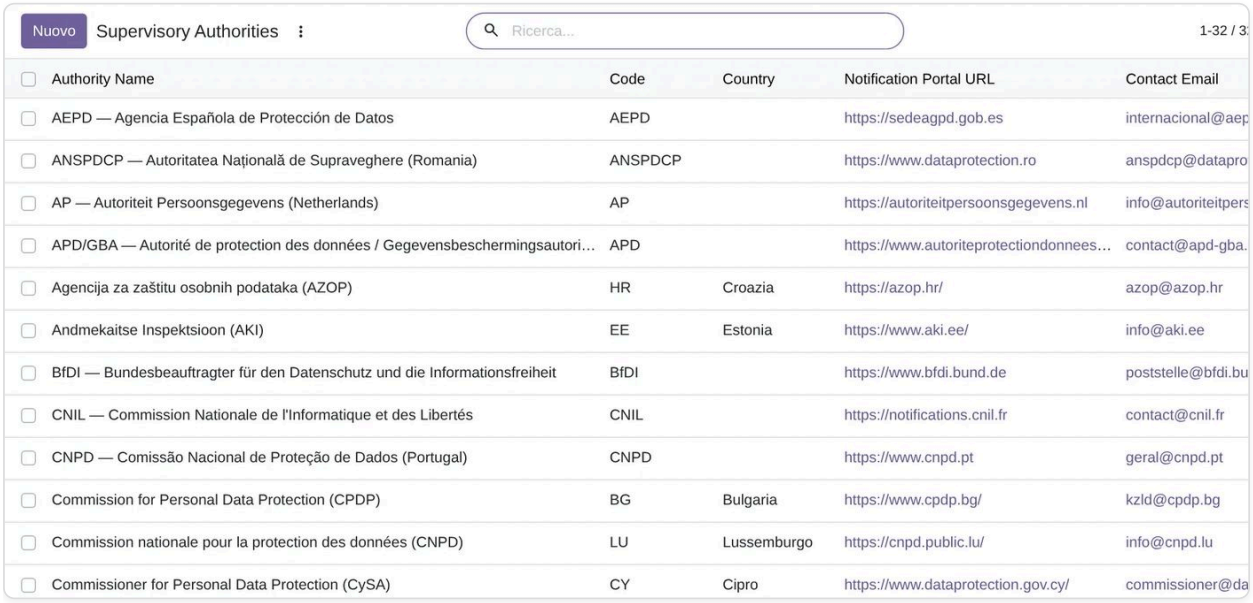
Cosa non si può fare

Le voci si possono solo creare. Qualsiasi tentativo di modificarle o eliminarle, indipendentemente dall'utente, termina con un messaggio di errore. Il messaggio cita l'art. 5(2) del RGPD, il principio di responsabilizzazione, come motivo della loro conservazione.

Un esempio dall'inizio alla fine

Entra in **GDPR Toolkit › Reports › Export RoPA (Excel)**, lascia non selezionato **Include Archived Activities** e premi **Export**. Ricevi il file con una riga per attività. Poi apri **GDPR Toolkit › Configuration › Audit Log** e filtra con **Exports**: lì vedi l'esportazione con il tuo utente e la data e l'ora. Nello stesso elenco compaiono le creazioni e le modifiche delle tue attività e violazioni, con il nome di ogni registro.

14 Autorità di controllo e basi giuridiche

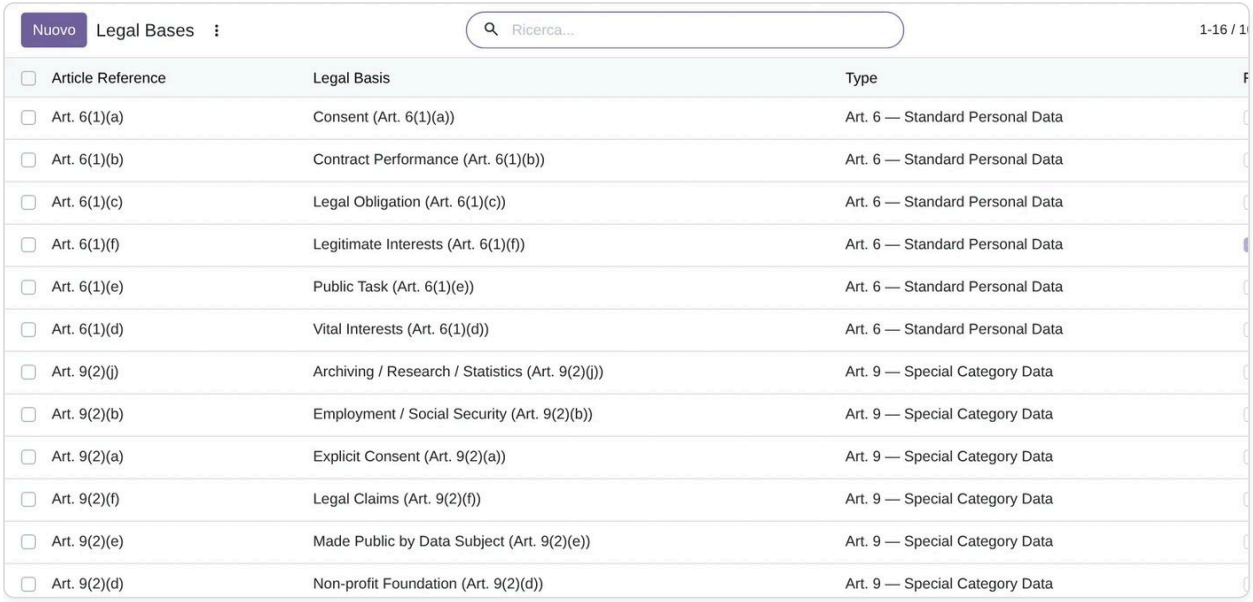


- **Schermata reale di Odoo 20.** L'elenco **Supervisory Authorities** con i suoi 32 record.

Il modulo include 32 autorità di controllo. Le trovi in **GDPR Toolkit › Configuration › Supervisory Authorities**. Vengono caricate una sola volta, all'installazione. Non c'è un'attività pianificata né un pulsante che le aggiorni, e solo un amministratore di Odoo può modificarle.

Authority Name	Nome completo dell'autorità. È obbligatorio.
Country	Paese a cui appartiene l'autorità.
Code	Sigla dell'autorità, ad esempio AEPD, CNIL o BfDI.
Notification Portal URL	Indirizzo del portale dove si effettuano le notifiche.
Contact Email	Email di contatto dell'autorità.
Breach Notification Form URL	Indirizzo del modulo per notificare una violazione.
Active	Casella che indica se l'autorità è in uso. È selezionata di default.

L'autorità principale si sceglie in **GDPR Toolkit › Configuration › DPO & Settings**.



- **Schermata reale di Odoo 20.** L'elenco **Legal Bases** con i suoi 16 record.

Le basi giuridiche si trovano in **GDPR Toolkit › Configuration › Legal Bases**. Sono 16 e vengono caricate all'installazione: quelle dell'articolo 6 e quelle dell'articolo 9.

Legal Basis	Nome della base. È obbligatorio.
Article Reference	Articolo di riferimento, ad esempio art. 6(1)(a).
Type	Indica se si tratta di una base dell'articolo 6, per i dati personali ordinari, o dell'articolo 9, per le categorie particolari di dati.
Requires Legitimate Interests Balancing Test	Casella che contrassegna le basi che richiedono quel test di bilanciamento.

> Queste liste non hanno stati né flusso di lavoro. Entrambe vengono caricate all'installazione del modulo e solo un amministratore di Odoo può modificarle.

Cosa contiene ogni lista e come si identifica

Ogni autorità ha tre dati che la identificano: il suo **Authority Name**, il suo **Country** e il suo **Code**. Il codice è testo libero e l'aiuto stesso del campo indica come esempi AEPD, CNIL e BfDI. Gli altri tre dati (il portale di notifica, l'email di contatto e il modulo per le violazioni) sono indirizzi e un'email che puoi consultare dalla scheda.

Attiva o non attiva

Ogni autorità ha la casella **Active**, selezionata per default. È l'unico elemento del record che indica se un'autorità è considerata in uso. Le basi giuridiche hanno anch'esse un campo attivo, ma non compare in nessuna schermata del modulo, quindi non puoi vederlo né modificarlo dall'interfaccia.

I due tipi di base giuridica

TYPE	COSA INCLUDE
Base dell'articolo 6	Le basi per trattare dati personali ordinari.

TYPE	COSA INCLUDE
Base dell'articolo 9	Le basi per trattare categorie particolari di dati.

Il test di bilanciamento

La casella **Requires Legitimate Interests Balancing Test** contrassegna le basi che richiedono quel giudizio di bilanciamento. Nell'elenco compare, ad esempio, **Legitimate Interests (Art. 6(1)(f))**, con il riferimento dell'articolo nella sua colonna. La descrizione di ogni base esiste nel modello, ma non compare in nessuna schermata.

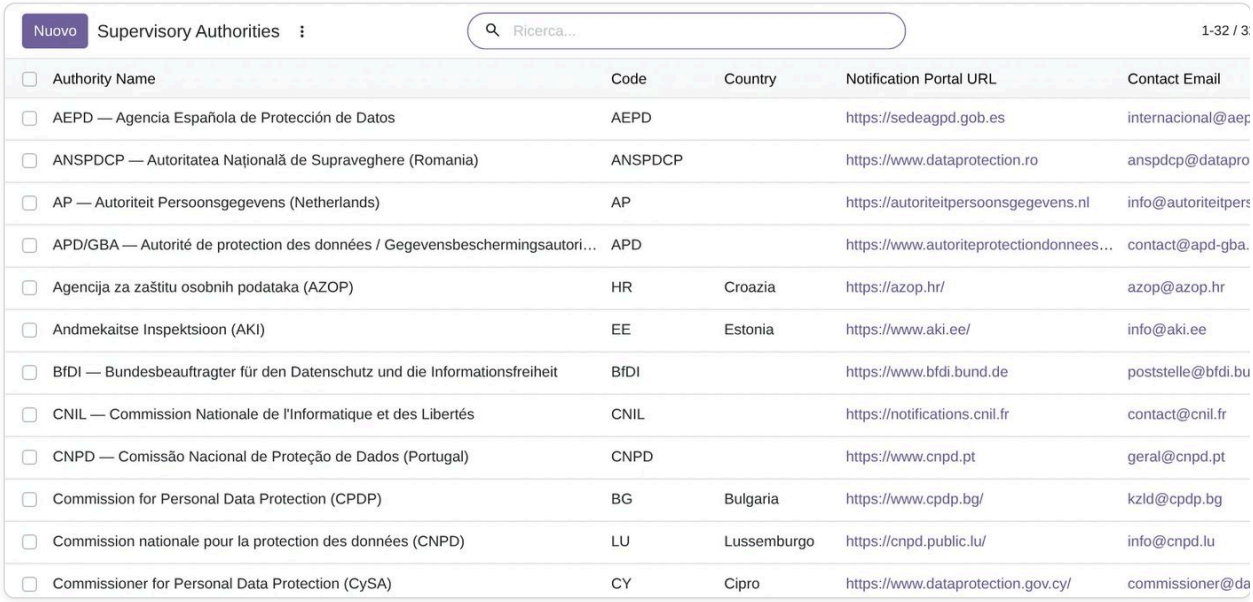
Regole e limiti

- Il nome dell'autorità e il nome della base giuridica sono obbligatori.
- Il tipo della base è obbligatorio e, se non lo cambi, appare come base dell'articolo 6.
- Le liste vengono caricate all'installazione. Il modulo non le ricarica né le aggiorna da solo.
- Il modulo non notifica nulla all'autorità. Il portale e il modulo sono indirizzi per notificare tu dall'esterno e annotare qui ciò che hai fatto.

Esempio dall'inizio alla fine

1 Apri le autorità

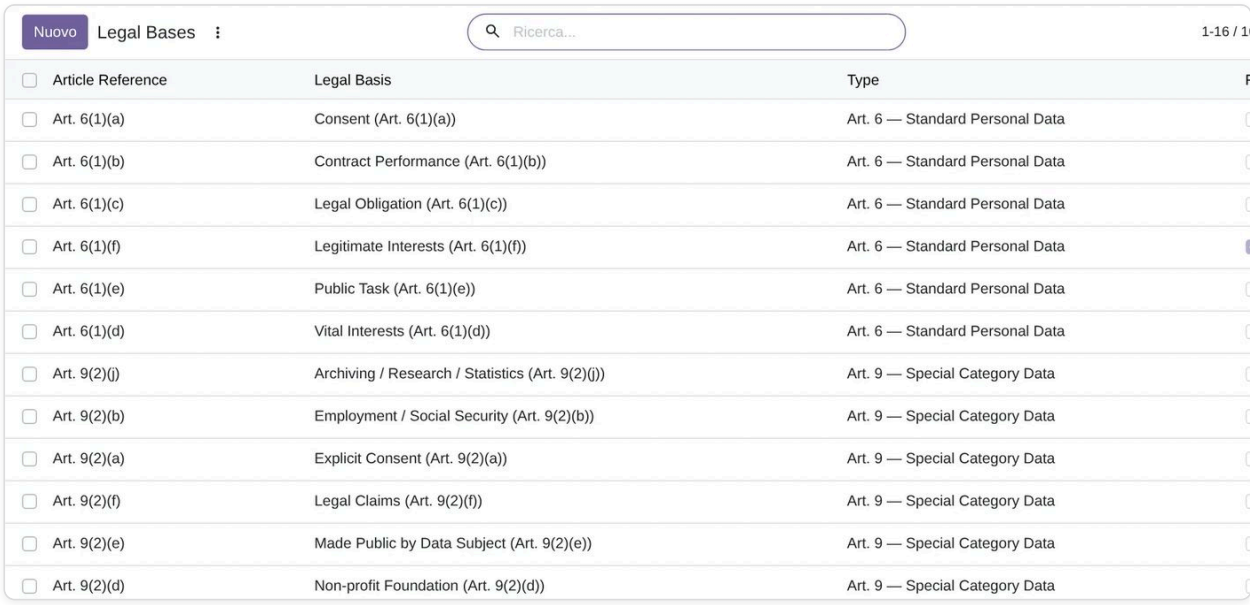
Entra in **GDPR Toolkit › Configuration › Supervisory Authorities**. L'elenco mostra 32 record, tra cui l'AEPD: il suo codice è AEPD.



- **Schermata reale di Odoo 20.** L'elenco mostra il nome, il codice, il paese, il portale e l'email di ogni autorità.

2 Apri le basi giuridiche

Entra in **GDPR Toolkit › Configuration › Legal Bases**. L'elenco mostra 16 record. Cerca **Consent (Art. 6(1)(a))** e **Legitimate Interests (Art. 6(1)(f))**, che ha selezionata la casella del test di bilanciamento.



- **Schermata reale di Odoo 20.** L'elenco mostra il riferimento dell'articolo, la base giuridica e il suo tipo.

GUIDA DEL MODULO · GDPR COMPLIANCE

15 Cosa va a FlexigoTech Cloud e cosa torna

DATO	DESTINAZIONE	QUANDO
L'identificazione della base: il suo identificatore, il suo indirizzo e il suo codice pubblico, la versione di Odoo e i nomi dei suoi moduli	Dal tuo Odoo a FlexigoTech Cloud	Al collegamento della base con il servizio
L'accettazione delle condizioni e del contratto di incarico del trattamento, con l'email di chi accetta	Dal tuo Odoo a FlexigoTech Cloud	Quando premi **Connetti e inizia la prova** dopo aver confermato di aver letto l'elenco
La richiesta del permesso del servizio per il modulo	Dal tuo Odoo a FlexigoTech Cloud	I moduli lo richiedono da soli; **Verifica ora** lo richiede al momento
Le richieste degli avvisi di monitoraggio	Dal tuo Odoo a FlexigoTech Cloud	Ogni 6 ore, quando la base richiede i nuovi avvisi
Gli avvisi di monitoraggio	Da FlexigoTech Cloud al tuo Odoo	Nella richiesta successiva dopo che una fonte è cambiata

Cosa monitora il servizio

FlexigoTech Cloud controlla ogni giorno sei fonti ufficiali e avvisa quando una cambia. Sono gli atti dell'Unione Europea che modificano il RGPD, pubblicati nell'Ufficio delle pubblicazioni; la procedura 2025/0360(COD), nota come omnibus digitale, nell'Osservatorio legislativo del Parlamento europeo; la LOPDGDD consolidata, nel BOE; la pagina delle decisioni di adeguatezza della Commissione europea; e le pagine di guide e strumenti dell'AEPD.

Gli avvisi compaiono in **Impostazioni › FlexigoTech Cloud** e arrivano anche in un'email giornaliera.

Cosa resta nel tuo Odoo

Il registro delle attività di trattamento, le richieste degli interessati, le violazioni, le valutazioni d'impatto e il registro di audit restano nel tuo database. Il modulo non invia nulla di tutto ciò a FlexigoTech né a nessun servizio esterno. La schermata di connessione lo ricorda così: i tuoi clienti, ordini, fatture e prodotti non vengono inviati da questa connessione a FlexigoTech Cloud.

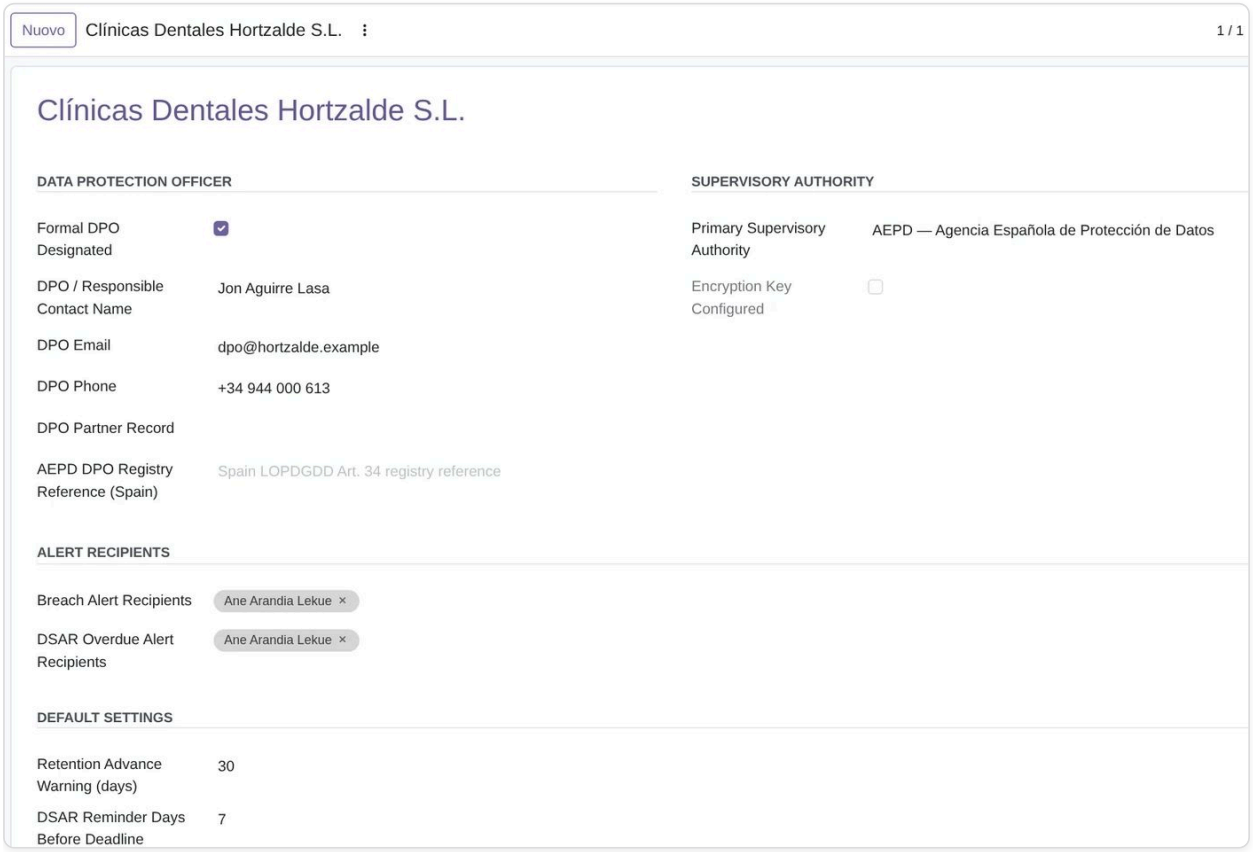
GUIDA DEL MODULO · GDPR COMPLIANCE

16 Cosa succede da solo

ATTIVITÀ	FREQUENZA	COSA FA
GDPR: DSAR Deadline Reminder	Ogni giorno	Invia un'email quando a una richiesta aperta mancano i giorni indicati in **DSAR Reminder Days Before Deadline**: alla persona assegnata o, se non ha un'email, ai gestori del RGPD.
GDPR: Breach Countdown Alert	Ogni ora	Nelle ultime 6 ore del termine di una violazione aperta non ancora segnata come notificata, invia un'email ai **Breach Alert Recipients** o ai gestori del GDPR.
GDPR: Retention Expiry Check	Ogni giorno	Crea un'attività di avviso e invia un'email per ogni attività attiva la cui scadenza di conservazione si avvicina e che non è stata rivista negli ultimi 30 giorni.
GDPR: DSAR Overdue Escalation	Ogni settimana	Invia il riepilogo delle richieste scadute ai **DSAR Overdue Alert Recipients** o ai gestori del GDPR.
GDPR: Annual RoPA Review Reminder	Ogni 12 mesi	Ricorda via email che è il momento di rivedere il registro delle attività di trattamento.

Gli avvisi vengono inviati via email agli utenti con un indirizzo email, nella lingua di ciascuno. Le frequenze si modificano in **Impostazioni › Funzioni tecniche › Automazione › Azioni pianificate**, con la modalità sviluppatore attivata.

17 Le opzioni del modulo e il loro valore iniziale



- **Schermata reale di Odoo 20.** Le opzioni della configurazione GDPR: il DPO, l'autorità di controllo, i destinatari degli avvisi e i giorni di anticipo.

OPZIONE	VALORE INIZIALE	COSA FA
DPO Partner Record, **DPO / Responsible Contact Name**, **DPO Email** e **DPO Phone**	Vuoti	Dati di chi svolge il ruolo di responsabile della protezione dei dati o di persona di contatto.
Formal DPO Designated	Attivo	Indica se è stato designato formalmente un DPO.
AEPD DPO Registry Reference (Spain)	Vuoto	Conserva il riferimento con cui il DPO risulta registrato presso l'AEPD.
Primary Supervisory Authority	Vuoto	Si sceglie tra le autorità di controllo caricate nel modulo.
Breach Alert Recipients	Vuoto	Utenti che ricevono gli avvisi di violazione. Se non ne scegli nessuno, li riceve il gruppo **GDPR Toolkit / Manager** dell'azienda.
DSAR Overdue Alert Recipients	Vuoto	Utenti che ricevono l'avviso delle richieste scadute. Se non ne scegli nessuno, lo riceve il gruppo **GDPR Toolkit / Manager** dell'azienda.
Retention Advance Warning (days)	30	Giorni di anticipo con cui si avvisa prima che scada il termine di conservazione.
DSAR Reminder Days Before Deadline	7	Giorni prima della scadenza di una richiesta in cui parte il promemoria.

OPZIONE	VALORE INIZIALE	COSA FA
Art. 30(5) SME Exception Note Acknowledged	Disattivo	Dichiari di aver letto la nota sull'eccezione dell'art. 30.5 per le aziende con meno di 250 dipendenti.
Encryption Key Configured	Secondo il server	Sola lettura. Indica se sul server è configurata la chiave di cifratura.

C'è una sola configurazione per società. Se provi a crearne una seconda, Odoo mostra «Only one GDPR configuration record per company is allowed. A configuration already exists for company ....»

Non si possono modificare i termini di legge (un mese per rispondere a una richiesta e due mesi di proroga, art. 12.3; 72 ore per notificare una violazione, art. 33.1) né la matrice dei rischi (impatto per probabilità), che appartengono al modulo.

Cosa si fa a mano

SCHERMATA	PULSANTI
Attività del RoPA	**Set Active** fa passare l'attività da bozza ad attiva; non è possibile se richiede una DPIA e non ne è collegata una approvata. **Archive** la archivia. **Set to Draft** la riporta in bozza. Il pulsante di creazione della DPIA apre una valutazione per quell'attività.
Richiesta di diritti	**Verify Identity** registra la verifica. **Draft Response** porta la richiesta allo stato di risposta redatta. **Extend Deadline (2 months)** aggiunge due mesi di proroga (art. 12.3). **Close — Refused** e **Close — Partial Erasure** chiudono la richiesta con la tua decisione.
Violazione	**Mark DPA Notified** indica che la notifica è stata fatta da te. **Close** chiude la violazione. **Archive (Admin Only)** la archivia.
DPIA	**Approve** e **Reject** registrano la decisione di chi revisiona. **Re-sync Step 1 from RoPA** riempie di nuovo il passo 1 con i dati dell'attività collegata.
Procedure guidate	**Export RoPA (PDF)** apre una procedura guidata con **Export Format** e **Include Archived Activities**; **Export** genera il report e **Cancel** la chiude.

I pulsanti delle richieste, delle violazioni e delle DPIA li vede solo **GDPR Toolkit / Manager**. Quelli dell'attività del RoPA li vedono tutti, ma solo un gestore può usarli, perché **GDPR Toolkit / User** ha il registro in sola lettura. Archiviare una violazione può farlo solo un amministratore di Odoo.

18 Sicurezza e dati personali

- Il gruppo **GDPR Toolkit / User** vede il RoPA in sola lettura, può registrare richieste e vede quelle in **Received** o assegnate a lui; modificarle e usare i loro pulsanti spetta a **GDPR Toolkit / Manager**.
- Il gruppo **GDPR Toolkit / Manager** vede tutto ed è l'unico ad avere i pulsanti di lavoro: verificare l'identità, redigere la risposta, chiudere, approvare una DPIA, segnare una violazione come notificata, tra gli altri.
- **Archive (Admin Only)**, nelle violazioni, lo vede solo l'amministratore di Odoo.
- Ogni azienda vede solo i propri record.
- Richieste, violazioni e attività non si cancellano: si archiviano o si chiudono.
- La cronologia del RoPA e il registro di audit non si possono modificare.
- Il riepilogo di audit oscura i dati personali.
- Le note interne e la motivazione di un rifiuto (richieste), e la descrizione e le conseguenze (violazioni), vengono salvate cifrate solo se il server ha la variabile d'ambiente GDPR_FERNET_KEY. Senza di essa vengono salvate in chiaro, il log del server lo segnala e la configurazione lo mostra in **Encryption Key Configured**.
- A FlexigoTech Cloud non va nessuna richiesta, violazione, DPIA o attività di trattamento. I dati del tuo Odoo restano nel tuo Odoo. Il servizio a pagamento controlla sei fonti ufficiali e avvisa quando una cambia.

19 Più aziende

Ogni azienda di Odoo ha la propria configurazione GDPR. Se nessuno ha aperto il menu della configurazione, il modulo la crea con i valori predefiniti la prima volta che serve. Il menu **Dashboard** apre la configurazione dell'azienda attiva e la crea se non esiste.

Ogni record (attività, richiesta, violazione, DPIA) riporta la propria azienda, e ogni utente vede quelli delle aziende a cui ha accesso. Le attività pianificate percorrono ogni azienda con la sua configurazione. Gli avvisi vanno ai destinatari indicati da quella configurazione e, se non ce n'è nessuno, ai gestori GDPR di quell'azienda.

Il portale privacy crea la richiesta nell'azienda attiva nel momento in cui l'interessato la invia.

Il piano Standard costa 29 € al mese o 290 € all'anno, e il Pro 58 € al mese o 580 € all'anno (prezzi IVA esclusa). Ogni modulo ha un proprio abbonamento, per il database di produzione; le sue copie di prova sono incluse.

20 Se qualcosa non funziona

Un'attività di trattamento non si attiva e compare l'avviso che manca una DPIA approvata.	Completa e approva una DPIA collegata all'attività. Quando sarà approvata, premi di nuovo **Set Active**.
Una richiesta di diritti non torna a uno stato precedente.	Lo stato va solo avanti. Se hai sbagliato, annotalo nelle note interne e prosegui dallo stato attuale.
L'esportazione per la portabilità non viene generata.	Verifica prima l'identità della richiesta e collega un contatto di Odoo nel campo **Odoo Contact (for portability export)**.

Non puoi chiudere una richiesta come rifiutata.	Scrivi prima la motivazione del rifiuto. È obbligatoria.
Non puoi prorogare il termine di una richiesta.	Compila il motivo della proroga. Senza motivo, il modulo non consente la proroga.
Non puoi rifiutare una DPIA.	Scrivi i commenti del DPO. Sono obbligatori in caso di rifiuto.
Non puoi cancellare una violazione, una richiesta o un'attività di trattamento.	Fanno parte della traccia di audit. Archiviali. Per le violazioni, solo un amministratore di Odoo può archiviare e con un motivo scritto.
Le note interne vengono salvate in chiaro.	Manca la chiave di cifratura sul server. Nella configurazione, **Encryption Key Configured** ti dice se è impostata.

Gli avvisi di Odoo indicano cosa manca. Quasi sempre basta completarlo e ripetere l'azione.

Altri avvisi che potresti vedere

«Only GDPR Managers can submit a DPIA for review.»	Chiedi a un gestore GDPR di inviarla a revisione.
«Only GDPR Managers (acting as DPO) can approve a DPIA.»	L'approvazione spetta a un gestore GDPR, che agisce come DPO. Chiedila a chi ha questo permesso.
«Only GDPR Managers can perform this action.»	L'azione è riservata ai gestori GDPR o agli amministratori di Odoo. Chiedila a uno di loro.
«Only Odoo Administrators can archive breach records.»	Chiedi a un amministratore di archiviare la violazione. Deve indicare un motivo.
«Archive reason is required.»	Scrivi il motivo dell'archiviazione e conferma di nuovo.
«Extension justification is required when extending retention.»	Nella revisione della conservazione, scrivi la motivazione prima di salvare la proroga.
«New retention end date is required when extending retention.»	Indica la nuova data limite nella revisione prima di salvarla.
«No Odoo contact linked to this DSAR. Please link a res.partner record first.»	Collega il contatto alla richiesta e ripeti l'esportazione.
Avviso che i dati dell'interessato sono già stati anonimizzati e che serve una gestione manuale con il tuo DPO.	Il contatto è già anonimizzato in Odoo e non ci sono dati da esportare. Consulta il tuo DPO su come rispondere.
«No processing activities found for this company.»	Quando esporti il RAT, verifica che l'azienda attiva abbia delle attività.

21 Altri modi di farlo

MODALITÀ	COSA COMPORTA
Manuale	Fogli di calcolo per il registro delle attività, le richieste e le violazioni. Le scadenze si calcolano a mano e nessuno avvisa quando si avvicinano.
Solo Odoo	Odoo 17, 18, 19 e 20 includono di serie, in Community, la ricerca privacy nel menu tecnico delle Impostazioni (con la modalità sviluppatore). Cerca i record di una persona per nome o e-mail, permette di archiviarli o eliminarli e conserva un registro della privacy. Non include registro delle attività, richieste di diritti, registro delle violazioni né DPIA.
Questo modulo	Aggiunge il registro delle attività di trattamento, le richieste degli interessati con il termine di un mese dal ricevimento e la proroga di altri due mesi (art. 12.3), il registro delle violazioni con il conto alla rovescia di 72 ore dal momento in cui se ne ha conoscenza (art. 33.1) e le DPIA.

Per cancellare o anonimizzare i dati di una persona, la ricerca privacy di Odoo funziona insieme a questo modulo. Il modulo gestisce la richiesta e registra la tua decisione; la cancellazione o l'anonimizzazione la fai tu in Odoo.

22 Piani e prezzo

9 €

Licenza per versione di Odoo.

+ FlexigoTech Cloud

STANDARD

29 €/mese

o 290 € all'anno

- Prima risposta entro 1 giorno lavorativo

PRO

58 €/mese

o 580 € all'anno

- Prima risposta entro 4 ore lavorative
- Videochiamata se serve

14 giorni di prova, senza carta · **Prezzi IVA esclusa**

La licenza del modulo si acquista per versione di Odoo. FlexigoTech Cloud si paga al mese o all'anno, e la prova di 14 giorni non richiede carta di credito.

23 Domande frequenti

Funziona senza FlexigoTech Cloud?

No.

Cosa offre l'abbonamento a FlexigoTech Cloud?

Il monitoraggio quotidiano di sei fonti ufficiali, con un avviso quando una di esse cambia. Gli avvisi compaiono in **Impostazioni › FlexigoTech Cloud** e in un'e-mail giornaliera.

Quanto costa il servizio FlexigoTech Cloud?

Il piano Standard costa 29 € al mese o 290 € all'anno, e il Pro 58 € al mese o 580 € all'anno, IVA esclusa. In più, la licenza del modulo costa 9 € per versione di Odoo.

Quali fonti monitora il servizio?

Gli atti dell'Unione Europea che modificano il RGPD, la procedura del pacchetto digitale (omnibus digitale) nel Parlamento europeo, la LOPDGDD consolidata del BOE, le decisioni di adeguatezza della Commissione europea e le linee guida e gli strumenti dell'AEPD.

Cosa invia il mio Odoo a FlexigoTech Cloud?

L'identificazione della base (identificativo, indirizzo, codice pubblico, versione di Odoo e nomi dei moduli), l'accettazione delle condizioni con l'e-mail di chi accetta e la richiesta del permesso del servizio. Il registro delle attività, le richieste, le violazioni, le DPIA e il registro di audit restano nel tuo database.

Funziona su Odoo Online?

No. Odoo Online non consente di installare moduli di terze parti.

Richiede Odoo Enterprise?

No. Dipende solo da moduli di Odoo Community (base, mail e portal) e da flexigotech_cloud: funziona su Community e su Enterprise.

Per quali versioni di Odoo è disponibile?

È disponibile un ramo per ciascuna delle versioni 17, 18, 19 e 20.

Quale termine calcola per una richiesta di un interessato e da dove deriva?

Un mese dalla ricezione della richiesta, secondo l'art. 12.3 del GDPR. La colonna **Days Remaining** conta fino alla scadenza in vigore.

Come si proroga il termine?

Con **Extend Deadline (2 months)**, che aggiunge altri due mesi (art. 12.3) e richiede di scrivere il motivo. Cambia solo la **Current Deadline**; non cambia lo stato della richiesta.

Cosa succede quando scade il termine di una richiesta?

La richiesta compare nell'elenco **Overdue**. Ogni settimana, l'attività pianificata **GDPR: DSAR Overdue Escalation** invia il riepilogo di quelle scadute ai destinatari di quegli avvisi o, in mancanza, ai gestori del GDPR.

Come conta le 72 ore di una violazione e a chi avvisa?

Conta dalla data e dall'ora in cui annoti che se ne è venuti a conoscenza, secondo l'art. 33.1. Ogni ora, l'attività pianificata **GDPR: Breach Countdown Alert** avvisa via e-mail quando mancano 6 ore o meno, finché non la segni come notificata.

Notifica l'autorità di controllo?

No. La notifica la fai tu per conto tuo e qui registri lo stato, la data e l'ora, il mezzo e il riferimento.

Comunica qualcosa agli interessati in caso di violazione?

No. Se la comunicazione dell'art. 34 è obbligatoria, la fai tu e la annoti con **Mark Data Subjects Notified**.

Cancella o anonimizza i dati in una richiesta di cancellazione?

No. **Retention Conflict Check** conta ciò che c'è e annota la tua decisione. Cancellare o anonimizzare lo fai tu in Odoo.

Invia la lettera di risposta all'interessato?

No. La rediggi nella scheda della risposta a partire da un modello e la invii tu. L'unica e-mail che parte da sola verso l'interessato è la conferma di ricevimento di una richiesta fatta dal portale.

Cosa esporta la portabilità e in quali formati?

I dati di contatto, lo storico degli ordini (con l'app Vendite) e la scheda del dipendente (con l'app Dipendenti, con conferma esplicita). I formati sono JSON o CSV.

Di cosa ha bisogno l'esportazione per la portabilità per essere generata?

L'identità verificata e un contatto di Odoo collegato alla richiesta. Senza questo, la procedura guidata si rifiuta.

Come chiede un interessato un diritto tramite il portale e cosa gli serve?

Entra in /my/privacy-rights del tuo Odoo, che richiede l'accesso, quindi serve un account portale. Il modulo non inserisce un link in Il mio account: l'indirizzo glielo fornisci tu.

Quando segna una DPIA come obbligatoria?

Quando sono soddisfatti due o più dei nove criteri della scheda **DPIA Criteria**, oppure se la imposti a mano. Questa regola dei due criteri è un orientamento generale delle linee guida WP248, non un obbligo di legge.

Cos'è la consultazione preventiva?

La consultazione all'autorità dell'art. 36. Con rischio residuo alto o critico, **Prior Consultation Required (Art. 36)** si seleziona da sola. Se la presenti, annoti qui ciò che hai fatto tu; il modulo non la presenta.

Posso cancellare una richiesta, una violazione o un'attività?

No. Le attività, le richieste e le violazioni si archiviano o si chiudono. Archiviare una violazione può farlo solo l'amministratore di Odoo e richiede un motivo.

Cosa conserva il registro di audit?

Data e ora, utente, operazione, modello, nome del record e, quando disponibile, l'indirizzo IP di ogni modifica. Nessuno può modificare o cancellare le sue voci, nemmeno un amministratore.

Cosa viene conservato cifrato?

Le note interne, la motivazione di un rifiuto e la descrizione e le conseguenze delle violazioni, solo se il server dispone della chiave di cifratura. Senza di essa vengono conservati senza cifratura.

Funziona con più aziende?

Sì. Ogni azienda ha la propria configurazione e ogni utente vede solo i record delle aziende a cui ha accesso.

In quali lingue compaiono le schermate?

In spagnolo, le schermate del modulo compaiono in spagnolo. Nelle altre lingue compaiono in inglese; i menu e i pulsanti di Odoo, nella lingua di ciascun utente.

Serve un'azienda con meno di 250 dipendenti?

L'art. 30.5 del RGPD esclude dagli obblighi dei paragrafi 1 e 2 le aziende con meno di 250 dipendenti, salvo che il trattamento possa comportare un rischio per i diritti e le libertà degli interessati, non sia occasionale o includa categorie particolari di dati o dati relativi a condanne e reati. Il modulo non esprime un parere su se ti riguarda.

Quante autorità di controllo e basi giuridiche include?

32 autorità di controllo e 16 basi giuridiche, che si caricano all'installazione. Scegli l'autorità principale in **GDPR Toolkit › Configuration › DPO & Settings**.

Quali report ed esportazioni ha?

Puoi esportare il RAT in PDF o in Excel. Ci sono anche report dello storico delle richieste di diritti, del registro delle violazioni e dello stato delle DPIA.

Quali avvisi invia via e-mail?

Cinque attività pianificate: il promemoria giornaliero della scadenza delle richieste, il conto alla rovescia orario delle violazioni, il controllo giornaliero della conservazione, l'escalation settimanale delle richieste oltre il termine e il promemoria della revisione annuale del RAT.

Cosa mostra il menu Cruscotto?

Tre pulsanti che aprono elenchi: **View Open DSARs**, **View Active Breaches** e **DPIAs Pending Review**. Non mostra cifre.

Decide lei al posto mio se notificare una violazione o fare una DPIA?

No. La decisione finale spetta al titolare del trattamento o al suo DPO. La matrice di rischio, impatto per probabilità, è del modulo, non della legge.

È consulenza legale?

No.

GUIDA DEL MODULO · GDPR COMPLIANCE

24 Glossario

RGPD	Il Regolamento generale sulla protezione dei dati, il Regolamento (UE) 2016/679. È la norma europea da cui derivano i termini e gli obblighi che gestisce il modulo.

LOPDGDD	La legge spagnola sulla protezione dei dati e la garanzia dei diritti digitali. FlexigoTech Cloud monitora il suo testo consolidato nel BOE.
AEPD	L'Agenzia spagnola per la protezione dei dati. È una delle 32 autorità di controllo incluse nel modulo.
Autorità di controllo	L'autorità pubblica che vigila sulla protezione dei dati in ciascun paese. A essa si notificano le violazioni (art. 33.1). In **Primary Supervisory Authority** scegli la tua.
DPO	Il responsabile della protezione dei dati o, in sua assenza, la persona responsabile della privacy. I suoi dati sono conservati nella configurazione.
Titolare del trattamento	Chi decide per quali scopi e con quali mezzi vengono trattati i dati. Il suo registro delle attività è quello dell'art. 30.1.
Responsabile del trattamento	Chi tratta dati per conto del titolare. Il suo registro delle attività è quello dell'art. 30.2.
Interessato	La persona i cui dati vengono trattati e che può esercitare i propri diritti.
RAT	Il registro delle attività di trattamento (art. 30): una scheda per attività, con il suo storico.
Richiesta di diritti	Ciò che chiede un interessato: accesso (art. 15), rettifica (art. 16), cancellazione (art. 17), limitazione (art. 18), portabilità (art. 20) od opposizione (art. 21).
Scadenza in vigore	La data entro cui occorre rispondere a una richiesta: un mese dal ricevimento e, se prorogata, altri due mesi (art. 12.3).
Portabilità	Il diritto a ricevere i dati personali forniti dall'interessato in un formato strutturato, di uso comune e leggibile da dispositivo automatico (art. 20.1). Il modulo li esporta in JSON o CSV.
Cancellazione	Il diritto alla cancellazione dei dati (art. 17). Il modulo conta i dati presenti e registra la tua decisione; la cancellazione la esegui tu.
Violazione dei dati personali	Una violazione della sicurezza dei dati personali. Va notificata all'autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore da quando se ne ha conoscenza, salvo che sia improbabile che presenti un rischio (art. 33.1).
DPIA	La valutazione d'impatto sulla protezione dei dati (art. 35), con cinque passaggi.
Rischio residuo	Il rischio che rimane dopo l'applicazione delle misure di mitigazione. Con rischio residuo alto o critico si segna la consultazione preventiva.
Consultazione preventiva	La consultazione dell'autorità prima del trattamento quando la DPIA indica che il trattamento presenterebbe un rischio elevato in assenza di misure di mitigazione (art. 36.1). La presenti tu.
Base giuridica	Il motivo che consente il trattamento dei dati. Il modulo ne prevede 16: 6 dell'art. 6 e 10 dell'art. 9.
Categorie particolari	I dati di cui all'art. 9, come quelli sanitari. Hanno proprie basi giuridiche.
Trasferimento internazionale	L'invio di dati verso un paese terzo. La scheda dell'attività riporta il paese e la garanzia che lo copre.
Conservazione	Il tempo per cui si conservano i dati di ciascuna attività, con la relativa data limite stimata e lo storico delle revisioni.
Registro di audit	L'elenco di chi ha effettuato quali modifiche, quando e da quale indirizzo IP. Non può essere modificato né cancellato.

Monitoraggio	Il servizio di FlexigoTech Cloud che ogni giorno controlla sei fonti ufficiali e avvisa quando ne cambia una.

GUIDA DEL MODULO · GDPR COMPLIANCE

25 Checklist e contatti

- [ ] Hai Odoo 17, 18, 19 o 20 su Odoo.sh o sul tuo server. Odoo Online non consente di installare moduli di terze parti.
- [ ] Hai installato il modulo e la sua dipendenza, flexigotech_cloud.
- [ ] Hai attivato la prova di 14 giorni di FlexigoTech Cloud in **Impostazioni › FlexigoTech Cloud** e hai letto l'elenco dei dati che vengono inviati.
- [ ] Hai aperto **GDPR Toolkit › Configuration › DPO & Settings** e hai compilato i dati del DPO e la **Primary Supervisory Authority**.
- [ ] Hai indicato i destinatari degli avvisi di violazione e delle richieste.
- [ ] Hai assegnato a ciascuna persona il gruppo **GDPR Toolkit / Manager** o **GDPR Toolkit / User**.
- [ ] Se vuoi cifrare le note interne e la descrizione delle violazioni, hai impostato la chiave di cifratura sul server e **Encryption Key Configured** lo conferma.
- [ ] Hai creato le attività del RAT con i criteri della DPIA e il periodo di conservazione.
- [ ] Hai registrato una prima richiesta e verificato il suo **Current Deadline**.
- [ ] Hai fornito agli interessati l'indirizzo /my/privacy-rights del tuo Odoo.
- [ ] Se vuoi, hai provato il registro delle violazioni con una violazione di prova e hai visto il conto alla rovescia di 72 ore.

Se vuoi che lo configuriamo insieme, scrivici. 2 mesi di supporto inclusi in tutto ciò che acquisti: ti aiutiamo a installarlo, configurarlo e farlo funzionare, via email e videochiamata.

E-mail

Per installarlo, configurarlo o per qualsiasi dubbio.
comercial@flexigotech.com

Sul web

La pagina del modulo, con la guida e i prezzi.
flexigotech.com/it/odoo-gdpr.html

Su Odoo Apps

La pagina del modulo nello store di Odoo.
apps.odoo.com

GDPR Compliance è un modulo di FlexigoTech per Odoo. FlexigoTech è un marchio di Flexibles y Accesorios Gobe, S.L. (Barcellona, Spagna).