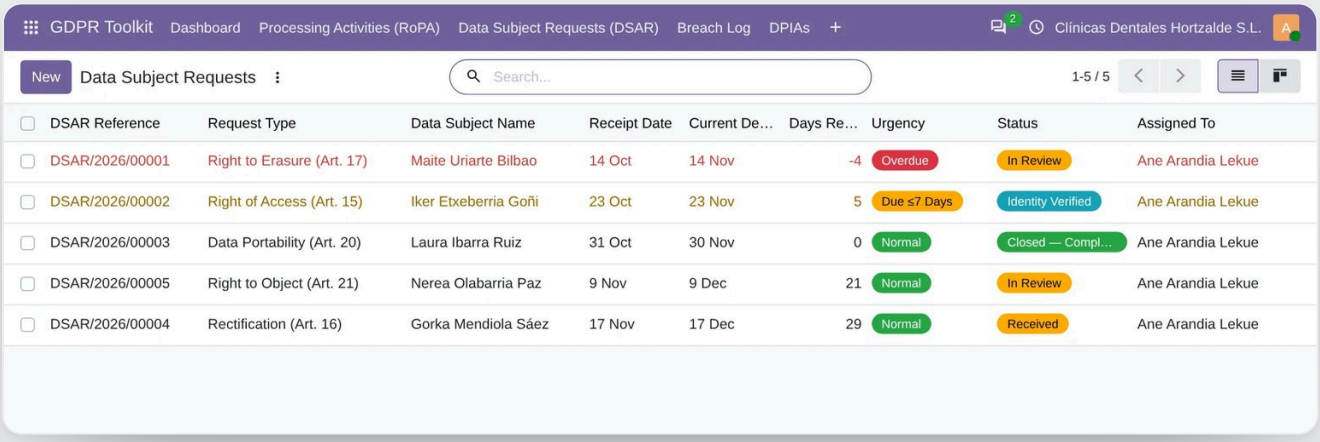
USER MANUAL · DATA PROTECTION

GDPR Compliance for Odoo

For those who already have the module: install it, activate it, set it up and use it, step by step.

Module version 20.0.1.1.13 | Odoo 20 screenshots | Edition of 18-11-2026





Real Odoo 20 screenshot. The list of requests with their deadline and urgency, and a breach with the 72-hour countdown.

Contents

On the right, the page where each section starts. Menu and button names are those of Odoo in English.

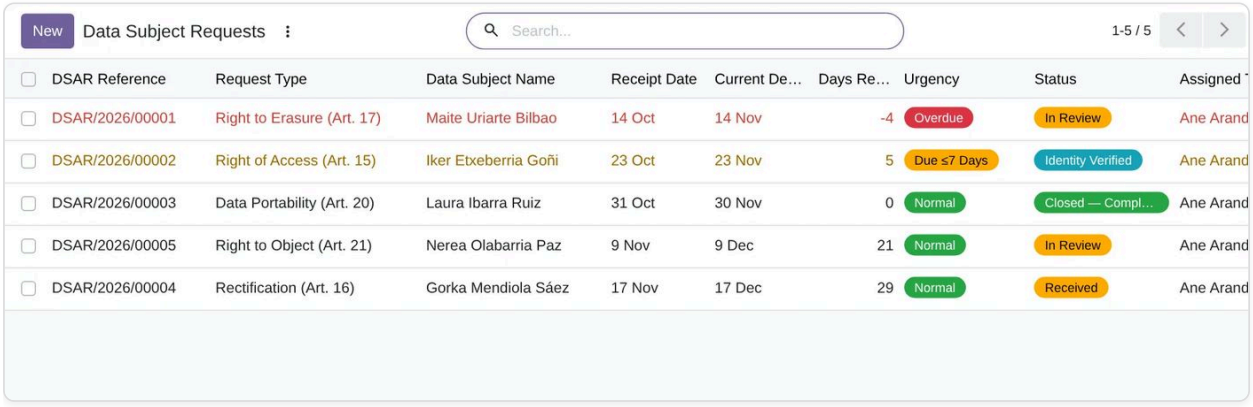
1	What it is and where it is	3
2	Before you start	4
3	Installation	4
4	FlexigoTech Cloud: monitoring of official sources	5
5	Getting it running	7
6	The module's options	9
7	Keeping the record of processing activities	10
8	Handling a data subject request	12
9	Portability, erasure and portal	15
10	Log a breach	16
11	Carry out an impact assessment	18
12	Review retention	20
13	Reports and audit log	22
14	Supervisory authorities and legal bases	24
15	What happens automatically	25
16	If something fails	26
17	Support	27

This manual describes version 20.0.1.1.13 of the module (Odoo branch 20.0, commit e15afc58d). Everything it says comes from its code: menus, buttons, fields, scheduled actions and error messages.

The screenshots come from a test Odoo 20 database, with a made-up company and data and no real connection to FlexigoTech Cloud. In Odoo 17, 18 and 19 the module has its own version: if something on your screen does not match, write to us.

1 What it is and where it is

The module keeps inside Odoo the register of processing activities, the data subjects' requests with their deadlines, the breaches with their 72-hour countdown and the impact assessments. Everything hangs from the **GDPR Toolkit** menu.



- **Real Odoo 20 screenshot.** The **Data Subject Requests** list with the current deadline, the days remaining and the urgency of each request.

Dashboard	Three buttons that open lists. It is explained below.
Processing Activities (RoPA)	**All Activities** and **DPIA Required**.
Data Subject Requests	**All Requests**, **Overdue** and **Due This Week**.
Breach Log	**All Breaches** and **Active Incidents**. Only **GDPR Toolkit / Manager** can see it.
DPIA	**All DPIAs** and **Awaiting DPO Review**. Only **GDPR Toolkit / Manager** can see it.
Retention Management	**Retention Schedule** and **Review History**. Only **GDPR Toolkit / Manager** can see it.
Reports	**Export RoPA (PDF)**, **Export RoPA (Excel)**, **DSAR History Report**, **Breach Log Report** and **DPIA Status Report**. Only **GDPR Toolkit / Manager** can see it.
Configuration	**DPO & Settings**, **Supervisory Authorities**, **Categories of Data**, **Categories of Data Subjects**, **Categories of Recipients**, **Legal Bases** and **Audit Log**. Only **GDPR Toolkit / Manager** can see it.

The **Dashboard** menu opens the company settings with three buttons: **View Open DSARs**, **View Active Breaches** and **DPIAs Pending Review**. Each button opens a list. It does not show figures or indicators.

Outside its menu, the module adds the privacy portal at the address /my/privacy-rights of your Odoo, for those who have a portal account. The module does not place a link on the portal's My Account page: you give the address to the data subject yourself. Five scheduled tasks send alerts by email: the daily request deadline reminder, the breach countdown alert, the daily retention expiry check, the weekly escalation of overdue requests and the annual RoPA review reminder.

2 Before you start

Several of these things are prepared outside Odoo, before installing the module.

- Odoo 17, 18, 19 or 20, on Odoo.sh or on your own server. Odoo Online does not work, as it does not allow installing third-party modules.
- Who will be the **GDPR Toolkit / Manager** and who the **GDPR Toolkit / User**. When the module is installed, the administrator becomes **GDPR Toolkit / Manager**.
- The details of the DPO or, if there is none, of the person responsible for privacy: name, email and phone.
- The primary supervisory authority. It is chosen in the settings from among the authorities the module provides.
- If you want internal notes, the justification for a refusal and the description and consequences of breaches to be stored encrypted, the GDPR_FERNET_KEY variable on the server. Whoever administers the server sets it. Without it those texts are stored unencrypted and **Encryption Key Configured** shows it.
- To include sales or employee data in the portability export, the Sales and Employees apps installed.
- The FlexigoTech Cloud subscription or its 14-day trial. With it, six official sources are monitored every day and an alert arrives when one changes.

> The module does not delete or anonymise data: the erasure check counts what there is and records your decision. Nor does it notify the supervisory authority or communicate anything to the affected persons: you record here what you did. It does not send the reply letter to the data subject. The final decision belongs to the controller or its DPO, and the module is not legal advice.

3 Installation

The module is installed like any third-party Odoo module. An administrator is required.

How to get it

From its page on Odoo Apps (**https://apps.odoo.com/apps/modules/20.0/flexigo_gdpr_toolkit**) or from the module page on flexigotech.com. Choose the Odoo version you use: each version is a separate module.

The module depends on `flexigotech_cloud`, the connection to FlexigoTech Cloud. On Odoo Apps, the module page lists it under «Community Apps Dependencies» and its price is already included; it is also free and has its own page (**https://apps.odoo.com/apps/modules/20.0/flexigotech_cloud**). Place both folders together in the same modules path and Odoo installs `flexigotech_cloud` at the same time.

On Odoo.sh

1. **Upload the folders to your repository**
   Copy `flexigo_gdpr_toolkit` and `flexigotech_cloud` into the branch of your project, in your modules folder, and push.

2. **Wait for Odoo.sh to build the branch**
   When it finishes, both modules are in the branch.

3 **Install the app**

In **Apps**, click **Update Apps List** (with developer mode), search for "GDPR Compliance for Odoo" and click **Activate**.

On your own server

1 **Copy the folders**

Leave `flexigo_gdpr_toolkit` and `flexigotech_cloud` in a folder that is in the `addons_path` of your Odoo.

2 **Restart Odoo**

This way it reads the new modules.

3 **Install the app**

In **Apps**, **Update Apps List**, search for "GDPR Compliance for Odoo" and click **Activate**.

> When installed, Odoo also installs the apps the module depends on: Discuss and the Odoo portal. If you already use them, nothing you have changes.

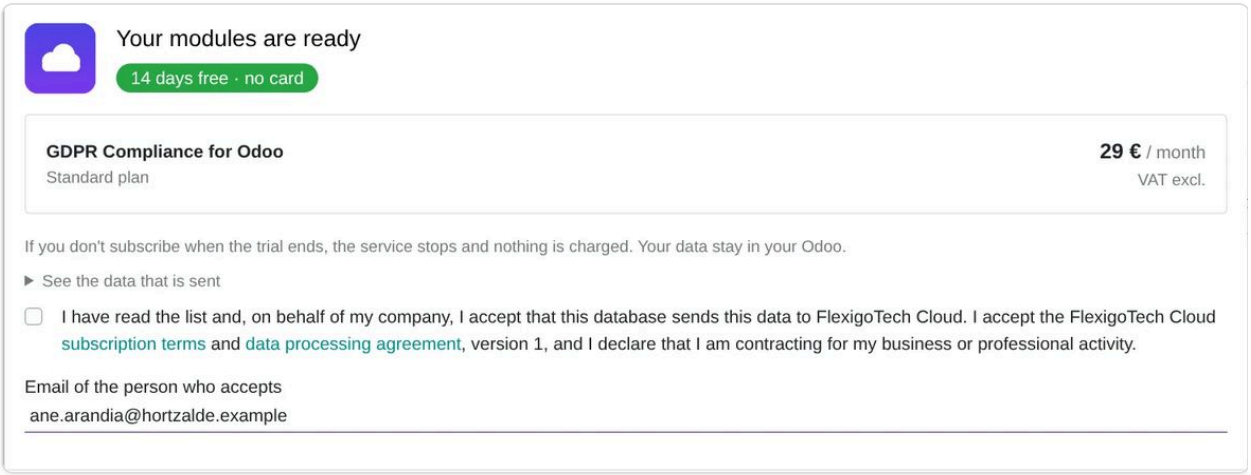
USER MANUAL · GDPR COMPLIANCE

4 FlexigoTech Cloud: monitoring of official sources

The processing register, requests, breaches and impact assessments stay in your Odoo: the module does not send them to FlexigoTech or to any external service. With the subscription, FlexigoTech Cloud monitors six official data protection sources every day and alerts you when one changes. The alerts appear in **Settings › FlexigoTech Cloud** and also arrive by email.

1 **Click Activate in the top bar**

It appears as soon as you install the module. It opens the **Activate FlexigoTech Cloud** window, with the Standard plan and its 14 free days, no card required.



- **Real Odoo 20 screenshot.** The activation window: read the list of data, tick the box and enter your email.

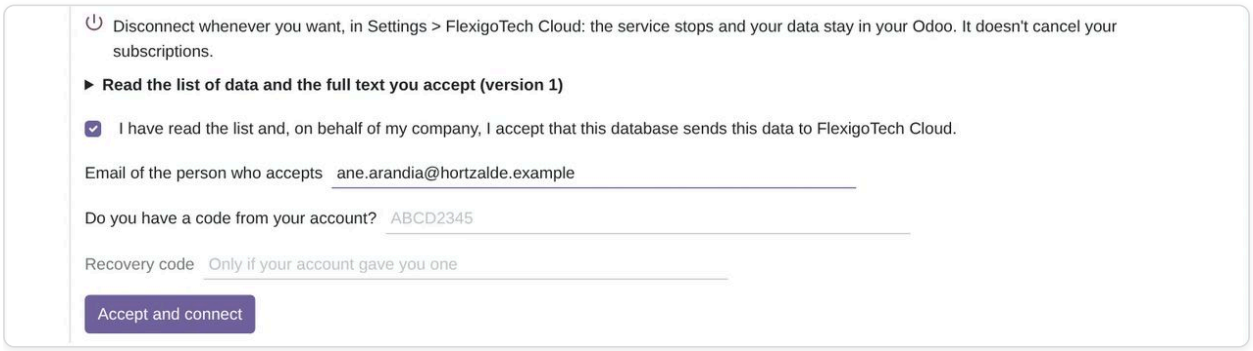
2 **Accept and enter your email**

Tick "I have read the list and, on behalf of my company..." (it covers the subscription terms and the data processing agreement) and enter the **Email of the person who accepts**.

3. **Click Connect and start the trial**
   Odoo registers the database with FlexigoTech Cloud and starts the module trial. If you prefer to leave it for later, **Later** closes the window.

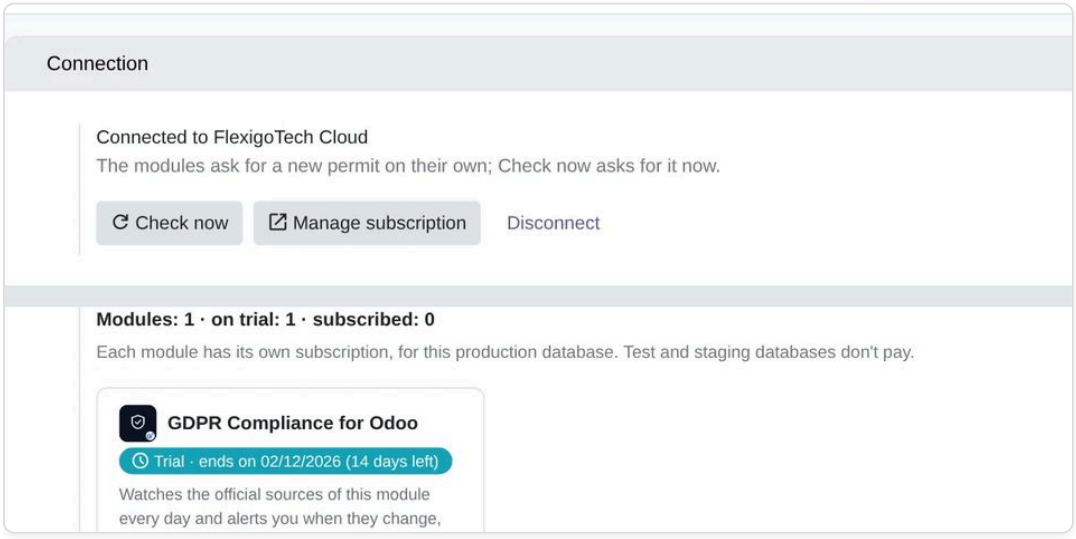
The same, from Settings

In **Settings › FlexigoTech Cloud** is the full list of what the database sends. Tick the box, enter the email and click **Accept and connect**. If you already have an account at app.flexigotech.com, the field **Do you have a code from your account?** links the database to it (the code is valid for 10 minutes).



- **Real Odoo 20 screenshot.** Settings › FlexigoTech Cloud, before connecting: the ticked box, the email and **Accept and connect**.

With the database connected, the **Modules** block shows each module with its status: **On trial** and the date it ends, **Subscribed**, etc. From there you choose the plan (Standard or Pro, monthly or yearly) and click **Subscribe**: payment is made on the Stripe page, outside Odoo.



- **Real Odoo 20 screenshot.** Settings › FlexigoTech Cloud with the database connected and the module on trial.

PLAN	PRICE	INCLUDES
Standard	€29 per month or €290 per year	Support response within 1 business day
Pro	€58 per month or €580 per year	Response within 4 business hours and video call if needed

Prices exclude VAT. If you do not subscribe when the trial ends, the service stops and nothing is charged; your data stays in your Odoo. **Check now** requests the permission immediately (otherwise the module renews it automatically every 6 hours).

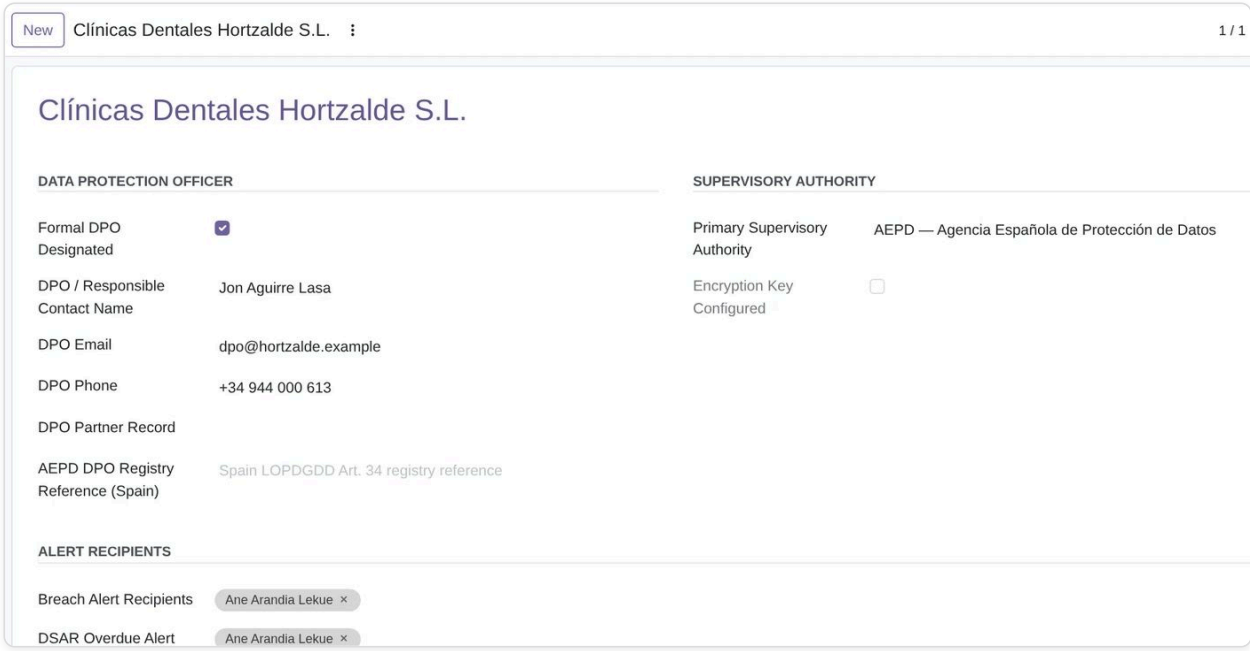
> You cannot start a trial on a neutralised copy (staging) or on a database with demo data: Settings says "This database is a neutralised copy or has demo data, so trials can't be started here."

5 Getting it running

This is done once, after starting the FlexigoTech Cloud trial.

1 Open the configuration

Go to **GDPR Toolkit › Configuration › DPO & Settings**. The GDPR configuration of your company opens; if it does not have one yet, Odoo creates it with the default values.



- **Real Odoo 20 screenshot.** The GDPR configuration of the company, with the DPO details, the supervisory authority and who receives the alerts.

2 Fill in the DPO details

Complete **DPO / Responsible Contact Name**, **DPO Email** and **DPO Phone**. If no DPO is formally designated, clear **Formal DPO Designated**.

3 Choose the supervisory authority

Select the **Primary Supervisory Authority**.

4 Indicate who receives the alerts

Fill in **Breach Alert Recipients** and **DSAR Overdue Alert Recipients**. If you leave them empty, the alerts go to those who have **GDPR Toolkit / Manager** in the company.

5 Adjust the advance days

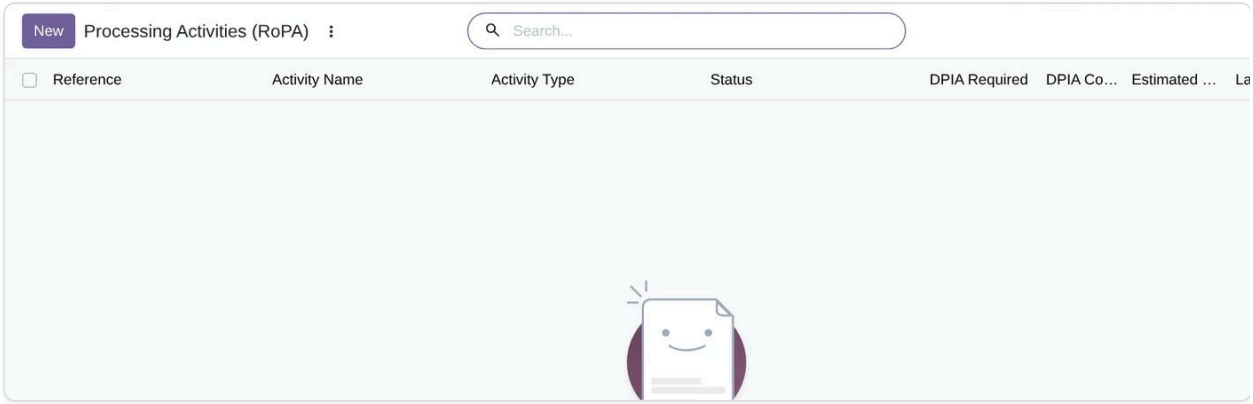
Check **Retention Advance Warning (days)**, which comes set to 30, and **DSAR Reminder Days Before Deadline**, which comes set to 7.

6 **Assign the groups**

Give **GDPR Toolkit / Manager** and **GDPR Toolkit / User** to whoever needs them.

7 **Create the first activity**

Go to **GDPR Toolkit › Processing Activities (RoPA) › All Activities**. At first the list is empty. Click **New** and fill in the activity.



- **Real Odoo 20 screenshot.** The list of processing activities, still with none.

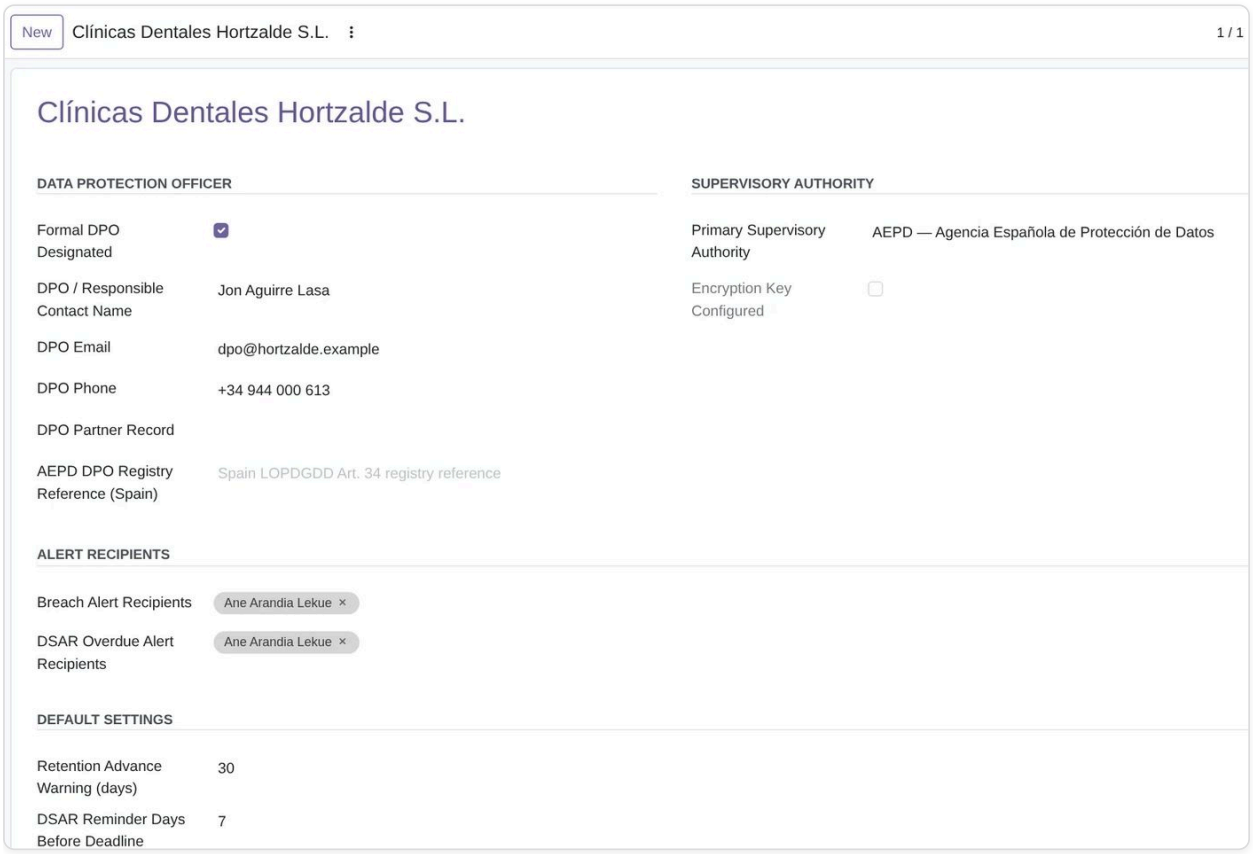
8 **Give the portal address**

If you want data subjects to make requests through the portal, give each one with a portal account the address /my/privacy-rights of your Odoo. The module does not place a link on the My Account page.

After this, the scheduled tasks work on their own. Every day the reminders for requests that are due soon go out and the end of retention is checked. Every hour, in the last 6 hours of a breach's deadline, its alert goes out. Every week the summary of overdue requests goes out and, once a year, the reminder to review the processing register. The reminder for a request goes to the assigned person; the other alerts go to the recipients you have set or, if there are none, to the company's GDPR managers.

6 The module's options

The module's settings are those of your company's GDPR configuration, which is opened from **GDPR Toolkit › Configuration › DPO & Settings**.



- **Real Odoo 20 screenshot.** The options of the GDPR configuration: the DPO, the supervisory authority, the alert recipients and the advance days.

OPTION	HOW IT COMES	WHAT IT DOES
DPO Partner Record, **DPO / Responsible Contact Name**, **DPO Email** and **DPO Phone**	Empty	Details of whoever acts as data protection officer or contact person.
Formal DPO Designated	On	Indicates whether a DPO has been formally designated.
AEPD DPO Registry Reference (Spain)	Empty	Stores the reference under which the DPO is registered with the AEPD.
Primary Supervisory Authority	Empty	Choose from the supervisory authorities loaded in the module.
Breach Alert Recipients	Empty	Users who receive breach alerts. If you choose none, the **GDPR Toolkit / Manager** group of the company receives them.
DSAR Overdue Alert Recipients	Empty	Users who receive the alert for overdue DSARs. If you choose none, the **GDPR Toolkit / Manager** group of the company receives it.

OPTION	HOW IT COMES	WHAT IT DOES
Retention Advance Warning (days)	30	Number of days in advance of the end of the retention period at which the warning is sent.
DSAR Reminder Days Before Deadline	7	Number of days before a request's deadline at which the reminder is sent.
Art. 30(5) SME Exception Note Acknowledged	Off	You confirm that you have read the note on the Art. 30(5) exception for companies with fewer than 250 employees.
Encryption Key Configured	Per server	Read only. Shows whether the server has an encryption key configured.

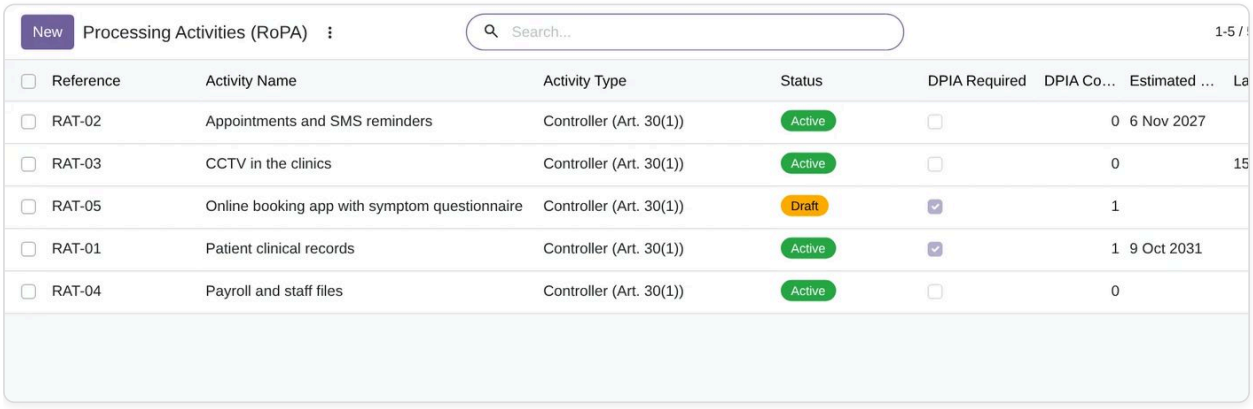
There is only one configuration per company. If you try to create a second one, Odoo shows "Only one GDPR configuration record per company is allowed. A configuration already exists for company ...."

The statutory deadlines cannot be adjusted (one month to respond to a request and two further months of extension, Art. 12.3; 72 hours to notify a breach, Art. 33.1), nor the risk matrix (impact by likelihood), which belongs to the module.

USER MANUAL · GDPR COMPLIANCE

7 Keeping the record of processing activities

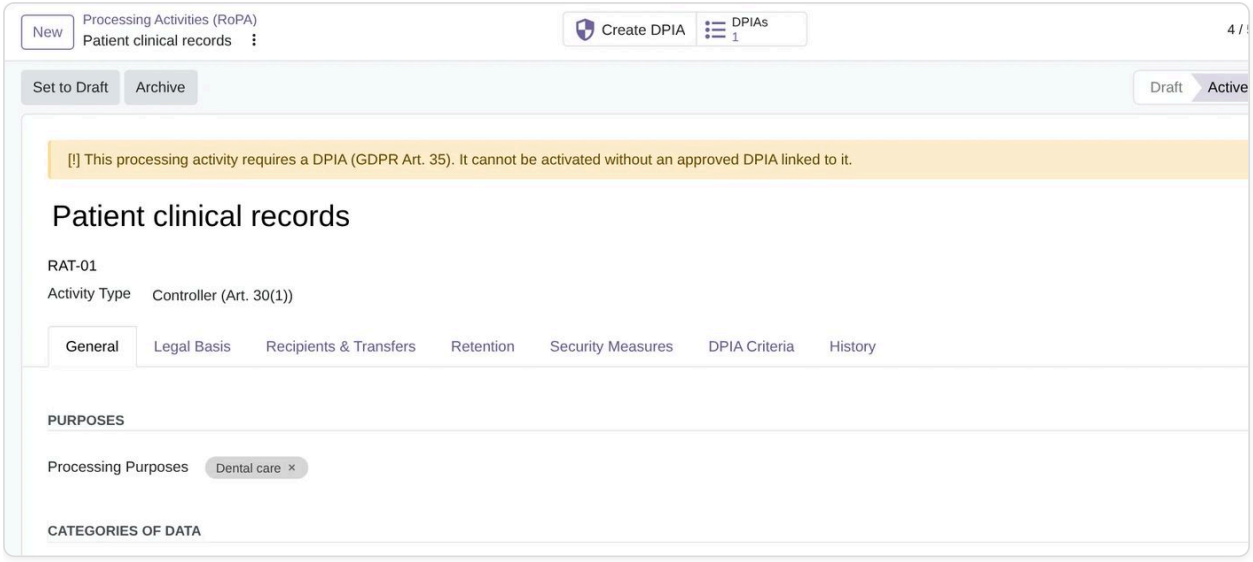
The record of processing activities (RoPA) is kept from **GDPR Toolkit › Processing Activities (RoPA) › All Activities**, with one record per activity.



- **Real Odoo 20 screenshot.** The **Processing Activities (RoPA)** list with its five activities.

Each record covers what Art. 30.1 requires if you act as controller, or Art. 30.2 if you act as processor. You choose this in **Activity Type**. You fill in purposes, categories of data subjects, of data and of recipients, the legal basis under Art. 6 and the one under Art. 9, transfers to third countries with their safeguard, retention and security measures.

The categories of data, of data subjects and of recipients are chosen from the lists in **GDPR Toolkit › Configuration › Categories of Data**, **GDPR Toolkit › Configuration › Categories of Data Subjects** and **GDPR Toolkit › Configuration › Categories of Recipients**. Purposes are created by typing them into the record itself. Odoo assigns the **Reference** when the activity is created and it cannot be edited.



- **Real Odoo 20 screenshot.** The record of an activity with its tabs.

Set Active	Moves the activity to **Active**. It is not shown when the activity is already active.
Set to Draft	Returns the activity to **Draft**. Only shown when the activity is active.
Archive	Moves the activity to **Archived**. It is not shown when the activity is already archived.

Statuses

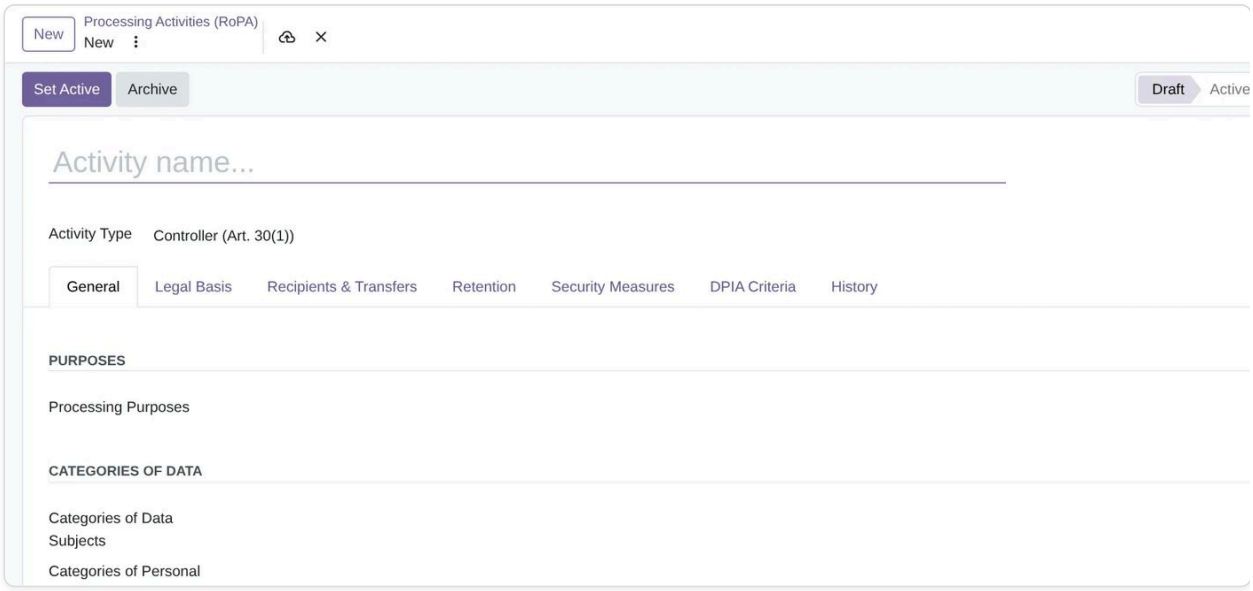
- **Draft**: the status an activity is created with.
- **Active**: the activity that is in force.
- **Archived**: the activity that is no longer used. It remains in the register.

History

Each time the activity is created or a change is saved, the module adds an entry to the history, which can be seen in the **History** tab. These entries cannot be edited or deleted.

Creating an activity

1. **Create the activity**
   In the **Processing Activities (RoPA)** list, click **New**.



- **Real Odoo 20 screenshot.** The form of a new activity in **Draft** status.

2 **Fill in the tabs**

Complete **General**, **Legal Basis**, **Recipients & Transfers**, **Retention** and **Security Measures**.

3 **Activate it**

Click **Set Active**.

> An activity cannot be deleted: the module prevents it in order to keep the audit trail, so it must be archived with **Archive**. Nor can an activity that requires a DPIA be activated if it has no linked approved DPIA.

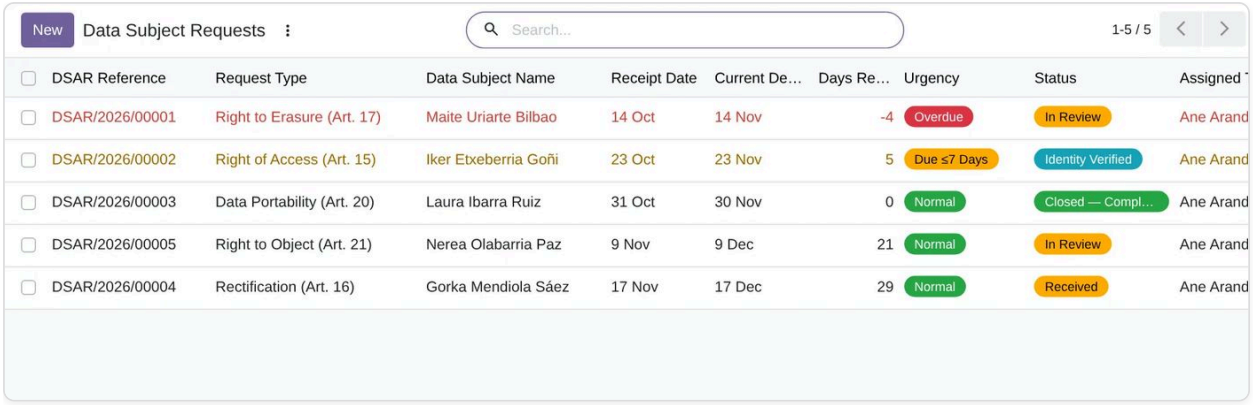
USER MANUAL · GDPR COMPLIANCE

8 Handling a data subject request

Each request from a data subject is handled from its record in **GDPR Toolkit › Data Subject Requests › All Requests**, where you can see the deadline, who is handling it and what status it is in.

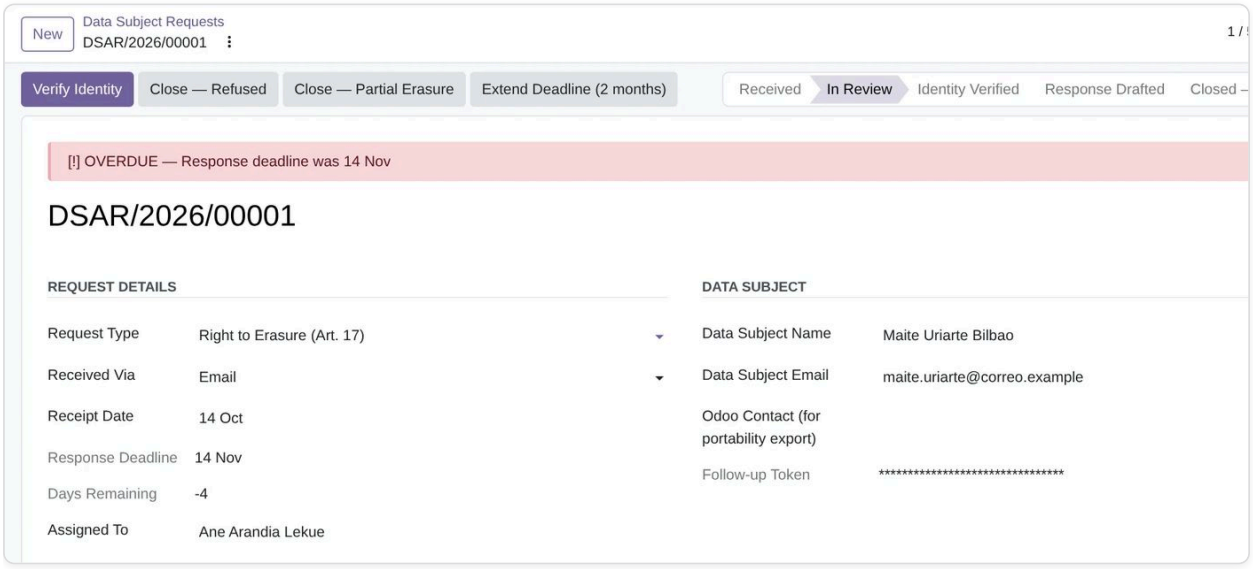
There are six types of request: **Right of Access (Art. 15)**, **Rectification (Art. 16)**, **Right to Erasure (Art. 17)**, **Restriction of Processing (Art. 18)**, **Data Portability (Art. 20)** and **Right to Object (Art. 21)**. The **Received Via** channel can be **Portal Submission**, **Email**, **Letter**, **Phone** or **Manual Entry**.

The **Response Deadline** is one month from the **Receipt Date** (Art. 12.3 GDPR). If necessary, it can be extended by a further two months, also under Art. 12.3, and then the **Current Deadline** becomes the extended one. The **Days Remaining** column counts down to that current deadline.



- **Real Odoo 20 screenshot.** The list of requests with their current deadline, the days remaining, the urgency and the assigned person.

The **Overdue** list shows open requests whose deadline has already passed, and the **Due This Week** list shows those due in seven days or fewer. The **Urgency** column distinguishes these two cases from the rest, which appear as **Normal**.



- **Real Odoo 20 screenshot.** A request with the overdue warning and the buttons for its status.

The person handling each request is shown in **Assigned To**. The **Identity Verification** tab stores the method, the date and who verified it. The **Response** tab holds the **Response Letter**: **Load Response Template** fills it with the general template and, as **Draft Response**, moves the request to **Response Drafted**. **Generate Refusal Letter** produces the refusal letter without changing the status. The letter is not sent from the module.

To refuse, the **Refusal** tab requires the **Refusal Legal Basis** and the **Refusal Justification**. Without a justification the request cannot be closed as refused.

Record buttons

Start Review	Moves the request from **Received** to **In Review**.
Verify Identity	Moves it from **In Review** to **Identity Verified**.
Draft Response	Moves it from **Identity Verified** to **Response Drafted** and loads the template.
Close — Completed	Closes a request with the drafted response.
Close — Refused	Visible when in review, with identity verified or with the response drafted.

Close — Partial Erasure	Only on erasure requests, in those same statuses.
Extend Deadline (2 months)	Visible while the request is still open and not already extended. Asks for the reason.

Statuses

The statuses are **Received**, **In Review**, **Identity Verified** and **Response Drafted**. A request is closed as completed, as refused or with partial erasure. Statuses only move forward: it is not possible to return to an earlier one.

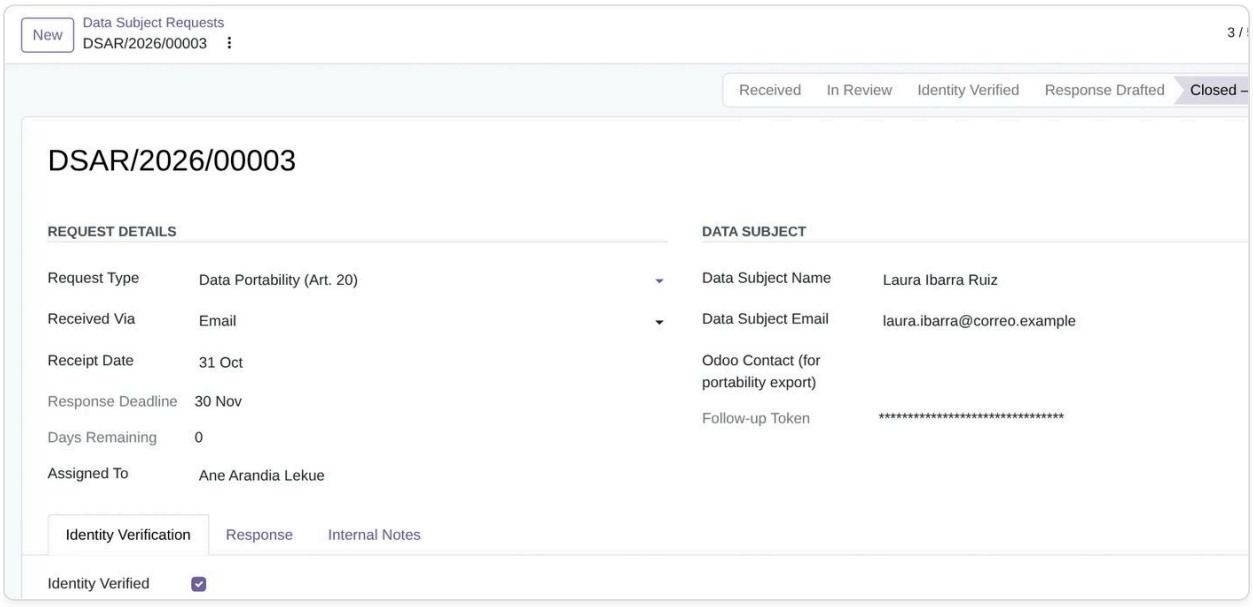
Reminders

The **GDPR: DSAR Deadline Reminder** scheduled task runs daily and sends an email when an open request has reached the number of days set in **DSAR Reminder Days Before Deadline**: to the assigned person; if they have no email, to the GDPR managers; and if there are none either, to the company email. If it cannot reach anyone, it notes this on the request. The **GDPR: DSAR Overdue Escalation** scheduled task runs weekly and sends the summary of overdue requests to the **DSAR Overdue Alert Recipients** or, if there are none, to the GDPR managers.

> A request is not deleted: it is archived. Nor can it return to an earlier status. Only GDPR managers can use the request buttons.

9 Portability, erasure and portal

From a request you prepare the portability export or, if it is an erasure request, the check of what must be retained. The portal lets account holders submit requests themselves.



- **Real Odoo 20 screenshot.** A portability request with identity verified, already closed as completed.

Portability export

The export is generated by hand from the request, using a wizard. No scheduled task prepares it. It requires two things: identity verified and an Odoo contact linked on the request.

DSAR	The request the export is made for. Required.
Contact Data (res.partner)	Checkbox ticked by default. Includes the data on the contact record.
Order History (sale.order)	Includes the contact's orders. Only with the Sales app installed.
HR Data (hr.employee)	Includes the employee record. Only with the Employees app installed.
I confirm explicit HR data inclusion	Confirmation checkbox that goes with the HR data.
Export Format	Two options: **JSON (machine-readable)** or **CSV**.
Export File	The generated file, when the export is ready.
Generate Export	Creates the file. Hidden once the export has already been made.
Close	Closes the wizard.

Checking erasure conflicts

On an erasure request, **Retention Conflict Check** counts what exists for the contact: posted invoices, employee records and sales orders, depending on the apps installed. The wizard shows the groups **Data Subject**, **Conflict**

Findings and **Your Decision per Category**. For each category you choose **Retain (legal obligation)** or **Erase / Anonymise**. The marketing and consent category is set to **Erase / Anonymise** by default.

Record Decision & Close DSAR records the decision in the internal notes and closes the request: as completed if everything is erased, and with partial erasure if anything is retained. **Cancel** exits without recording anything.

Privacy portal

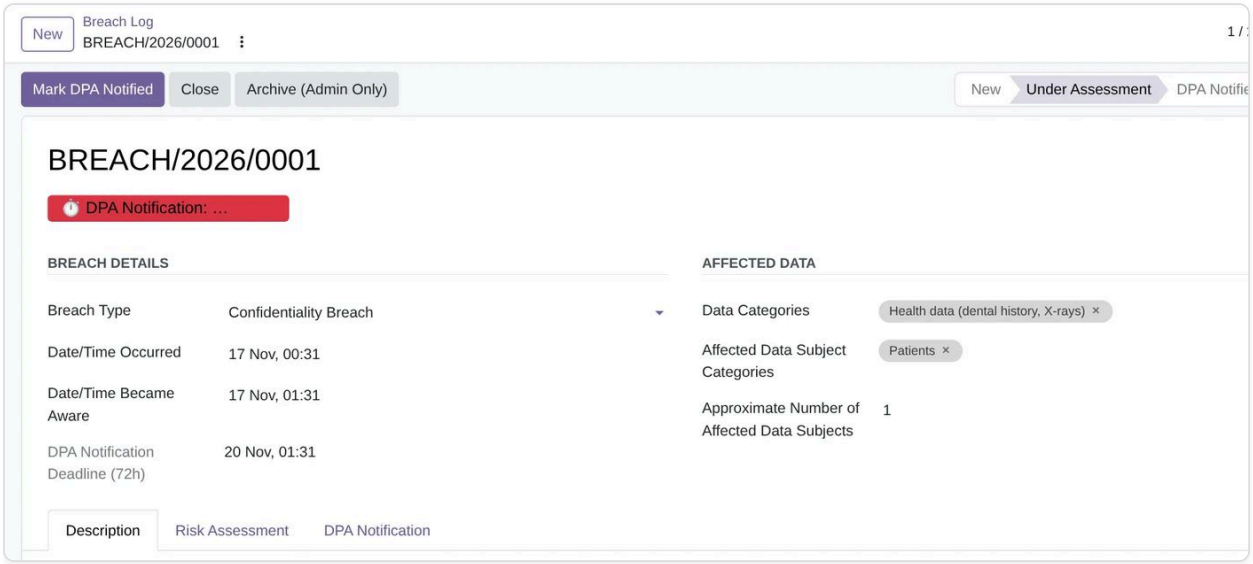
The portal is at /my/privacy-rights on your Odoo and requires logging in, so the data subject needs a portal account. The module does not add a link under My Account: you provide the address yourself. The form asks for the type of right, a text of up to 2,000 characters and up to 3 documents of 50 MB each. On submission, an acknowledgement is sent by email, along with a status page with its own link, which shows the type and the status without any personal data.

> The module does not delete or anonymise data: the erasure check only counts what is there and records your decision. You carry out deletion or anonymisation yourself in Odoo. It does not send the response letter either.

USER MANUAL · GDPR COMPLIANCE

10 Log a breach

Each personal data security breach has its own record, with the Art. 33.1 deadline in view, its assessment, what you notified and the post-breach review.



- **Real Odoo 20 screenshot.** A breach under assessment, showing the deadline countdown and the **Mark DPA Notified** button.

Breaches are under **GDPR Toolkit › Breach Log › All Breaches**. Click **New** to open one. The **Breach Reference** is set by Odoo when you create it and cannot be changed. You enter the data yourself in the form. No data comes in from outside.

What to fill in

Breach Type	Required: **Confidentiality Breach**, **Integrity Breach**, **Availability Breach** or **Multiple Types**.
Date/Time Occurred	When the breach took place.
Date/Time Became Aware	Required. The notification deadline starts from this point.
DPA Notification Deadline (72h)	Odoo calculates it from the date on which you became aware of the breach.
Breach Description and Likely Consequences	Free text, on the **Description** tab.
Impact Score and Likelihood Score	On the **Risk Assessment** tab you choose each one, from 1 to 5.

The 72-hour deadline

Article 33.1 of the GDPR requires the breach to be notified to the supervisory authority without undue delay and, where feasible, no later than 72 hours after becoming aware of it. The module sets that 72-hour deadline from the **Date/Time Became Aware**. When you open the form you see how much time is left, in hours and minutes; once the deadline has passed it reads "EXPIRED". The countdown is calculated when the form is opened and does not update on screen by itself. The **GDPR: Breach Countdown Alert** task runs every hour and, during the last 6 hours of the deadline, sends an email while the breach is not marked as notified: to the **Breach Alert Recipients** or, if there are none, to the GDPR managers.

Risk and notification to data subjects

From impact and likelihood, Odoo calculates the **Risk Score** and the **Risk Level**: low up to 4, medium up to 9, high up to 19 and critical from 20. This matrix belongs to the module, not to the GDPR. With high or critical risk, **Art. 34 Data Subject Notification Required** is flagged. The final decision is taken by the controller or its DPO, and you can record it in **DPO Final Art. 34 Determination**.

Statuses and buttons

Start Assessment	Moves the breach from **New** to **Under Assessment**.
Mark DPA Notified	Shown only under **Under Assessment**. Changes the status to **DPA Notified** and records the date and time. The module does not notify anything: you fill in the method, the reference number and the supporting documents yourself on the **DPA Notification** tab.
Mark Data Subjects Notified	Shown only under **DPA Notified** and when the Art. 34 notification is mandatory. Moves the breach to **Data Subjects Notified** and records the date. You make the notification yourself outside Odoo; the supporting document goes on the **Art. 34 Notification** tab.
Close	Hidden under **New** and **Closed**. Before closing, complete the **Post-Breach Review** tab: root cause, corrective actions, preventive measures, who approves and the date.
Archive (Admin Only)	Visible only to an Odoo administrator. Opens a wizard that asks for the **Archive Reason**.

The statuses are **New**, **Under Assessment**, **DPA Notified**, **Data Subjects Notified** and **Closed**.

1. **Create the breach**
   Click **New**, choose the **Breach Type** and fill in when you became aware of it.

2. **Assess**
   Click **Start Assessment** and score impact and likelihood.

3. **Notify yourself and record it**
   If applicable, notify the authority yourself and click **Mark DPA Notified**.

4. **Communicate and close**
   If mandatory, communicate with the data subjects yourself and click **Mark Data Subjects Notified**. Finish with the post-breach review and **Close**.

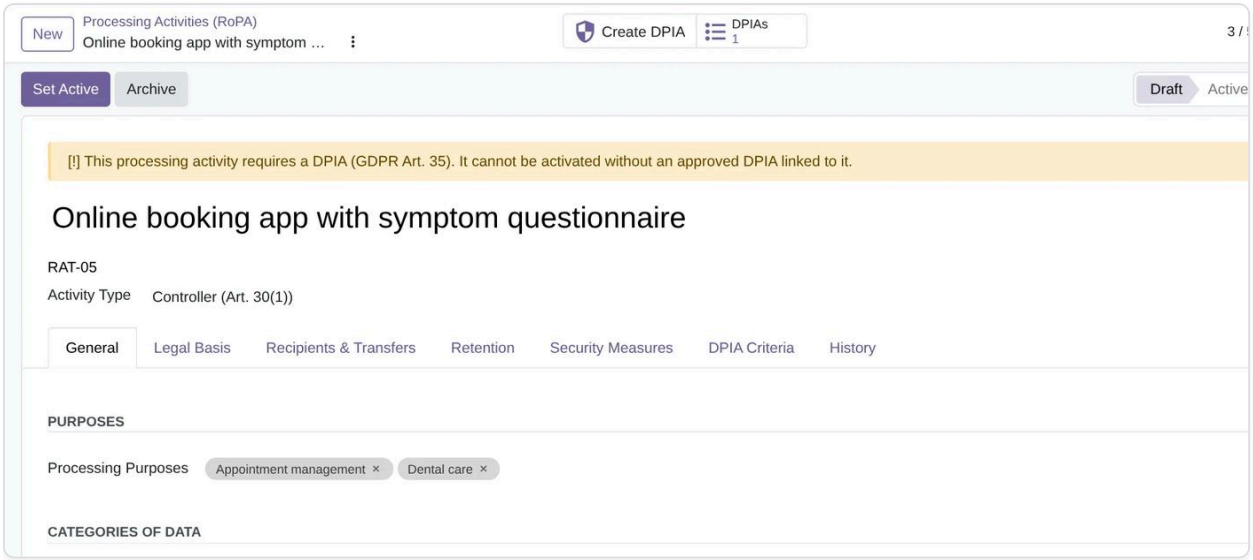
> A breach cannot be deleted: Odoo replies "Breach records are append-only and cannot be deleted. Only an Odoo Administrator can archive a breach record with a written reason.". Only an administrator can archive it, and without a reason you get "Archive reason is required.".

USER MANUAL · GDPR COMPLIANCE

11 Carry out an impact assessment

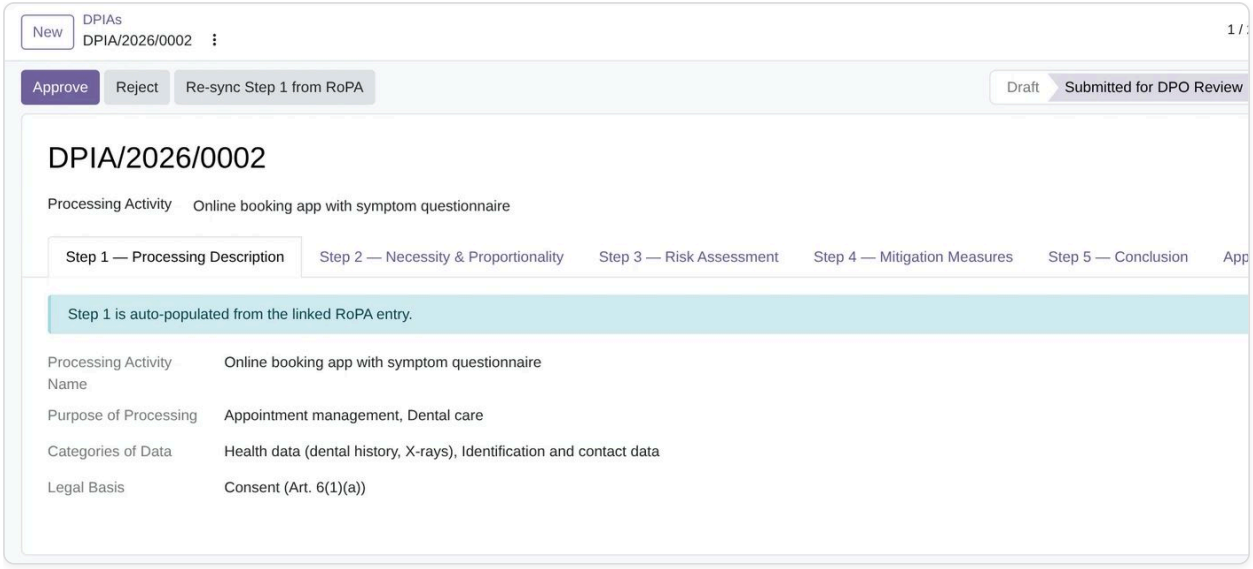
The impact assessment (DPIA, Art. 35 of the GDPR) is carried out under **GDPR Toolkit › DPIA › All DPIAs** and hangs off a RoPA processing activity.

On the **DPIA Criteria** tab of each activity there are nine tick boxes, one per criterion from the WP248 rev.01 guidelines. With two or more ticked, or with the manual flag, the activity shows **DPIA Required**. This is a general rule from those guidelines, not a legal obligation in itself. Flagged activities are listed under **GDPR Toolkit › Processing Activities (RoPA) › DPIA Required**.



- **Real Odoo 20 screenshot.** An activity in **Draft** with the warning that it requires a DPIA.

The assessment is opened from the activity record or from **GDPR Toolkit › DPIA › All DPIAs**. Odoo sets the reference by itself when the record is created.



- **Real Odoo 20 screenshot.** A DPIA submitted for review, with the tabs for the five steps and **Approval**.

The five steps and the approval tab

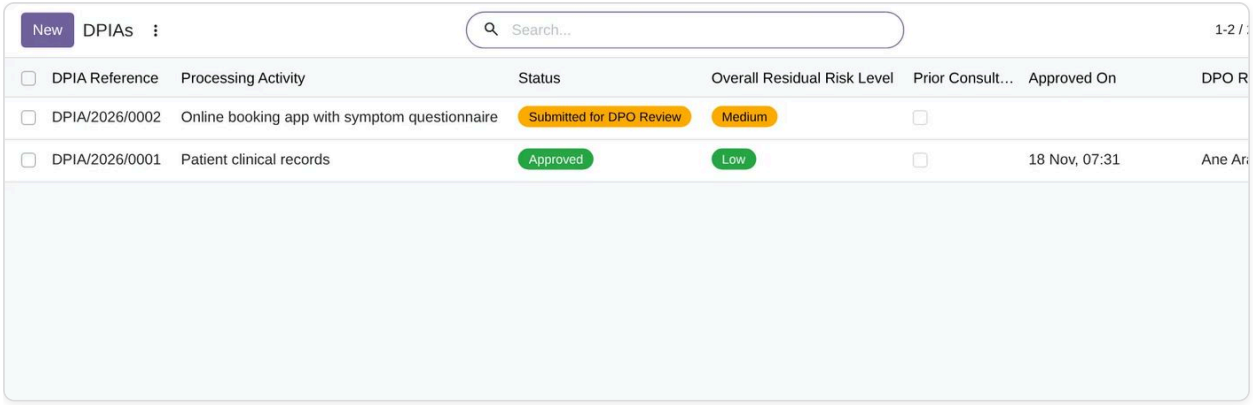
- Step 1, the description of the processing: the name, purpose, data categories and the Art. 6 legal basis are filled in automatically from the RoPA activity.
- Step 2, necessity and proportionality: purpose limitation, data minimisation, justification of the retention period and measures for data subjects' rights.
- Step 3, risk assessment: the list of identified risks.
- Step 4, mitigation measures, in free text.
- Step 5, conclusion and residual risk.
- The **Approval** tab: who submitted it, who reviewed it, when, and their comments.

Each risk carries its impact and likelihood before the measures, and the same two residual values after applying them. Each pair gives a score and a level: up to 4 low, up to 9 medium, up to 19 high and from 20 critical. That matrix belongs to the module, not to the GDPR or the European Data Protection Board guidance. With high or critical residual risk, **Prior Consultation Required (Art. 36)** is ticked automatically. If you submit the prior consultation, record here what you did under **Prior Consultation Submitted** and **Prior Consultation Notes**. The module does not submit it to the authority.

Record buttons

Submit for DPO Review	Moves the DPIA from **Draft** to **Submitted for DPO Review**. Only visible under **Draft**.
Approve	Approves the DPIA. Only visible under **Submitted for DPO Review**.
Reject	Rejects the DPIA. Only visible under **Submitted for DPO Review** and requires comments from the DPO.
Reset to Draft	If a DPIA is in **Rejected**, it returns it to **Draft**.
Re-sync Step 1 from RoPA	Copies step 1 again from the RoPA activity.

The statuses are **Draft**, **Submitted for DPO Review**, **Approved** and **Rejected**. DPIAs awaiting review are under **GDPR Toolkit › DPIA › Awaiting DPO Review**.



- **Real Odoo 20 screenshot.** The list of DPIAs with their status and overall residual risk level.

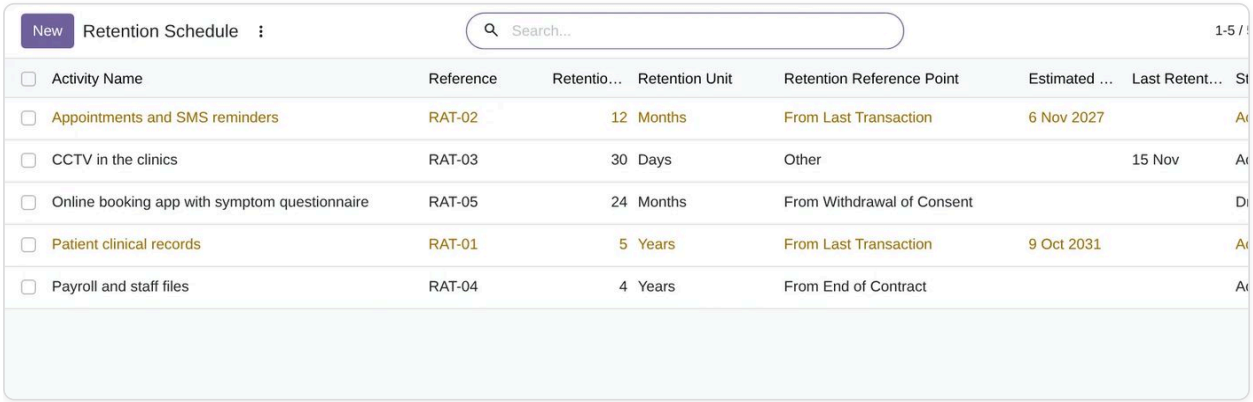
> Submitting, approving and rejecting can only be done by GDPR managers. The final decision rests with the controller or its DPO. The module does not submit the prior consultation to the authority and is not legal advice.

> An activity that requires a DPIA cannot be activated without a linked approved DPIA: the activity record warns you on screen.

USER MANUAL · GDPR COMPLIANCE

12 Review retention

Under **GDPR Toolkit › Retention Management** you see the retention period of each processing activity and record each review you carry out.



- **Real Odoo 20 screenshot.** The **Retention Schedule** with the five activities in the register.

The period for each activity (duration, unit and start of the count) is filled in on the **Retention** tab of the activity, under **GDPR Toolkit › Processing Activities (RoPA) › All Activities**. Odoo calculates the **Estimated Retention End Date** only when the count starts from a **Fixed Date** or from the **From Last Transaction** and that date is set. With **From End of Contract**, **From Withdrawal of Consent** or **Other** it stays empty and that activity receives no alert. The **Retention Schedule** shows the activities with a period set, their estimated date and their **Last Retention Review**, which is filled in automatically each time you save a review.

The alert is raised by the scheduled task **GDPR: Retention Expiry Check**, every day. For each active activity whose estimated date falls within the **Retention Advance Warning (days)** and that has not been reviewed in the last 30 days, it leaves a warning activity on the record and sends an email to the alert recipients set in the

configuration or, if there are none, to the GDPR managers. Another task, **GDPR: Annual RoPA Review Reminder**, reminds you once a year that the activity register is due for review.

Where to record a review

Reviews are listed under **GDPR Toolkit › Retention Management › Review History**, which opens the **Retention Review History** list. Each review is created with **New** and has these fields:

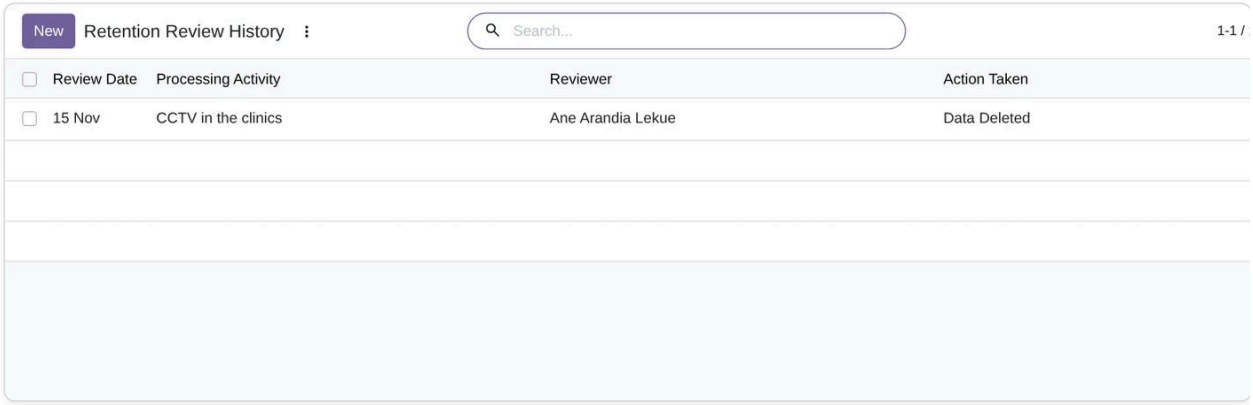
Processing Activity	The activity you are reviewing. Required.
Review Date	Defaults to today's date. Required.
Reviewer	Defaults to your user. Required.
Action Taken	What you did after the review. Required. It has four options: **Data Deleted**, **Data Anonymised**, **Retention Extended** and reviewed with no action needed.
Extension Justification	The reason for extending retention.
New Retention End Date	The date up to which you extend retention.
Notes	Free text.

The review record has no buttons or statuses of its own. The **Action Taken** options are what you note down, not a status of the record.

How to record a review

1. **Open the history**

   Go to **GDPR Toolkit › Retention Management › Review History** and click **New**.



   - **Real Odoo 20 screenshot.** The **Retention Review History** with one review already recorded.

2. **Choose the activity**

   Fill in **Processing Activity**. Today's date and your user are already set.

3. **Indicate the action**

   Choose in **Action Taken** what you did with the data.

4. **If you extend retention**

   With **Retention Extended**, fill in **Extension Justification** and **New Retention End Date**.

5 **Save**

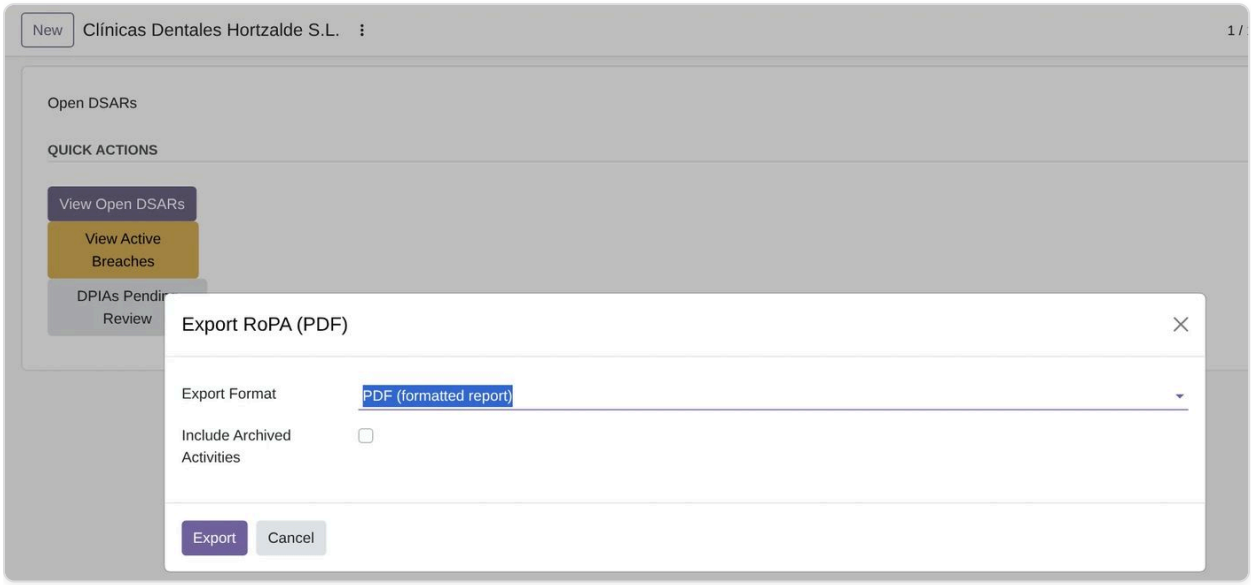
On saving, the activity's **Last Retention Review** becomes the date of this review.

> The module does not delete or anonymise data. The **Data Deleted** and **Data Anonymised** options only record what you did outside this screen. With **Retention Extended**, Odoo will not let you save if the justification is missing ("Extension justification is required when extending retention.") or the new date is missing ("New retention end date is required when extending retention."). The **New Retention End Date** is kept in the review, but it does not change the activity's estimated date: to move it, change the period or its reference date on the **Retention** tab.

USER MANUAL · GDPR COMPLIANCE

13 Reports and audit log

From the **GDPR Toolkit › Reports** menu you export the RoPA to PDF or Excel and the reports on requests, breaches and DPIAs, and under **GDPR Toolkit › Configuration › Audit Log** you see who did what.



- **Real Odoo 20 screenshot.** The RoPA export wizard, with the format and the checkbox for archived activities.

Export the RoPA

1 **Opens the export menu**

Go to **GDPR Toolkit › Reports › Export RoPA (PDF)** or **GDPR Toolkit › Reports › Export RoPA (Excel)**. Both open the same wizard.

2 **Choose the format**

Under **Export Format**, pick **PDF (formatted report)** or **Excel (.xlsx)**. The format from the menu you used comes pre-selected.

3 **Decide about archived ones**

Tick **Include Archived Activities** if you want them in the report. If left unticked, archived activities are not included.

4 **Click Export**

The file is generated. **Cancel** closes the wizard without generating anything.

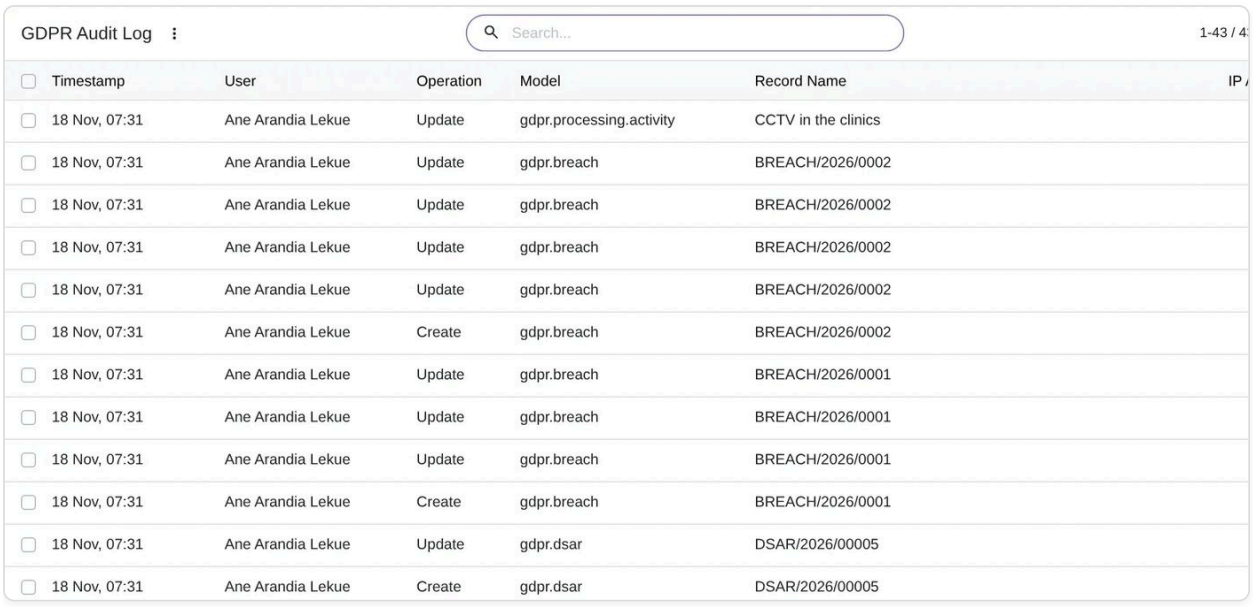
The Excel file has one row per activity. Column headers are always in English, whatever the language.

- If your company has no processing activities, the wizard warns you with "No processing activities found for this company.".
- If the Excel library is missing on the server, it warns you with "openpyxl is not installed. Please install it via pip to use Excel export.". It has to be installed on the server.

Other reports

In the same **Reports** menu, **DSAR History Report** opens the list of all requests, **Breach Log Report** the list of breaches and **DPIA Status Report** the list of DPIAs, so you can filter, group or export them. Each request, breach, DPIA and activity can be printed to PDF from its record.

Audit log



- **Real Odoo 20 screenshot.** The **GDPR Audit Log** with date and time, user, operation, model, record name and IP address.

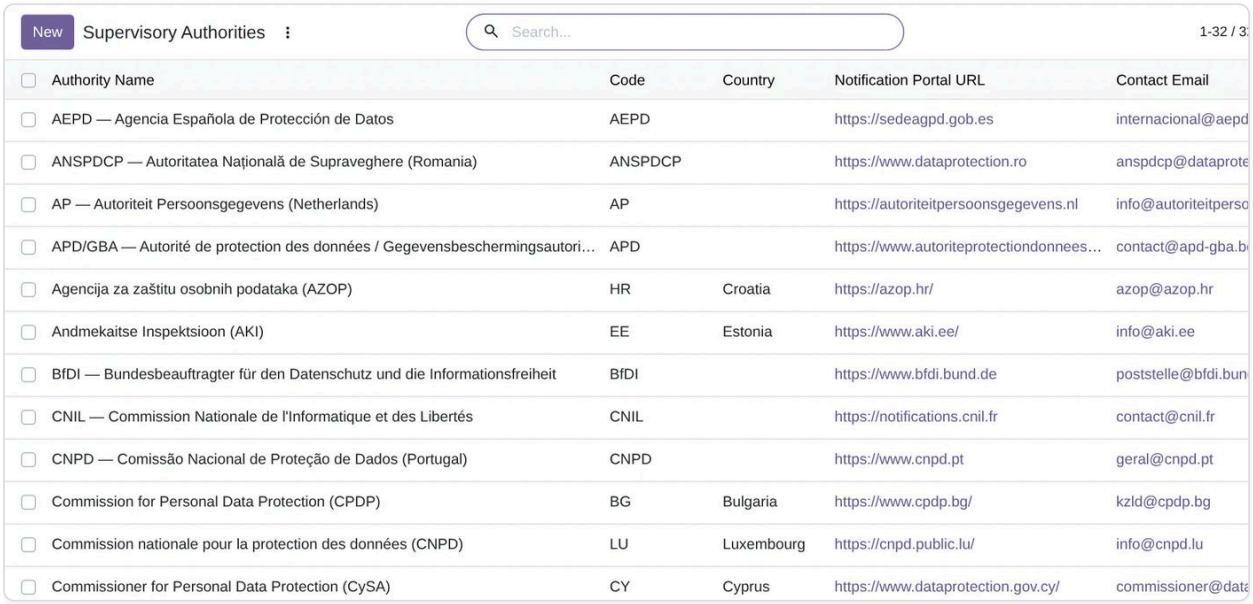
Each entry records who made the change, when, on which record and from which IP address. The change summary masks fields containing personal data. The operations logged are **Create**, **Update**, **Archive**, **Export** and **Portal Submission**.

Create Operations	Filter that shows only creations.
Updates	Filter that shows only changes.
Exports	Filter that shows only exports.
By User	Groups entries by user.
By Model	Groups entries by model.
Change Summary	On each entry's record: the changed fields, with personal data struck through.

> Nobody can modify or delete audit log entries, not even an administrator. Odoo warns you with "You do not have access rights to modify GDPR Audit Log records. Audit log entries are immutable compliance records." or with "You do not have access rights to delete GDPR Audit Log records. They are permanent compliance records per Art. 5(2) GDPR accountability principle.".

14 Supervisory authorities and legal bases

These two lists under **GDPR Toolkit › Configuration** are loaded when the module is installed, and you choose from them the authority in the configuration and the legal bases for each activity.



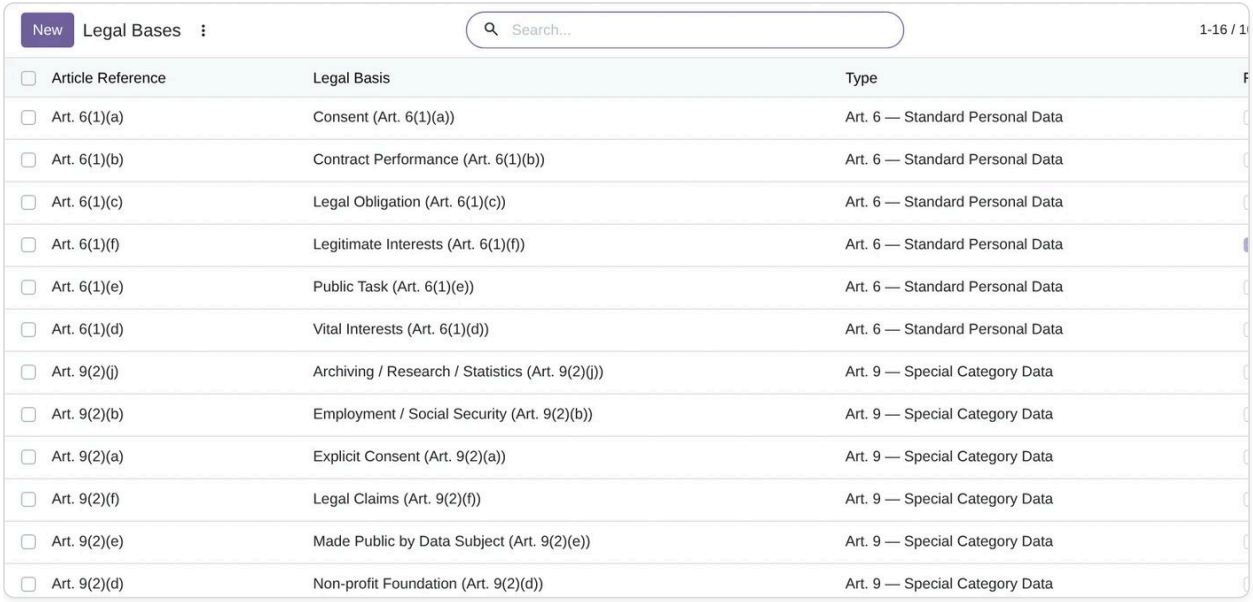
Authority Name	Code	Country	Notification Portal URL	Contact Email
AEPD — Agencia Española de Protección de Datos	AEPD		https://sedeagpd.gob.es	internacional@aepd
ANSPDCP — Autoritatea Națională de Supraveghere (Romania)	ANSPDCP		https://www.dataprotection.ro	anspdcp@dataprote
AP — Autoriteit Persoonsgegevens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

- **Real Odoo 20 screenshot.** The **Supervisory Authorities** list with its 32 records.

The module ships with 32 supervisory authorities. You find them under **GDPR Toolkit › Configuration › Supervisory Authorities**. They are loaded once, at installation. There is no scheduled task or button that updates them, and only an Odoo administrator can change them.

Authority Name	Full name of the authority. Required.
Country	Country the authority belongs to.
Code	Acronym of the authority, for example AEPD, CNIL or BfDI.
Notification Portal URL	Address of the portal where notifications are made.
Contact Email	Contact email of the authority.
Breach Notification Form URL	Address of the form used to notify a breach.
Active	Checkbox that shows whether the authority is in use. Ticked by default.

The main authority is chosen under **GDPR Toolkit › Configuration › DPO & Settings**.



- **Real Odoo 20 screenshot.** The **Legal Bases** list with its 16 records.

Legal bases are under **GDPR Toolkit › Configuration › Legal Bases**. There are 16 and they are loaded at installation: those from Article 6 and those from Article 9.

Legal Basis	Name of the basis. Required.
Article Reference	Reference article, for example art. 6(1)(a).
Type	Shows whether it is an Article 6 basis, for ordinary personal data, or an Article 9 basis, for special categories of data.
Requires Legitimate Interests Balancing Test	Checkbox that marks the bases requiring that balancing test.

> These lists have no states or workflow. Both are loaded when the module is installed, and only an Odoo administrator can change them.

USER MANUAL · GDPR COMPLIANCE

15 What happens automatically

The module ships with five scheduled tasks, all active on installation, that notify whoever runs GDPR compliance in your company.

TASK	FREQUENCY	WHAT IT DOES
GDPR: DSAR Deadline Reminder	Daily	Sends an email when an open request has the number of days set in **DSAR Reminder Days Before Deadline** left: to the assigned person or, if they have no email, to the GDPR managers.
GDPR: Breach Countdown Alert	Hourly	In the last 6 hours before the deadline of an open breach not marked as notified, sends an email to the **Breach Alert Recipients** or to the GDPR managers.

TASK	FREQUENCY	WHAT IT DOES
GDPR: Retention Expiry Check	Daily	Creates a reminder activity and sends an email for each active activity whose retention end is approaching and has not been reviewed in the last 30 days.
GDPR: DSAR Overdue Escalation	Weekly	Sends the summary of overdue requests to the **DSAR Overdue Alert Recipients** or to the GDPR managers.
GDPR: Annual RoPA Review Reminder	Every 12 months	Emails a reminder that the record of processing activities is due for review.

Alerts are emailed to users with an email address, in each user's own language. Frequencies are changed under **Settings › Technical › Automation › Scheduled Actions**, with developer mode enabled.

USER MANUAL · GDPR COMPLIANCE

16 If something fails

When the module stops you or warns you, it is usually for one of these reasons.

A processing activity will not activate and shows a warning that an approved DPIA is missing.	Complete and approve a DPIA linked to the activity. Once it is approved, click **Set Active** again.
A request of rights does not go back to an earlier state.	The state only moves forward. If you made a mistake, note it in the internal notes and continue from the current state.
The portability export is not generated.	First verify the identity of the request and link an Odoo contact in the field **Odoo Contact (for portability export)**.
You cannot close a request as refused.	Write the reason for the refusal first. It is mandatory.
You cannot extend the deadline of a request.	Fill in the reason for the extension. Without a reason, the module will not allow the extension.
You cannot reject a DPIA.	Write the DPO's comments. They are mandatory when rejecting.
You cannot delete a breach, a request or a processing activity.	They form part of the audit trail. Archive them instead. For breaches, only an Odoo administrator can archive, and only with a written reason.
Internal notes are stored unencrypted.	The encryption key is missing on the server. In the configuration, **Encryption Key Configured** tells you whether it is set.

Odoo warnings say what is missing. Usually it is enough to complete it and repeat the action.

17 Support

Every purchase includes 2 months of support: we help you install it, set it up and get it working, by email and video call. While you're subscribed, support for the service stays included: on the Standard plan we respond within 1 business day; on Pro, within 4 business hours, and if needed we review it by video call. Tell us your Odoo version, the module version and, if there is an error, its full text.

Email

To install it, set it up or for any question.
comercial@flexigotech.com

On the web

The module page, with the guide and the prices.
flexigotech.com/en/odoo-gdpr.html

On Odoo Apps

The module page on the Odoo store.
apps.odoo.com

GDPR Compliance is a FlexigoTech module for Odoo. FlexigoTech is a brand of Flexibles y Accesorios Gobe, S.L. (Barcelona, Spain).