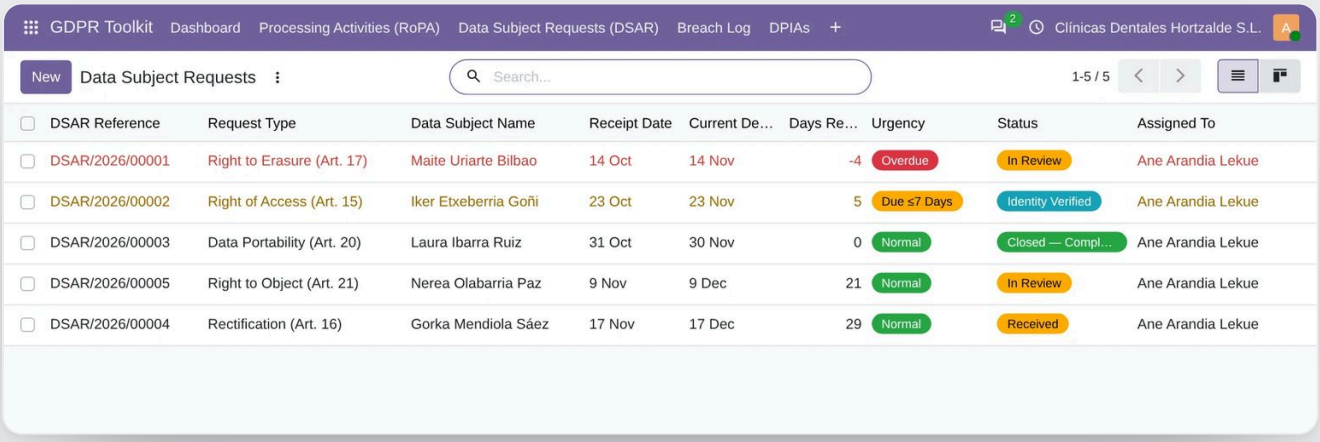
MODULE GUIDE · DATA PROTECTION

GDPR Compliance for Odoo

The record of processing, requests with their deadline, breaches with their 72 hours and DPIAs, inside Odoo.

Odoo 17 · 18 · 19 · 20 | 14-day trial, no card | Edition of 19-11-2026





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 chapter starts. Menu and button names are those of Odoo in English.

1	Who it is for and what it solves	3
2	The module in figures	4
3	Where you see it in your Odoo	5
4	What you need before you start	6
5	The FlexigoTech Cloud trial	6
6	Setting it up step by step	8
7	The register of processing activities	10
8	Data subject requests and their deadlines	13
9	Portability, erasure and the privacy portal	18
10	The breach log and the 72 hours	21
11	Data protection impact assessments (DPIAs)	24
12	The Retention Schedule and Its Reviews	28
13	Reports, Exports and the Audit Log	31
14	Supervisory Authorities and Legal Bases	34
15	What goes to FlexigoTech Cloud and what comes back	37
16	What happens automatically	38
17	Module options and their defaults	39
18	Security and personal data	41
19	Multiple companies	41
20	If something goes wrong	41
21	Other ways to do it	43
22	Plans and pricing	43
23	Frequently asked questions	44
24	Glossary	47
25	Checklist and contact	48

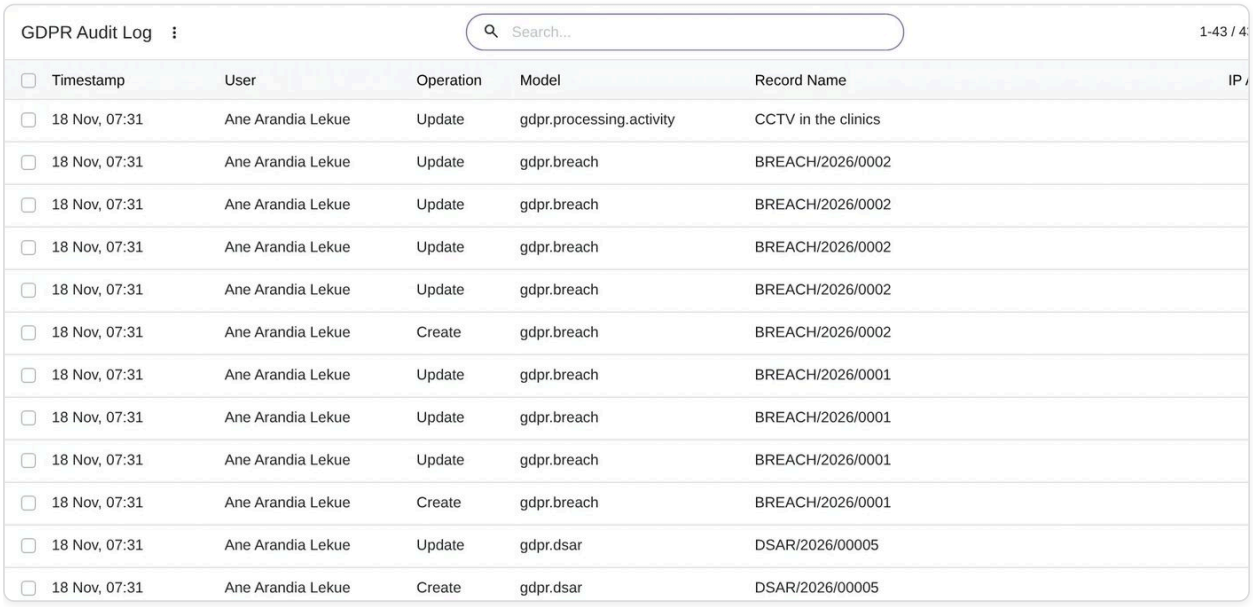
This guide describes version 20.0.1.1.13 of the module (Odoo branch 20.0, commit e15afc58d). Everything in it comes from its published code, the platform's official documentation or real screenshots.

The screenshots come from a test Odoo 20 database, with a made-up company and data and no real connection to FlexigoTech Cloud. The module also has a version for Odoo 17, 18 and 19.

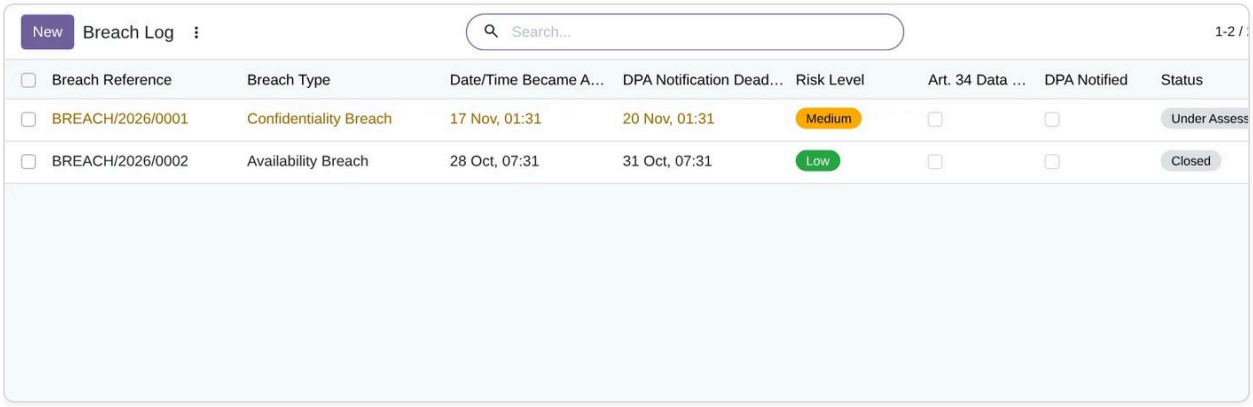
1 Who it is for and what it solves

Without the module, the processing register usually lives in loose spreadsheets. Request deadlines are counted by hand and nobody warns you when they are getting close. There is no history of who changed what and when. For a breach, nobody keeps track of the hours since awareness was established.

With the module, all of this lives inside Odoo, with its deadlines in view and an audit log that cannot be altered.



- **Real Odoo 20 screenshot.** The **GDPR Audit Log** with the date, user and operation for each change.



- **Real Odoo 20 screenshot.** The **Breach Log** list with the 72-hour notification deadline for each breach.

What changes day to day

- Each processing activity is recorded with its purposes, legal bases, categories of data and data subjects, recipients and retention period, and every change is saved in its history.
- Data subject requests carry a one-month deadline from receipt, extendable by a further two months if needed and justified (Art. 12.3). There are lists of those that are overdue and those due this week.
- A breach starts counting 72 hours from the moment you record when awareness was established (Art. 33.1), and, in its last 6 hours, the module sends an email every hour for as long as you do not mark it as notified.
- An activity that meets two of the WP248 criteria is marked **DPIA Required** and the module will not let you activate it until it has an approved DPIA. The DPIA (Art. 35) has five steps and flags prior consultation when the residual risk requires it (Art. 36).

- The data subject with a portal account submits their request from /my/privacy-rights and receives an acknowledgement by email.

What it does not do

- It does not delete or anonymise Odoo data. The deletion check counts what is there and records your decision; deleting or anonymising is up to you.
- It does not notify the supervisory authority or tell anyone affected. You record here what you did: the status, the date and time, the method and the reference.
- It does not send the reply letter to the data subject. You draft it in the response tab from a template and send it yourself.
- It does not decide for you whether a breach must be notified or whether a DPIA is needed. The risk matrix (impact by likelihood) and its cut-offs belong to the module, not to the GDPR or the European Data Protection Board guidelines; the final decision rests with the controller or its DPO.
- It is not legal advice.

MODULE GUIDE · GDPR COMPLIANCE

2 The module in figures

155
automated tests

7,013
lines of code in Odoo Apps (branch 20.0)

32
supervisory authorities

16
legal bases

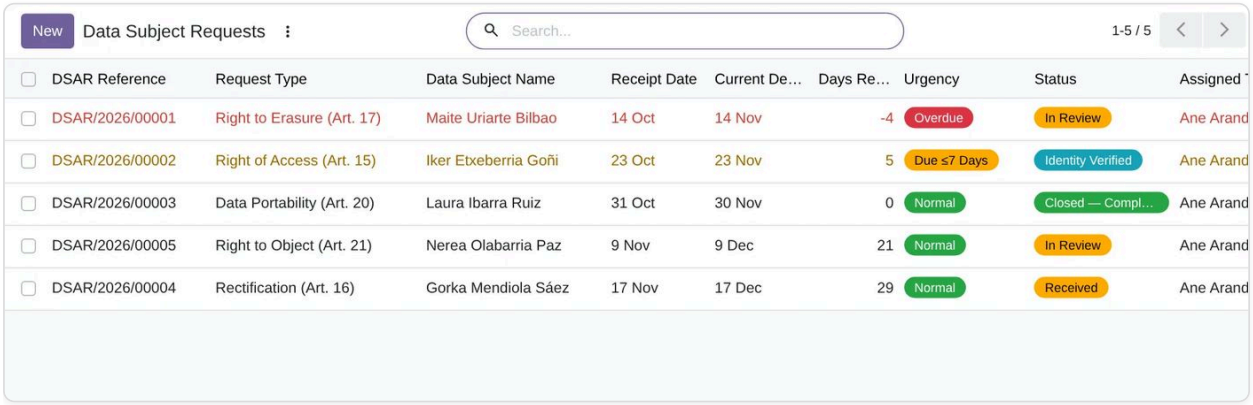
5
scheduled tasks

14
days of FlexigoTech Cloud trial

It only depends on Odoo Community modules (base, mail and portal) and on `flexigotech_cloud`, so it works on Community and on Enterprise. There is a version of the module for Odoo 17, 18, 19 and 20.

> How it was tested: the module comes with 155 automated tests in its Odoo 20 version. The FlexigoTech team tested it on Odoo 17, 18, 19 and 20, on Community databases and on Odoo.sh, and checked its deadlines against the published text of the GDPR on EUR-Lex (Articles 12.3, 33.1, 35 and 36). No authority has reviewed the module and it is not legal advice: the final decision is yours or your DPO's.

3 Where you see it in your Odoo



- **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. This 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**. Visible only to **GDPR Toolkit / Manager**.
DPIA	**All DPIAs** and **Awaiting DPO Review**. Visible only to **GDPR Toolkit / Manager**.
Retention Management	**Retention Schedule** and **Review History**. Visible only to **GDPR Toolkit / Manager**.
Reports	**Export RoPA (PDF)**, **Export RoPA (Excel)**, **DSAR History Report**, **Breach Log Report** and **DPIA Status Report**. Visible only to **GDPR Toolkit / Manager**.
Configuration	**DPO & Settings**, **Supervisory Authorities**, **Categories of Data**, **Categories of Data Subjects**, **Categories of Recipients**, **Legal Bases** and **Audit Log**. Visible only to **GDPR Toolkit / Manager**.

The **Dashboard** menu opens the company configuration with three buttons: **View Open DSARs**, **View Active Breaches** and **DPIAs Pending Review**. Each button opens a list. It shows no figures or indicators.

Outside its menu, the module adds the privacy portal at /my/privacy-rights on your Odoo, for those with 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 emails: 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.

4 What you need before you start

- 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 **GDPR Toolkit / Manager** and who **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 telephone.
- The primary supervisory authority. It is chosen in the configuration from among the authorities the module includes.
- 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. It is set by whoever administers the server. Without it, those texts are stored unencrypted and **Encryption Key Configured** shows so.
- To include sales or employee data in the portability export, the Sales and Employees apps must be installed.
- A FlexigoTech Cloud subscription or its 14-day trial. With it, six official sources are monitored every day and an alert arrives when one changes.

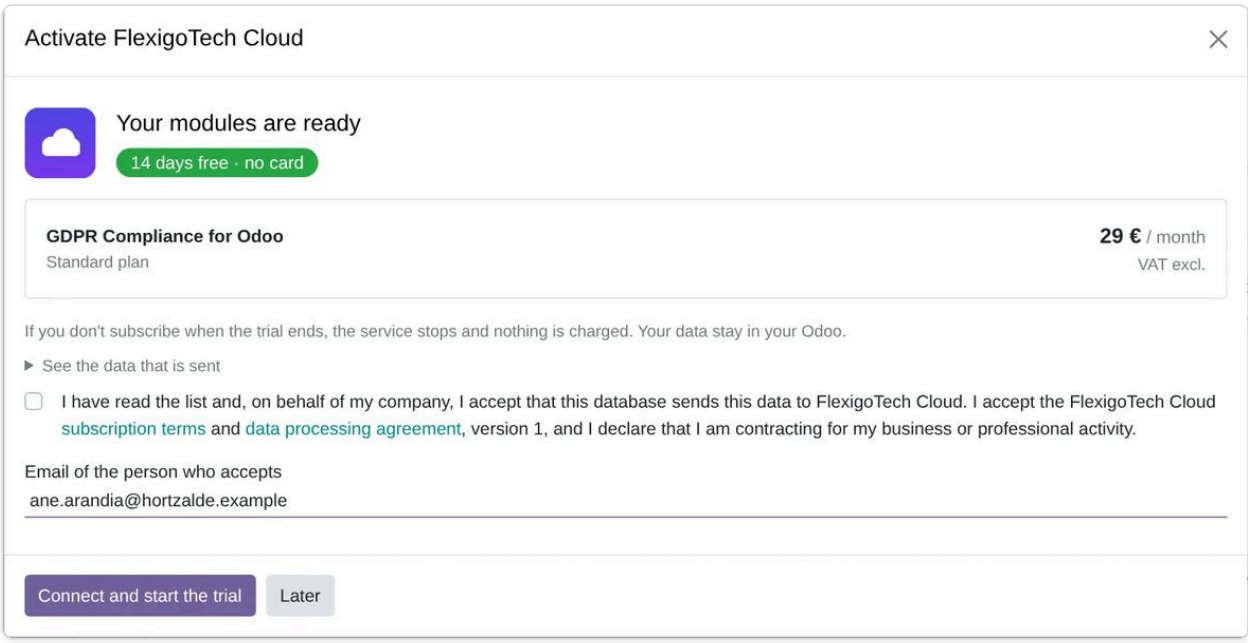
> The module does not delete or anonymise data: the deletion check counts what is there and records your decision. Nor does it notify the supervisory authority or tell anyone affected: you record here what you did. It does not send the reply letter to the data subject. The final decision rests with the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

It is installed like any third-party Odoo module, on Odoo.sh or on your server. Odoo installs `flexigotech_cloud`, the connection to FlexigoTech Cloud, at the same time, along with the Odoo apps it depends on: Discuss and the portal.

5 The FlexigoTech Cloud trial

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 days free, 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**

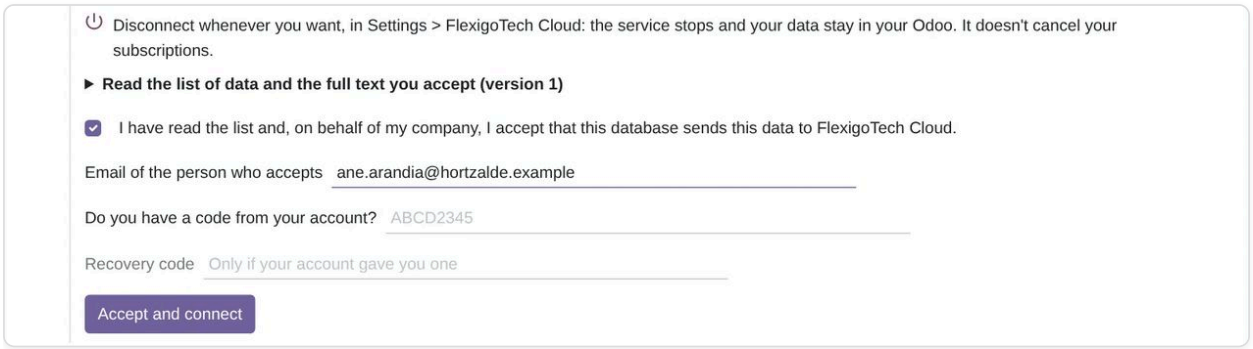
Tick «I have read the list and, on behalf of my company...» (it covers the subscription terms and the data processing agreement) and enter the **Email of the person who accepts**.

3 **Click Connect and start the trial**

Odoo registers the database with FlexigoTech Cloud and starts the module's trial. If you want to do it later, **Later** closes the window.

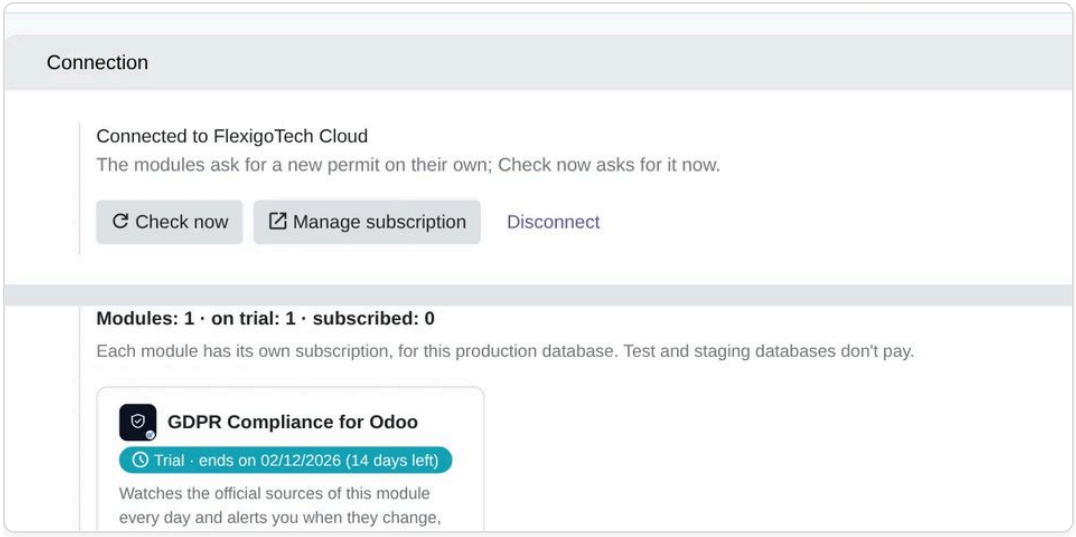
The same, from Settings

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**, and so on. 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.

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 permission immediately (otherwise the module renews it automatically every 6 hours).

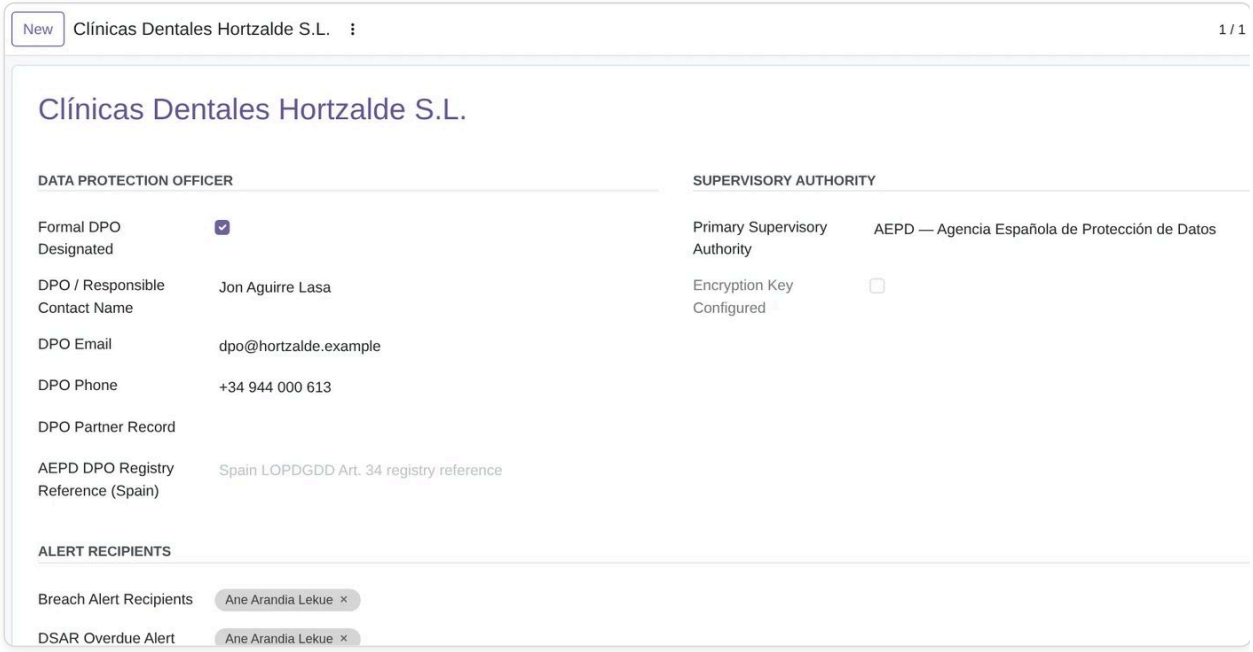
> You cannot start a trial on a neutralised copy (staging) or on a database with demo data: Settings says so with «This database is a neutralised copy or has demo data, so trials can't be started here.»

MODULE GUIDE · GDPR COMPLIANCE

6 Setting it up step by step

1 Open the configuration

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



- **Real Odoo 20 screenshot.** The company's GDPR configuration, 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 hold **GDPR Toolkit / Manager** in the company.

5 **Adjust the advance days**

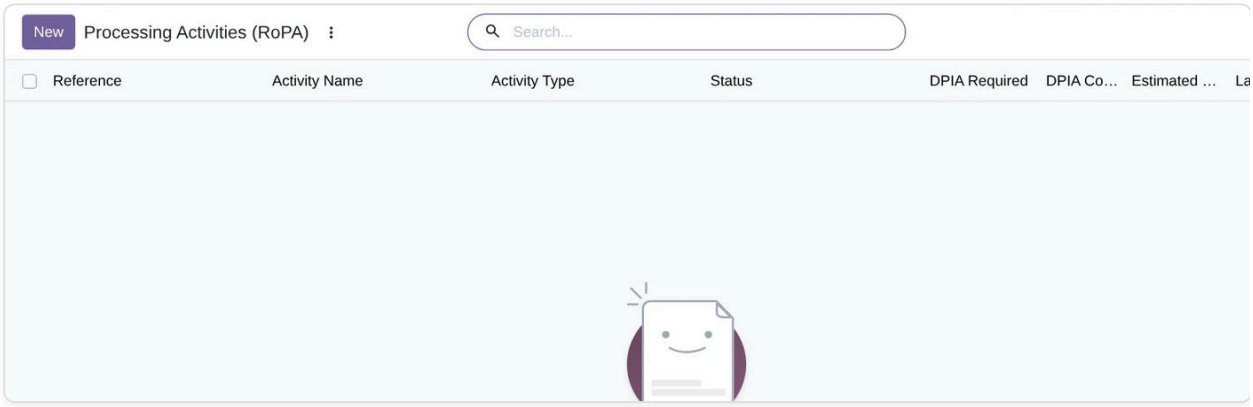
Review **Retention Advance Warning (days)**, which is set to 30, and **DSAR Reminder Days Before Deadline**, which is set to 7.

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.



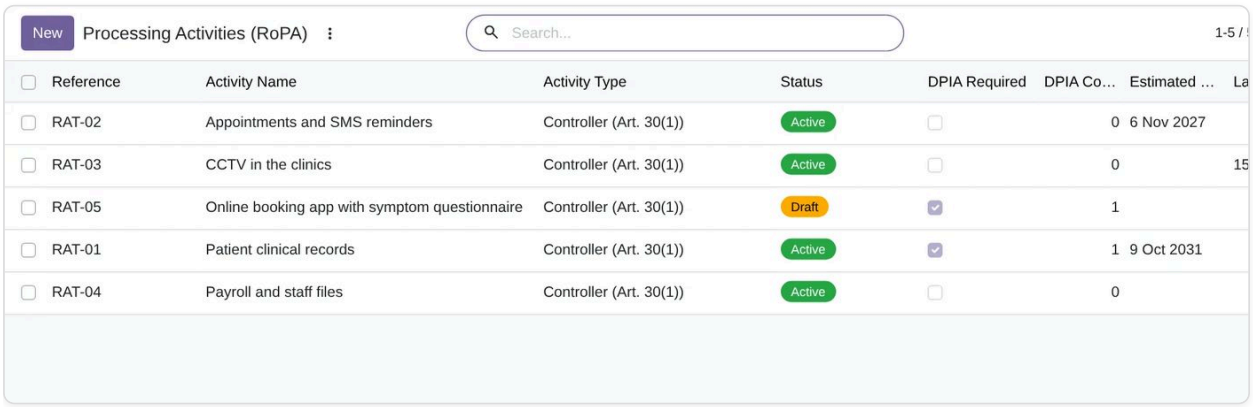
- **Real Odoo 20 screenshot.** The processing activities list, still with none.

8 **Give the portal address**

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

After this, the scheduled tasks work on their own. Each day the reminders for requests falling 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. Each 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 set or, if there are none, to the company's GDPR managers.

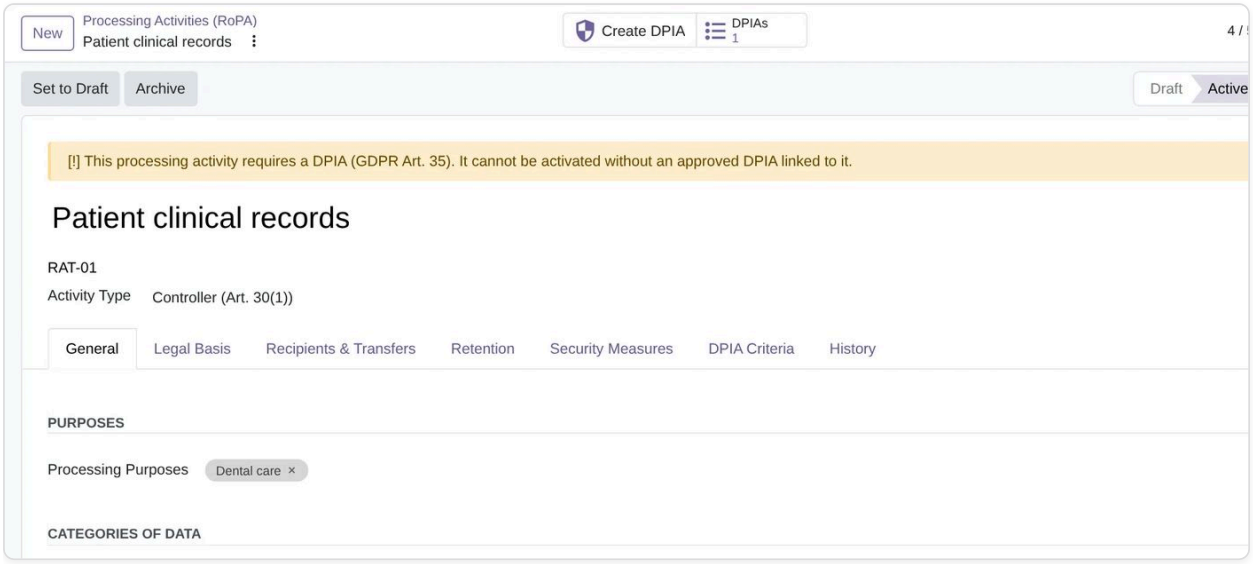
7 The register of processing activities



- **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 which in **Activity Type**. You fill in purposes, categories of data subjects, categories 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, data subjects and 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. The **Reference** is set by Odoo when the activity is created and cannot be edited.



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

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

Statuses

- **Draft**: the status the activity is created with.
- **Active**: the activity that is in force.

- **Archived**: the activity that is no longer used. It stays in the register.

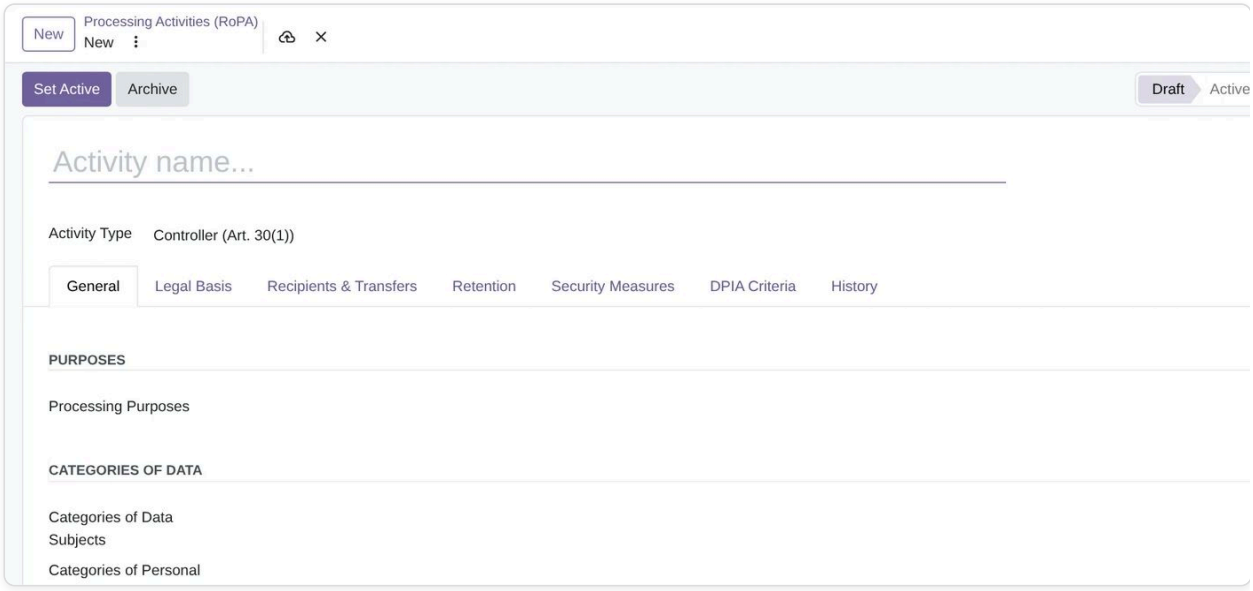
History

Each time the activity is created or a change is saved, the module adds an entry to the history, which you can see on 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 blocks this to keep the audit trail, so you must archive it with **Archive**. An activity that requires a DPIA cannot be activated either unless it has an approved DPIA linked.

What each status means

Draft	Initial status. You can fill in and correct the record while you complete it.
Active	The activity is in force. To get here, if it requires a DPIA, it must have an approved DPIA linked. From here, **Set to Draft** returns it to **Draft**.
Archived	The activity is withdrawn from use, but its record and history are kept. It is the only way to remove it, because it cannot be deleted.

When the module will not let you do something

- Activating an activity with **DPIA Required** and no approved DPIA linked: you get «Cannot activate processing activity "...": a DPIA is required but no approved DPIA is linked. Please complete and approve a DPIA first.»
- Deleting an activity: you get «Processing activity records cannot be deleted to preserve the audit trail. Please archive the record instead.»
- Modifying or deleting a history entry: you get «History records are immutable and cannot be deleted. They are part of the GDPR audit trail.» and «History records are immutable.»

When a DPIA is mandatory

DPIA Required is set automatically when two or more of the criteria on the **DPIA Criteria** tab are met, or when it is forced by hand with **DPIA Required (Manual Override)**. This two-criteria rule comes from the WP248 rev.01 guidelines and is a general rule of thumb, not a legal obligation. The criteria are **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** and **Prevents exercise of rights**. **DPIA Criteria Met** shows how many are met, and **DPIA Requirement Reason** records the justification.

Tabs and fields on the form

General	**Activity Name**, **Activity Type**, the **Purposes** and **Categories of Data** groups, and the processor details, which go in their own group, **Processor Details (Art. 30(2))**.
Legal Basis	**Legal Basis (Art. 6)** and **Special Category Legal Basis (Art. 9)**.
Recipients & Transfers	**Categories of Recipients**, **Third-Country Transfer**, **Third Countries**, **Transfer Safeguard** and **Safeguard Notes**.
Retention	**Retention Duration**, **Retention Unit** and **Retention Reference Point**, plus **Reference Date (fixed)**, **Last Transaction Date**, **Estimated Retention End Date** and **Last Retention Review**.
Security Measures	**Technical & Organisational Security Measures**.
History	**Version History**: one entry for each change.

The options for **Transfer Safeguard** are **Adequacy Decision**, **Standard Contractual Clauses (SCC)**, **Binding Corporate Rules (BCR)**, **EU-US Data Privacy Framework (DPF)**, **Other Safeguard** and **No Safeguard (document justification)**. In **Safeguard Notes** you record the SCC reference, the DPF certification number or the justification. **Retention Reference Point** accepts **From End of Contract**, **From Last Transaction**, **From Withdrawal of Consent**, **Fixed Date** and **Other**.

Filters and related lists

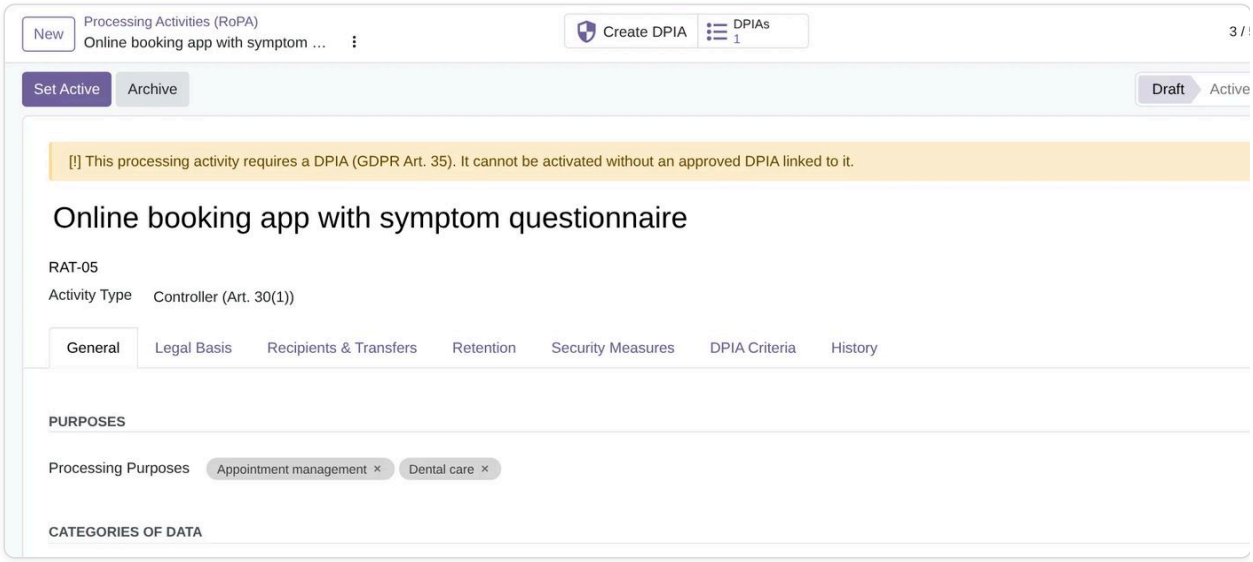
The search has the filters **Active**, **Draft** and **DPIA Required**, and the groupings **By Type** and **By Status**. The menu **GDPR Toolkit › Processing Activities (RoPA) › DPIA Required** opens the activities that need one. The menu **GDPR Toolkit › Retention Management › Retention Schedule** opens those that have a retention period set.

An end-to-end example

The example screens show a dental clinic with five activities. One of them, the patient clinical records, is active and requires a DPIA. Another, the online appointment app with a symptoms questionnaire, is still in **Draft** and also requires one.

1 **Create and fill in**

You click **New**, enter the name and complete the purposes, data subjects, data, legal basis, retention and security measures.



- **Real Odoo 20 screenshot.** The activity in **Draft**, with the notice that it requires a DPIA.

2 **Try to activate it**

You click **Set Active**. While there is no approved DPIA linked, the module blocks it and the error message appears.

3 **Resolve the DPIA**

The button to create the DPIA, at the top of the activity record, opens a new DPIA already linked to it. Once it is approved, you can activate the activity.

4 **Check the history**

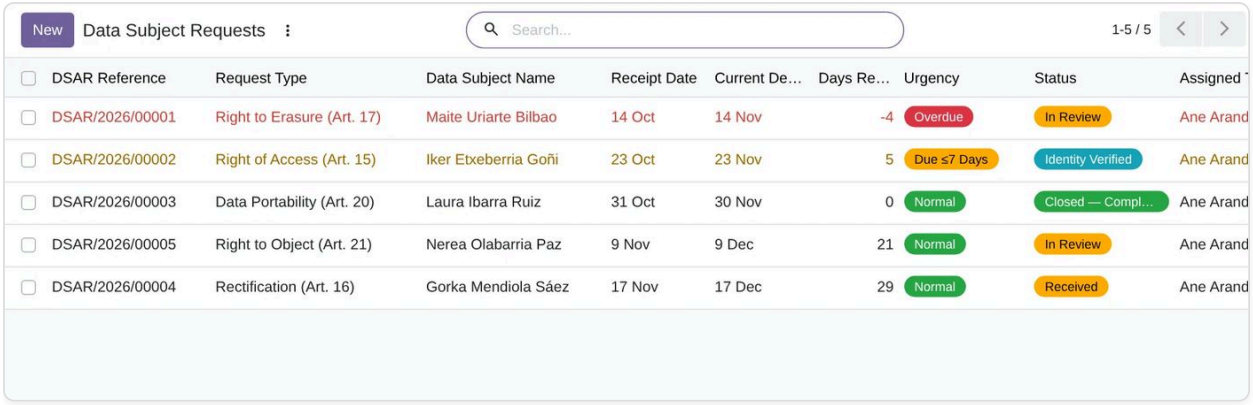
Each change is recorded on the **History** tab.

MODULE GUIDE · GDPR COMPLIANCE

8 Data subject requests and their deadlines

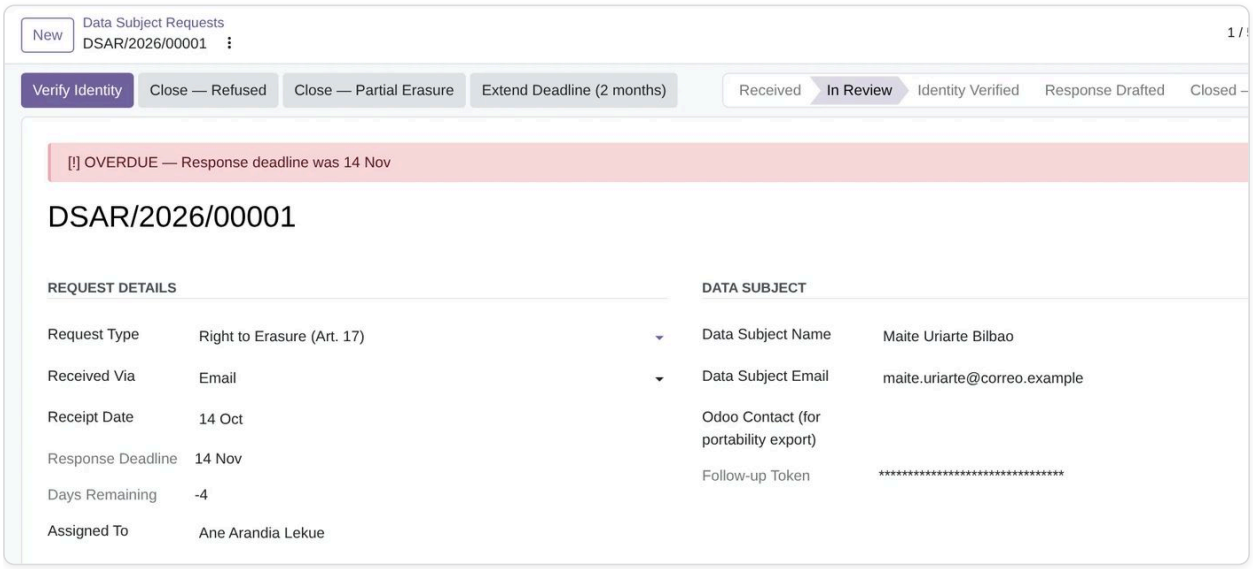
There are six types of request: **Right of Access (Art. 15)**, **Rectification (Art. 16)**, **Right to Erasure (Art. 17)**, **Restriction of Processing (Art. 18)**, **Data Portability (Art. 20)** and **Right to Object (Art. 21)**. The **Received Via** channel can be **Portal Submission**, **Email**,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

The **Response Deadline** is one month from the **Receipt Date** (Art. 12(3) GDPR). If needed, 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, days remaining, urgency and 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 show 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. On the **Response** tab is 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.

Buttons on the record

Start Review	Moves the request from **Received** to **In Review**.
Verify Identity	Moves from **In Review** to **Identity Verified**.
Draft Response	Moves 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 yet extended. It 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: you cannot go back to an earlier one.

Reminders

The **GDPR: DSAR Deadline Reminder** task runs daily and sends an email when an open request has the number of days set in **DSAR Reminder Days Before Deadline** left: to the assigned person; if they have no email, to the GDPR managers; and if there is none either, to the company email. If it reaches nobody, this is noted on the request. The **GDPR: DSAR Overdue Escalation** task runs weekly and sends a 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. You cannot move back to an earlier status. Only GDPR managers can use the request buttons.

The statuses, one by one

- **Received**: the request has just come in. Only **Start Review** is shown.
- **In Review**: someone is looking at it. You can **Verify Identity**, close it as refused, close it with partial erasure (if it is an erasure request) or extend the deadline.
- **Identity Verified**: the identity of the data subject is confirmed. You can **Draft Response**, and from here also close it as refused or extend the deadline.
- **Response Drafted**: the letter is ready. You can **Close — Completed** or close as refused.
- Closed as completed: answered and closed.
- Closed as refused: closed with its legal basis and justification.
- Closed with partial erasure: only for erasures, when something is retained.
- Closed with extended deadline: has no button. Extending the deadline keeps the request in its status and changes the **Current Deadline**.

Rules and Conditions

- The status does not move backwards. If you try, Odoo says «DSAR status cannot be moved backwards. The audit trail must be append-only.»
- When you extend the deadline you must enter the reason. Otherwise you get «Extension reason is required when extending the deadline.»
- To close as refused you need the justification. If it is missing, you get «Refusal justification is required before closing as refused.»
- **Generate Portability Export** only appears on access and portability requests with identity verified. If attempted without verification: "Identity must be verified before generating a portability export."
- **Retention Conflict Check** only exists on erasure requests. On any other type you get «Retention conflict check only applies to erasure requests.»

- A request cannot be deleted: you get «DSAR records cannot be deleted. Archive them instead (GDPR Manager / Admin only).»
- The buttons only work with the GDPR manager group or with an administrator. Otherwise you get «Only GDPR Managers can perform this action.»
- **Load Response Template**, on the **Response** tab, does the same as **Draft Response**: it loads the general template and moves the request to **Response Drafted**, even if it is still in **Received** or **In Review**. Use it once you have already verified the identity.

The erasure check

Retention Conflict Check counts the posted invoices, the employee records (with the Employees app) and the sales orders (with Sales) of the request's contact. It lets you choose to keep or erase each group and, with **Record Decision & Close DSAR**, records your decision in the internal notes and closes the request: completed if everything is to be erased, with partial erasure if something is kept. The module does not delete or anonymise anything: you do that in Odoo.

The record: groups and tabs

Request Details	The type, channel, receipt date, response deadline, days remaining and assigned person.
Data Subject	The data subject's name and email, the Odoo contact for the portability export, and the tracking token.
Extension	**Deadline Extended**, **Extension Reason**, **Extended Deadline (3 months)** and **Extension Notification Due**, which is the same date as the original deadline: one month from receipt.
Identity Verification	The verified identity checkbox, the method, the date and who verified it.
Response	The reply letter and the files from the portability export.
Refusal	The legal basis and the justification for the refusal.
Internal Notes	Notes from the person handling the case.

The basis for refusal can be **Manifestly Unfounded (Art. 12(5)(a))**, **Manifestly Excessive (Art. 12(5)(a))**, **Legal Exemption (Art. 23)** or **Other**. The internal notes and the justification are stored encrypted only if the server has the encryption key. Without it they are stored unencrypted. The configuration shows this under **Encryption Key Configured**.

Reminders and filters

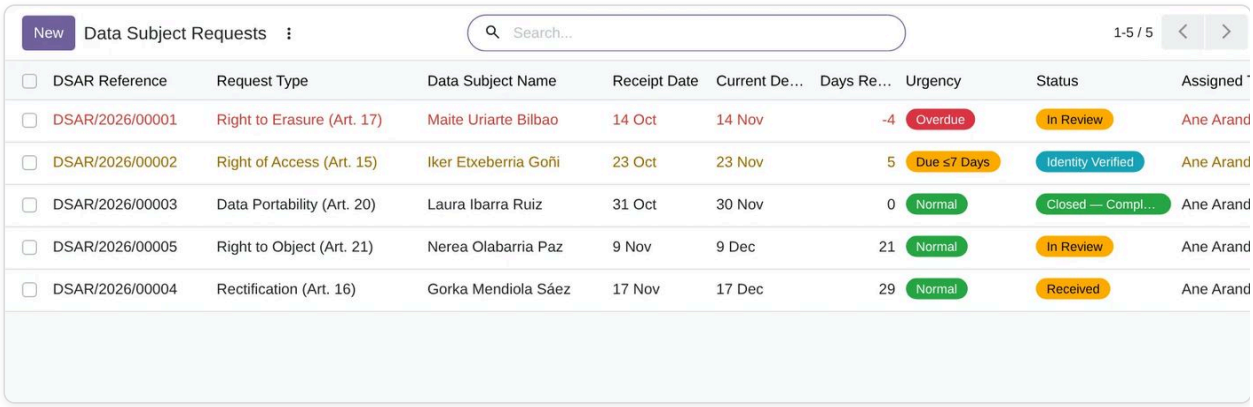
The list filters are **Open**, **Overdue**, the one for requests due in seven days or fewer, **Erasure Requests** and **Access Requests**, with the groupings **By Status** and **By Type**. In **GDPR Toolkit › Reports** you will find the **DSAR History Report**.

The only email to the data subject that is sent automatically is the acknowledgement of receipt for a request submitted through the portal. The reply letter is not sent from the module: you fill it in here and send it yourself through whatever channel you use.

An end-to-end example

1 The request comes in

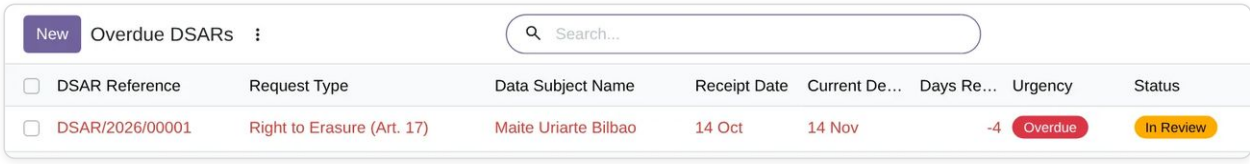
Maite Uriarte Bilbao asks for her data to be erased. Odoo sets the **Response Deadline** one month after the **Receipt Date**.



- **Real Odoo 20 screenshot.** The list with the erasure request, the access request, the portability request and two others.

2 The deadline passes

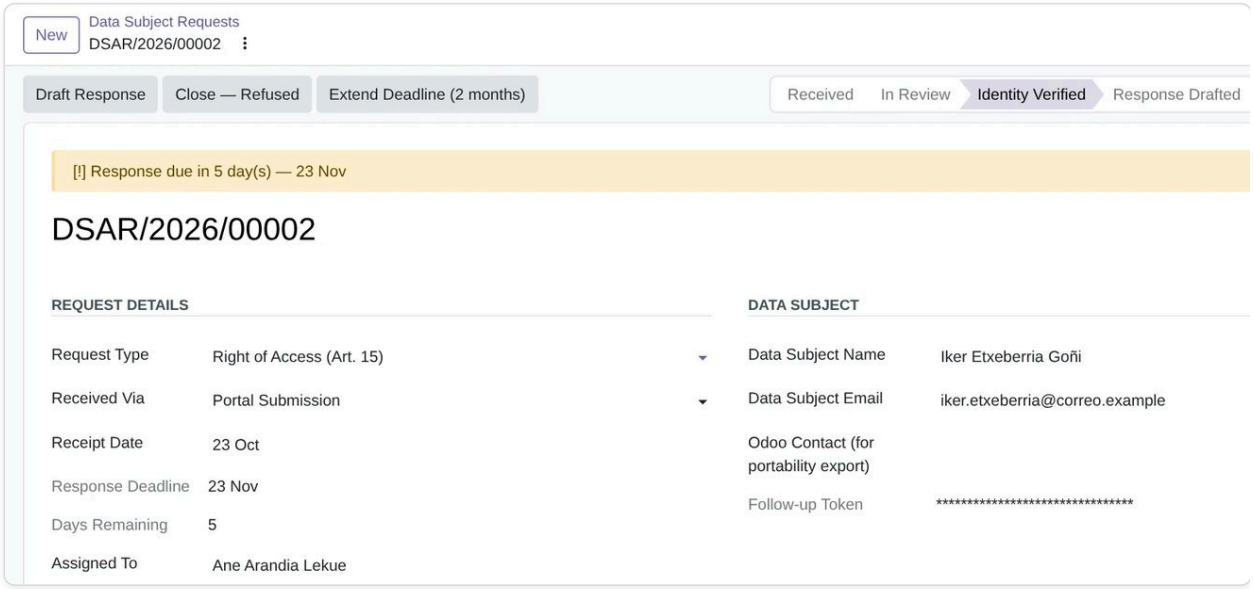
Nobody has closed it and the deadline has already passed: **Days Remaining** shows -4, the record warns that it is overdue, and the request appears under **Overdue**.



- **Real Odoo 20 screenshot.** The list of overdue requests, with a single request.

3 Another request is approaching

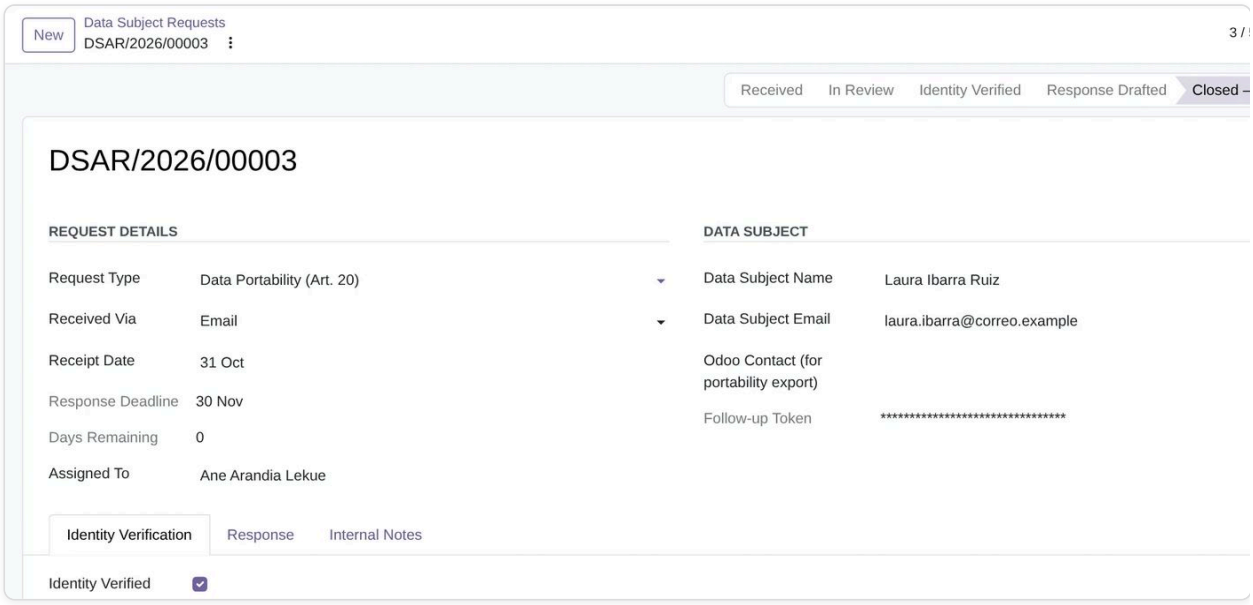
Iker Etxeberria Goñi asked for access to his data. His request has 5 days left and his identity is verified: it appears under **Due This Week**.



- **Real Odoo 20 screenshot.** A request due in 5 days, with verified identity.

4 **It is closed**

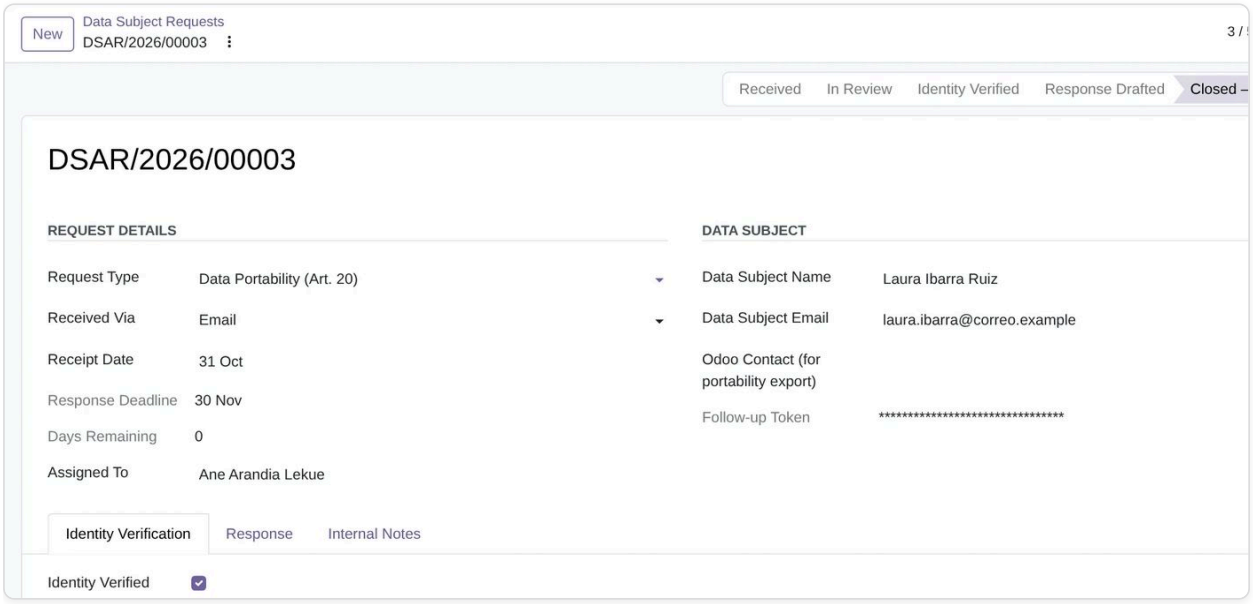
Laura Ibarra Ruiz's portability request has verified identity and is closed as completed.



- **Real Odoo 20 screenshot.** A portability request closed as completed.

MODULE GUIDE · GDPR COMPLIANCE

9 Portability, erasure and the privacy portal



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

Portability export

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

DSAR	The request the export is taken from. Required.
Contact Data (res.partner)	Checked by default. Includes the data on the contact's record.

Order History (sale.order)	Includes the contact's orders. Only available with the Sales app installed.
HR Data (hr.employee)	Includes the employee record. Only available 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, once the export is ready.
Generate Export	Creates the file. It is hidden once the export has already been made.
Close	Closes the wizard.

Erasure conflict check

On an erasure request, **Retention Conflict Check** counts what exists for the contact: published invoices, employee records and sales orders, depending on which apps are 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 defaults to **Erase / Anonymise**.

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

Privacy portal

The portal is at /my/privacy-rights on your Odoo and requires signing in, so the data subject needs a portal account. The module does not add a link under My Account: you give them 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 emailed and a status page with its own link is shown, which displays the type and status without personal data.

> The module does not delete or anonymise data: the erasure check only counts what exists and records your decision. You delete or anonymise in Odoo yourself. It does not send the reply letter either.

What happens in the portability export

The right to portability is the one in Art. 20.1 GDPR: receiving the data the data subject has provided in a structured, commonly used and machine-readable format. That is why the wizard offers JSON or CSV.

The wizard refuses to generate the export in three cases:

- If identity is not verified: "Identity must be verified before generating a portability export."
- If the request has no Odoo contact: «No Odoo contact linked to this DSAR. Please link a res.partner record first.» Link it in the **Odoo Contact (for portability export)** field of the request.
- If the contact's data has already been anonymised, the wizard warns that the data subject's data has already been anonymised, that manual handling is required, and that the DPO must be contacted.

Contact data is ticked. Orders are only included with the Sales app installed: up to 500, from the request's company. HR data is only included with the Employees app installed and the confirmation checkbox ticked: that person's employee record, with their job position, department and private contact details.

When the export finishes

Once generated, the wizard notifies you that the file is ready and attached to the request, and shows the **Export File**. The file is also kept on the **Response** tab of the request.

Request statuses and deadlines

The deadline to respond is one month from receipt of the request and can be extended by a further two months where necessary; the extension and its reasons must be communicated to the data subject within that first month (Art. 12.3). The module does not send that notice: you send it yourself, before the **Extension Notification Due** date.

Extend Deadline (2 months) requires a reason and does not change the request's status: it only changes the **Current Deadline** to the extended date. No button leads to a closed status with an extended deadline.

Erasure check rules

The wizard only opens on erasure requests and looks at the Odoo contact linked to the request; without a contact there is nothing to count. It counts published invoices, employee records and sales orders for that contact. The last two groups depend on the Employees and Sales apps being installed. Each group has its own warning checkbox: **Pending / Recent Invoices Found**, **Active HR Records Found** and **Active Orders Found**. The **Conflict Summary** gives the count as text.

Decisions are made per group: **Invoice Data Decision**, **HR Data Decision**, **Order Data Decision** and **Marketing / Consent Data Decision**. For the first three you choose between **Retain (legal obligation)** and **Erase / Anonymise**; for marketing, between **Retain** and **Erase / Anonymise**.

When the decision is recorded, the request is closed as completed if everything is erased, and as partially erased if any group is retained. The module only logs the decision in the internal notes. The wizard's summary is in English and cites retention periods from Spanish law: check them with your DPO, as they do not apply in every country.

The portal and its limits

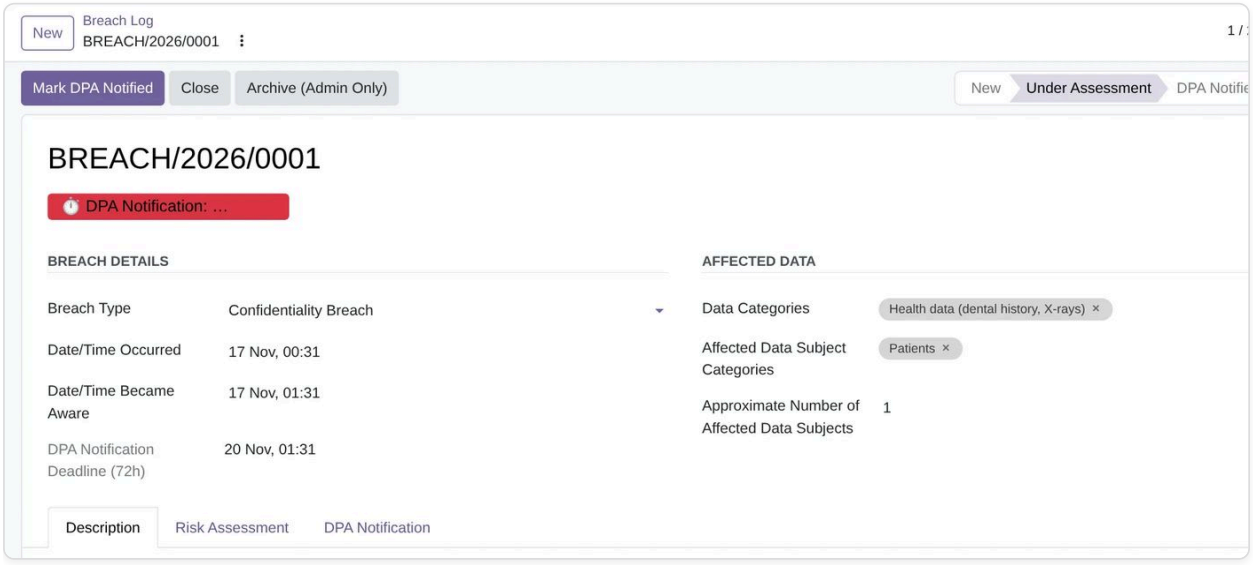
The portal sets two limits per person. With 3 requests in one day it will not accept more until the next day. With 5 in seven days it stops accepting them, adds a review flag to the contact's notes and asks them to get in touch with your company. Deciding whether a request is manifestly unfounded or excessive is the controller's job (Art. 12.5).

Anyone who opens the status link sees only the type and status of their request, without personal data. The only email sent automatically to the data subject is the acknowledgement of receipt for a request submitted through the portal; you write and send the reply letter yourself.

An end-to-end example

Laura Ibarra Ruiz requested portability of her data. Her request has verified identity and the Odoo contact is linked. You open the wizard, leave contact data ticked, choose JSON and click **Generate Export**: the file appears under **Export File** and is attached to the request. You then send her the reply through your usual channel and close the request as completed.

10 The breach log and the 72 hours



- **Real Odoo 20 screenshot.** A breach under assessment, with 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 assigned by Odoo when it is created 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 happened.
Date/Time Became Aware	Required. The notification deadline starts counting from this moment.
DPA Notification Deadline (72h)	Odoo calculates this from the date and time the organisation became aware.
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

Art. 33.1 GDPR requires notifying the breach 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 remains, in hours and minutes; once the deadline has passed it says "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 alert 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

Using 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. High or critical risk marks **Art. 34 Data Subject Notification Required**. The final decision is taken by the controller or its DPO, and you can record it under **DPO Final Art. 34 Determination**.

Statuses and buttons

Start Assessment	Moves the breach from **New** to **Under Assessment**.
Mark DPA Notified	Only visible in **Under Assessment**. Changes the status to **DPA Notified** and records the date and time. The module does not notify anyone: you fill in the method, the reference number and the evidence yourself on the **DPA Notification** tab.
Mark Data Subjects Notified	Only visible in **DPA Notified** and when the Art. 34 notification is required. Moves the breach to **Data Subjects Notified** and records the date. You carry out the notification outside Odoo; the evidence goes on the **Art. 34 Notification** tab.
Close	Hidden in **New** and **Closed**. Before closing, fill in the **Post-Breach Review** tab: root cause, corrective actions, preventive measures, who approves and the date.
Archive (Admin Only)	Only visible 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 awareness was established.
2. **Assess**
   Click **Start Assessment** and score impact and likelihood.
3. **Notify yourself and record**
   If applicable, notify the authority yourself and click **Mark DPA Notified**.
4. **Communicate and close**
   If it is mandatory, notify 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.»

The statuses, one by one

New	The breach has just been logged. Only the assessment can be started.
Under Assessment	Impact and likelihood are scored. From here it is marked as notified to the authority.
DPA Notified	Someone confirms that the authority was notified outside Odoo. If the risk level triggers the Art. 34 communication, it can be marked as notified to the data subjects.

Data Subjects Notified	It is recorded that the data subjects were notified.
Closed	The breach is finished and can no longer be closed again.

Rules and Conditions

- **Start Assessment** only appears in **New**.
- **Mark DPA Notified** only appears in **Under Assessment**.
- **Mark Data Subjects Notified** only appears in **DPA Notified** and only if the Art. 34 communication is mandatory.
- **Close** does not appear in **New** or **Closed**.
- The workflow buttons are for the module's managers group; **Archive (Admin Only)** is only for Odoo administrators.
- If a user without that permission tries to archive, you get «Only Odoo Administrators can archive breach records.»
- The archive wizard requires the **Archive Reason**; without it you get «Archive reason is required.»
- Art. 33.1 requires notification within 72 hours where feasible. If notification does not take place within that deadline, it must be accompanied by the reasons for the delay.

The module only changes the status and records the date. It does not notify the authority or communicate anything to the affected individuals: you do that, and here you record what you did.

The description and consequences are stored encrypted only if the server has the encryption key. Without it they are stored unencrypted, and the configuration shows this under **Encryption Key Configured**.

Fields and tabs of the record

Breach Details	Type, when it occurred, when it was discovered and the deadline for notifying the authority.
Affected Data	**Categories of Data**, **Affected Data Subject Categories** and **Approximate Number of Affected Data Subjects**.
Description	Description, consequences and **Measures Taken / Proposed**.
Risk Assessment	Impact, likelihood, score and risk level.
DPA Notification	**DPA Notification Date/Time**, **Notification Method**, **DPA Reference Number** and attachments.
Art. 34 Notification	If it was sent, when, and the attachments.
Post-Breach Review	Root cause, corrective actions, preventive measures, who approves and the date.

In the list, the filters **High/Critical Risk** and **DPA Notification Pending** help you see what is missing. The **Active Incidents** menu opens the breaches that are not closed.

An end-to-end example

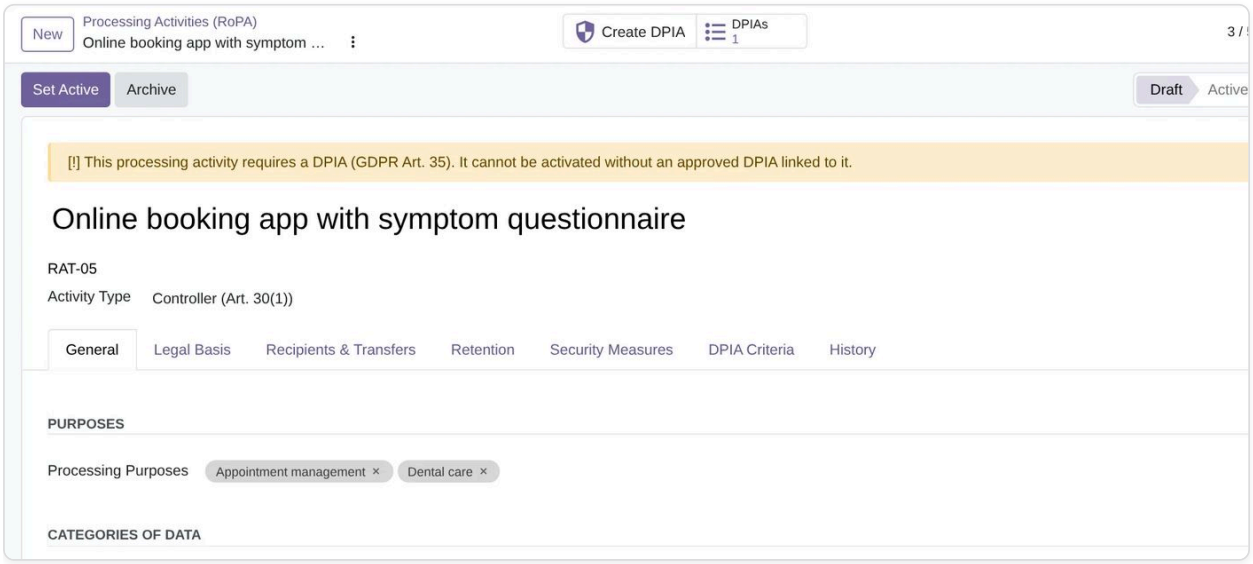
The first breach in the screens is a **Confidentiality Breach**: an X-ray sent by post to the wrong patient. It was discovered one hour after it occurred, Odoo set the deadline 72 hours later and, when it was opened, about 42 hours remained. It affects patient health data, has risk level **Medium**, is **Under Assessment** and shows the

button **Mark DPA Notified**. The second, an **Availability Breach** due to the theft of the reception laptop, with the disk encrypted, has level **Low** and is **Closed**: on a closed breach only the **Archive (Admin Only)** button remains.

MODULE GUIDE · GDPR COMPLIANCE

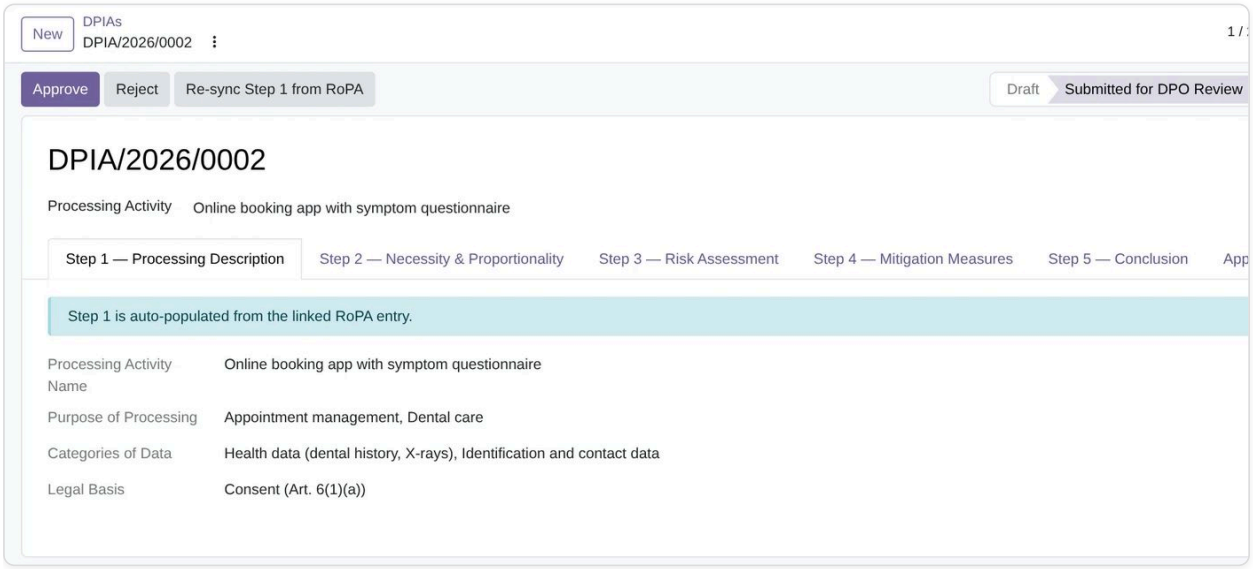
11 Data protection impact assessments (DPIAs)

On the **DPIA Criteria** tab of each processing activity there are nine checkboxes, one per criterion of the WP248 rev.01 guidelines. With two or more ticked, or with the manual flag, the activity is shown with **DPIA Required**. This is a general rule of 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 notice that it requires a DPIA.

The assessment is opened from the activity form or from **GDPR Toolkit › DPIA › All DPIAs**. Odoo assigns the reference automatically 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

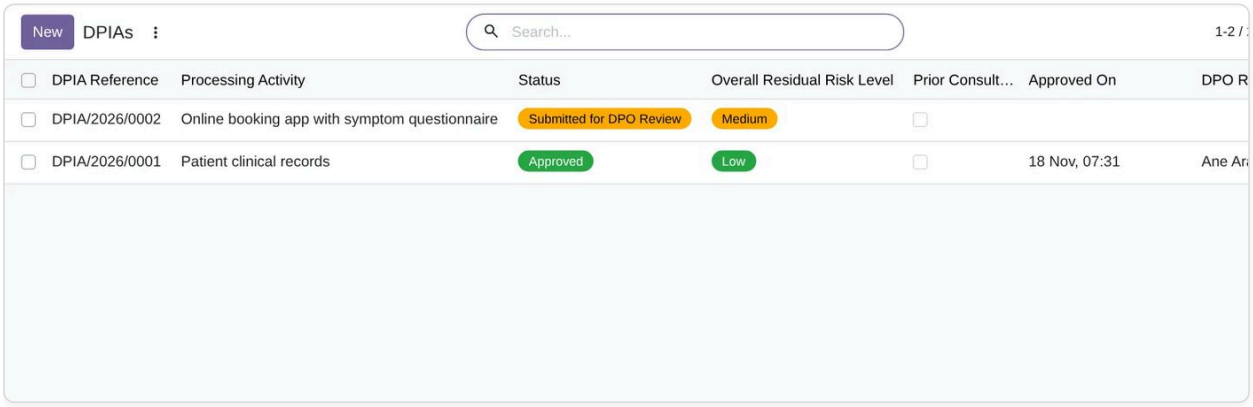
- Step 1, the description of the processing: the name, purpose, categories of data and the Art. 6 legal basis are filled in automatically from the processing activity in the RoPA.
- Step 2, necessity and proportionality: purpose limitation, data minimisation, justification of the retention period and 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. From each pair a score and a level are derived: up to 4 low, up to 9 medium, up to 19 high and from 20 critical. This matrix belongs to the module, not to the GDPR or the European Data Protection Board guidelines. With high or critical residual risk, **Prior Consultation Required (Art. 36)** is ticked automatically. If you submit the prior consultation, record what you did here under **Prior Consultation Submitted** and **Prior Consultation Notes**. The module does not submit it to the authority.

Buttons on the record

Submit for DPO Review	Moves the DPIA from **Draft** to **Submitted for DPO Review**. Only appears in **Draft**.
Approve	Approves the DPIA. Only appears in **Submitted for DPO Review**.
Reject	Rejects the DPIA. Only appears in **Submitted for DPO Review** and requires DPO comments.
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 processing activity in the RoPA.

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 their overall residual risk level.

> Only GDPR managers can submit, approve and reject. 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 form warns about this on screen.

DPIA statuses

STATUS	WHAT IT MEANS
Draft	This is the starting status: the steps are filled in and **Submit for DPO Review** is shown.
Submitted for DPO Review	The DPIA awaits the DPO's decision. In this status **Approve** and **Reject** are shown.
Approved	The DPO has approved it and its date is recorded in **Approved On**.
Rejected	The DPO has rejected it with their comments. The **Reset to Draft** button returns it to **Draft**.

When it will not let you

- Only GDPR managers can submit, approve and reject. If you are not one, you get the message «Only GDPR Managers can submit a DPIA for review.», «Only GDPR Managers (acting as DPO) can approve a DPIA.» or «Only GDPR Managers (acting as DPO) can reject a DPIA.», depending on the button.
- Rejecting without writing anything in **DPO Comments** gives the message "DPO comments are required when rejecting a DPIA."
- **Reset to Draft** only appears when the DPIA is **Rejected**.

Fields and tabs of the record

DPIA Reference	Odoo sets it when the record is created and it cannot be edited.
Processing Activity	The RoPA processing activity the DPIA belongs to. It is required.
Overall Residual Risk Level	Odoo calculates it: it is the highest of the residual risks in the list.
Submitted By and **Submitted On**	Who submitted the DPIA for review and when.
DPO Reviewer and **DPO Review Date**	Who reviewed it and when.
DPO Comments	Text of the review. Required for rejection.
Prior Consultation Submitted and **Prior Consultation Notes**	What you record if you have submitted the Art. 36 prior consultation. The module does not submit it.

The view has six tabs: the five steps and **Approval**. Each step holds its texts, and **Re-sync Step 1 from RoPA** updates step 1 if you change something in the activity. The filters are **Awaiting DPO Review**, **Approved** and **High/Critical Residual Risk**, grouped by **By Status** and **By Risk Level**.

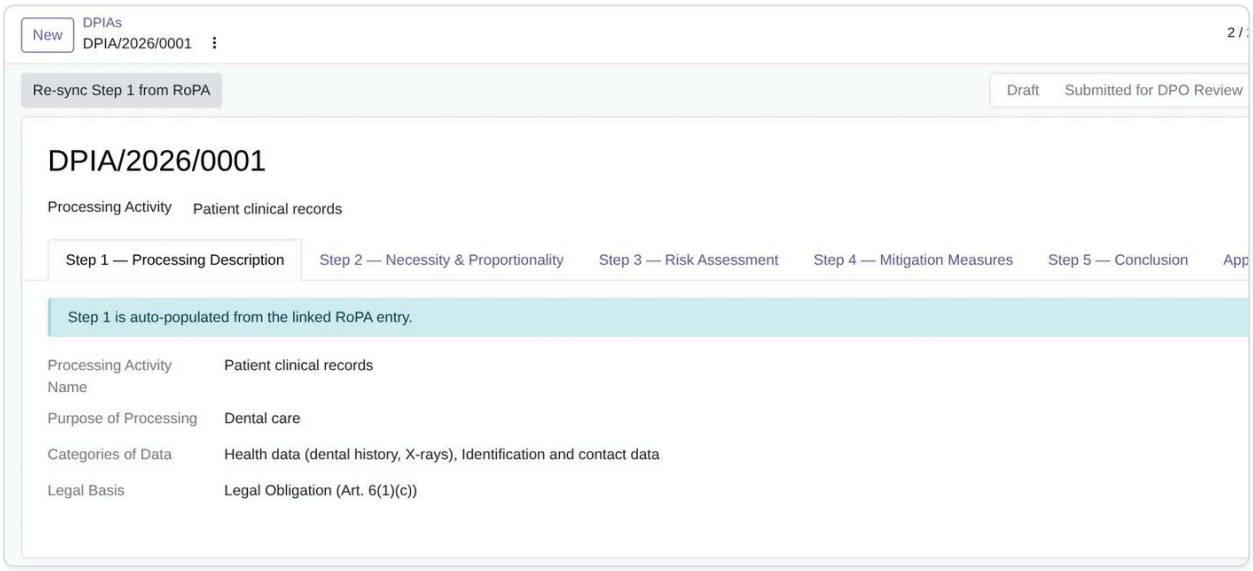
How risk is calculated

Each risk scores its impact from insignificant (1) to catastrophic (5) and its likelihood from very low (1) to very high (5). They are multiplied to give a score from 1 to 25. Up to 4 is **Low**, up to 9 is **Medium**, up to 19 is **High** and from 20 is **Critical**. After the measures it is repeated with the residual impact and residual likelihood. These cut-offs belong to the module. With high or critical residual risk, the Art. 36.1 prior consultation is flagged, which

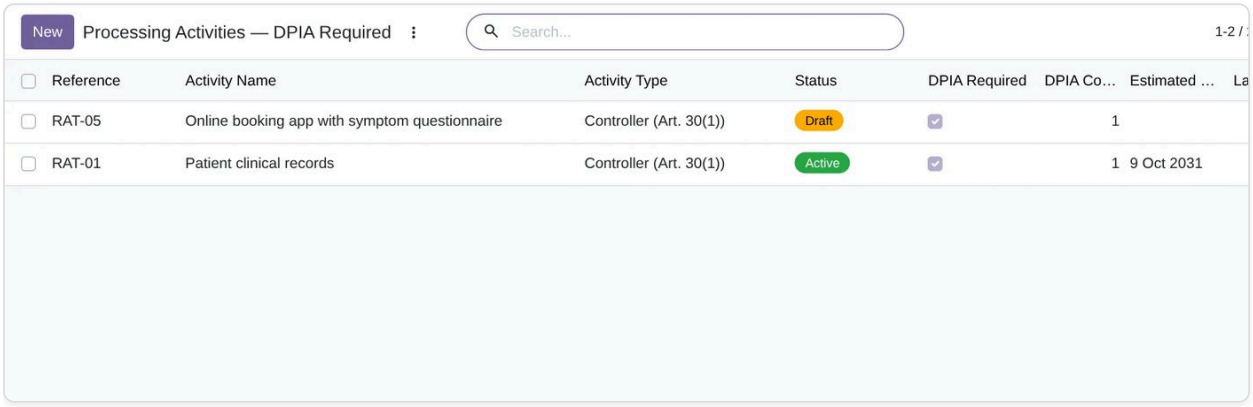
requires consulting the authority before processing when the assessment shows it would entail a high risk if no measures were taken to mitigate it.

An end-to-end example

In the example screens, RoPA activity RAT-05, the online appointment app with a symptom questionnaire, is in **Draft** and shows **DPIA Required**. Its form warns that it cannot be activated without an approved DPIA. From there the DPIA is created, which comes out with number DPIA/2026/0002, and step 1 already carries the purpose, categories of data and legal basis of the activity. After filling in the remaining steps it is submitted for review and in the list it is in **Submitted for DPO Review** with residual risk **Medium**. The DPO will see it under **Awaiting DPO Review** and will approve or reject it with their comments. Until it is approved, the activity stays in **Draft**.



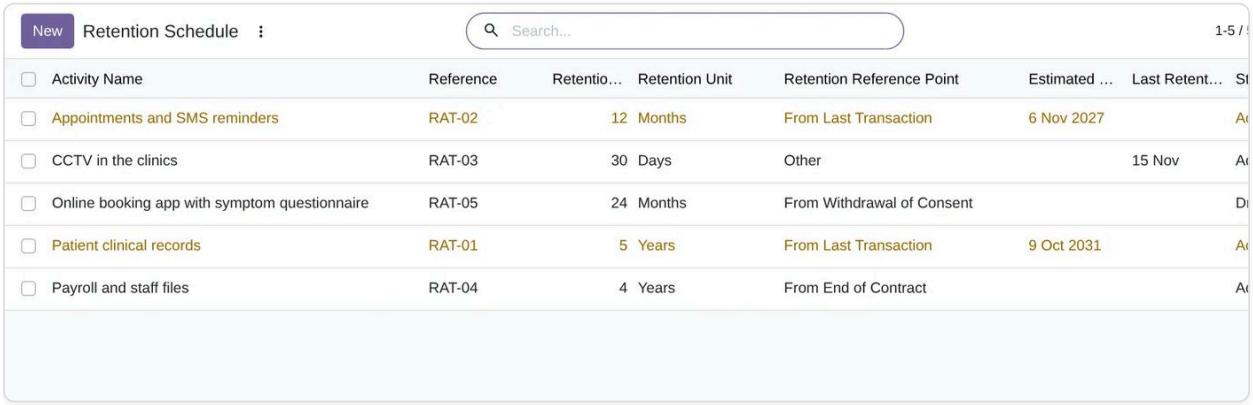
- **Real Odoo 20 screenshot.** The DPIA for patient medical records, with the status **Approved**.



- **Real Odoo 20 screenshot.** The activities with **DPIA Required** and their DPIA number.

> What this module does not do: it does not submit the prior consultation to the authority nor decide for you whether the assessment is acceptable. The final decision rests with the controller or its DPO, and this is not legal advice.

12 The Retention Schedule and Its Reviews



- **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, in **GDPR Toolkit › Processing Activities (RoPA) › All Activities**. Odoo calculates the **Estimated Retention End Date** only when the count start is **Fixed Date** or **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 gets 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 days set in **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 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 register of activities needs reviewing.

Where a Review Is Recorded

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

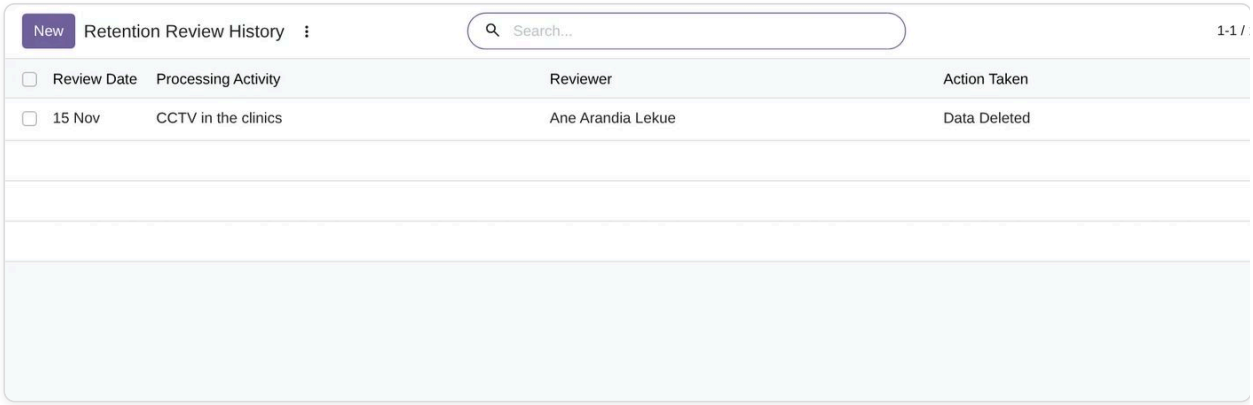
Processing Activity	The activity you are reviewing. Required.
Review Date	Comes pre-filled with today's date. Required.
Reviewer	Comes pre-filled with your user. Required.
Action Taken	What you did after the review. Required. It has four options: **Data Deleted**, **Data Anonymised**, **Retention Extended**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

The review record has no buttons or states of its own. The options in **Action Taken** are what you record, not a state 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 a 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 the retention

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

5 Save

On saving, the **Last Retention Review** of the activity 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 that, change the period or its reference date in the **Retention** tab.

What a Review Stores

Each review links a processing activity with the date you reviewed it, who did it and what you decided. The company is copied automatically from the activity. It only stores what you decided and did: the module does not delete or change any data.

The Four Possible Actions

Data Deleted	You record that, after the review, the data was deleted. You carry out the deletion outside the module.
Data Anonymised	You record that the data was anonymised. You carry out the anonymisation outside the module.

Retention Extended	You decide to keep the data for longer. It requires a justification and a new end date, which is stored on the review: the estimated date of the activity does not change.
The Reviewed With No Action Option	You reviewed the activity and nothing needs doing. It is the fourth option in the **Action Taken** list.

Rules and Conditions

- With **Retention Extended** and no **Extension Justification**, Odoo does not save and shows «Extension justification is required when extending retention.».
- With **Retention Extended** and no **New Retention End Date**, Odoo does not save and shows «New retention end date is required when extending retention.».
- With the other three actions, those two fields are not required.
- **Processing Activity**, **Review Date**, **Reviewer** and **Action Taken** are required.

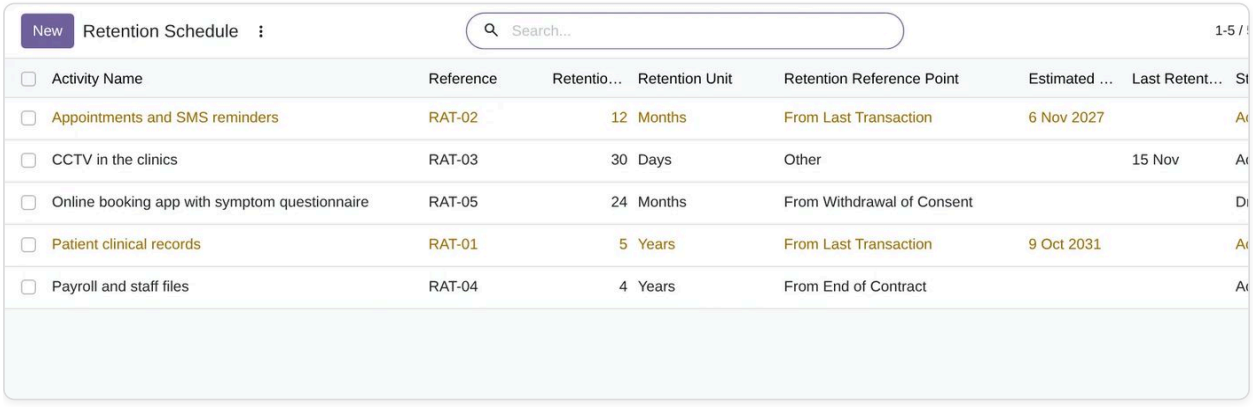
Each review you save updates the **Last Retention Review** on the activity with the **Review Date** of that review. It is shown in the columns of the **Retention Schedule** and in the list of **Processing Activities (RoPA)**.

The Alerts

The task **GDPR: Retention Expiry Check** runs every day. It warns about active activities whose estimated end date falls within the days set in **Retention Advance Warning (days)** (30 by default) and that have not been reviewed in the last 30 days: it leaves a warning activity on the record and sends an email. An activity without an estimated date gets no alert. The task **GDPR: Annual RoPA Review Reminder** reminds you once a year that the register of activities needs reviewing.

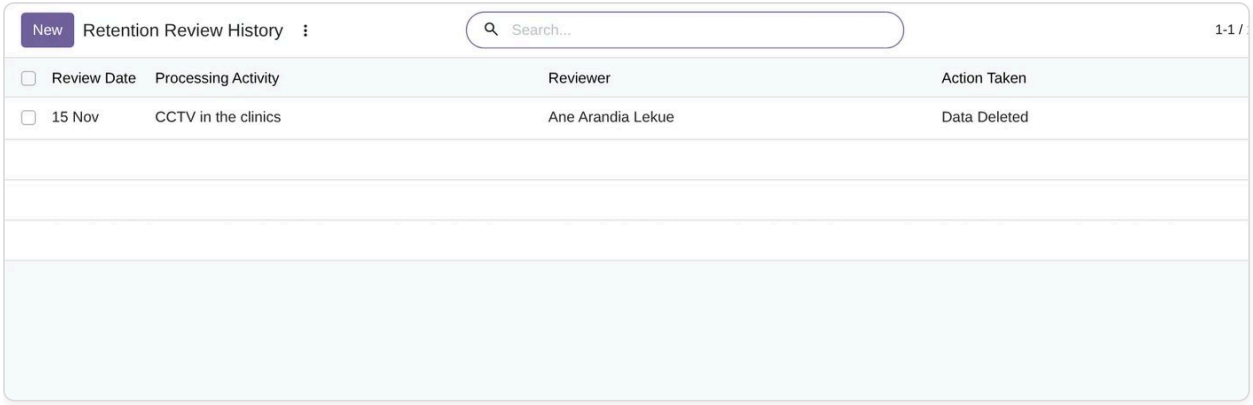
An end-to-end example

The **Retention Schedule** on the screens has five activities. Patient medical records are kept for 5 years from the last transaction and appointments and SMS reminders for 12 months: both have an estimated end date. The clinics' CCTV (30 days, with count start **Other**), payroll (4 years from the end of the contract) and the online booking app (24 months from the withdrawal of consent) do not, because their count start is not a date Odoo knows.



- **Real Odoo 20 screenshot.** The **Retention Schedule** with the five activities and their estimated dates.

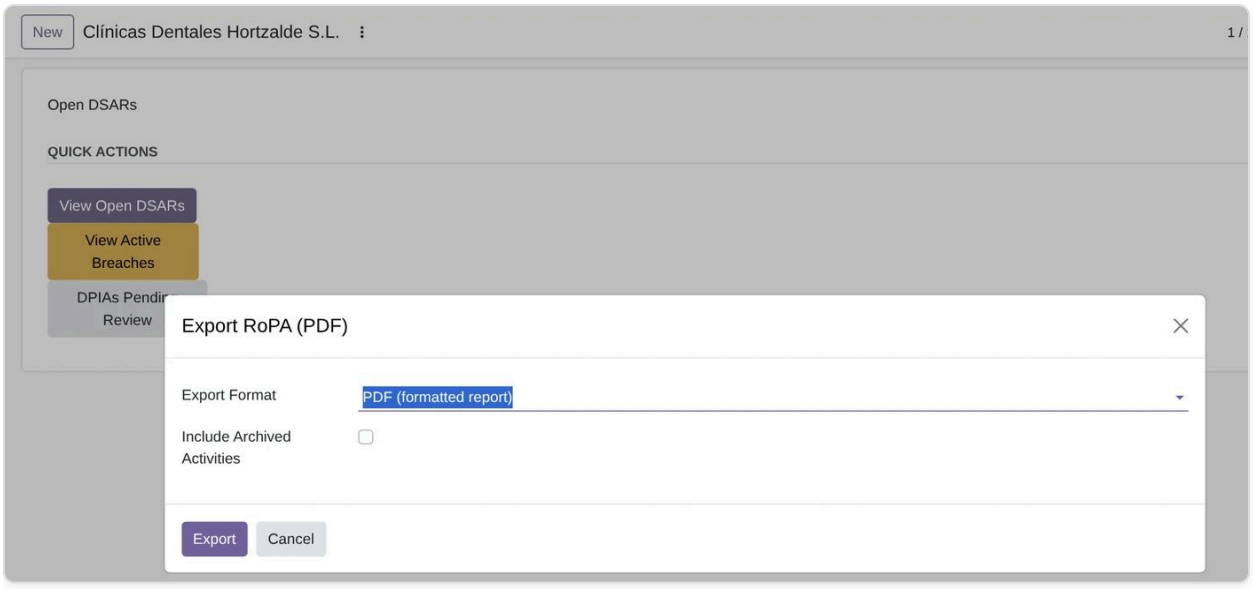
In the **Retention Review History** there is a review of the clinics' CCTV, done by Ane Arandia Lekue, with the action **Data Deleted**. It has no new end date because that action does not require one. In the schedule, that date becomes the activity's last review.



- **Real Odoo 20 screenshot.** The **Retention Review History** with the CCTV review.

MODULE GUIDE · GDPR COMPLIANCE

13 Reports, Exports and the Audit Log



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

Exporting the RoPA

1. **Open 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**

   In **Export Format** you choose **PDF (formatted report)** or **Excel (.xlsx)**. The format of the menu you came from is pre-selected.

3. **Decide on archived records**

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

4. **Click Export**

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

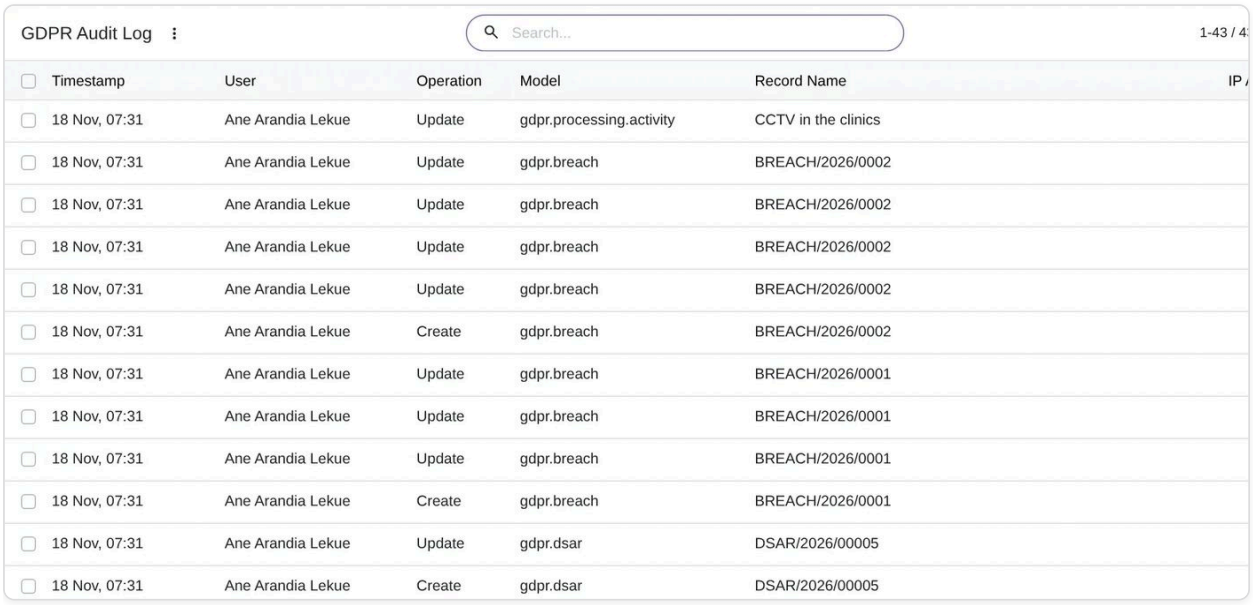
The Excel file has one row per activity. The column headers are shown in English in all languages.

- 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, to filter, group or export them. Each request, breach, DPIA and activity can be printed to PDF from its record.

Audit trail



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

Each entry stores who made the change, when, on which record and from which IP address. The change summary masks fields containing personal data. The operations recorded 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 the entries by user.
By Model	Groups the 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.».

Options in the Export Wizard

PDF (formatted report)	Formatted report, ready to read or print. Pre-selected if you enter via **Export RoPA (PDF)**.
Excel (.xlsx)	Spreadsheet with one row per activity, for you to filter and sort yourself.
Include Archived Activities	Checkbox unticked at the start. When ticked, archived activities are included in the report.

Both export menus lead to the same wizard.

When Export Is Not Allowed

- With no processing activities in your company, the wizard warns you with «No processing activities found for this company.» and generates nothing.
- Without the Excel library on the server, the Excel export fails with «openpyxl is not installed. Please install it via pip to use Excel export.».

Audit Log Operations

OPERATION	WHAT IT RECORDS
Create	A record creation.
Update	A change to an existing record.
Archive	The archiving of a record.
Export	The export of the RoPA to Excel or the portability export.
Portal Submission	A request submitted through the privacy portal.

Record fields

Timestamp	When it happened. It is filled in automatically.
User	Who did it.
Operation	One of the five listed above.
Model and **Record Name**	What type of record was touched and what it is called.
Record ID	Numeric identifier of the record touched.
The IP address	Where it was done from.
Change Summary	Names of the fields modified and their values. Fields containing personal data are masked.

Company	The company the entry belongs to.

What you cannot do

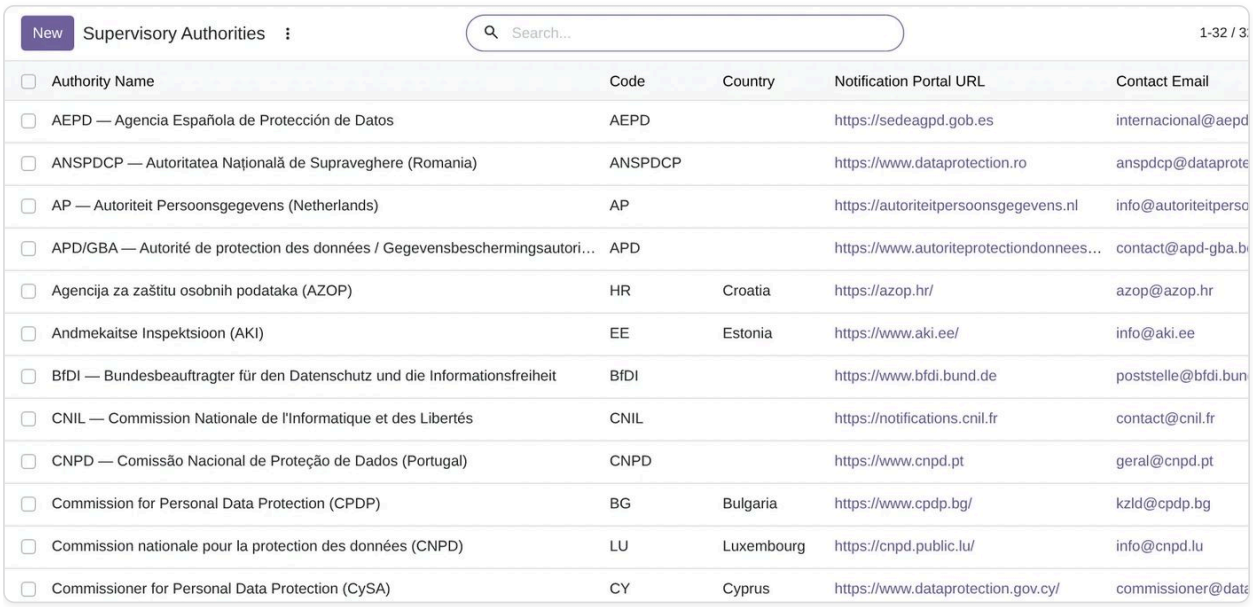
Entries can only be created. Any attempt to change or delete them, whichever user makes it, ends in an error message. The message cites Art. 5(2) of the GDPR, the accountability principle, as the reason they are kept.

An end-to-end example

You go to **GDPR Toolkit › Reports › Export RoPA (Excel)**, leave **Include Archived Activities** unticked and press **Export**. You receive the file with one row per activity. Then you open **GDPR Toolkit › Configuration › Audit Log** and filter by **Exports**: there you see the export with your user and the timestamp. The same list shows the creations and changes to your activities and breaches, with the name of each record.

MODULE GUIDE · GDPR COMPLIANCE

14 Supervisory Authorities and Legal Bases



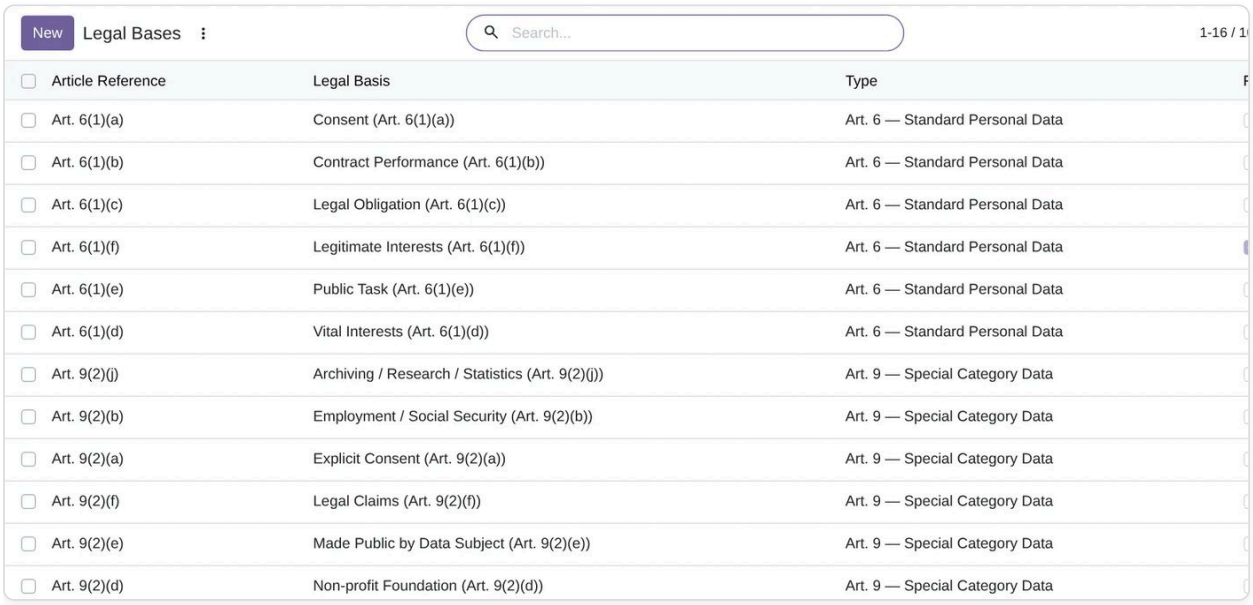
- **Real Odoo 20 screenshot.** The **Supervisory Authorities** list with its 32 records.

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	The authority's abbreviation, for example AEPD, CNIL or BfDI.
Notification Portal URL	Address of the portal where notifications are made.
Contact Email	The authority's contact email.
Breach Notification Form URL	Address of the form for notifying a breach.

Active	Tick box indicating whether the authority is in use. It is ticked by default.

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



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

The 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	Indicates 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	Tick box marking the bases that require that balancing test.

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

What each list contains and how it is identified

Each authority has three pieces of data that identify it: its **Authority Name**, its **Country** and its **Code**. The code is free text and the field's own help text gives AEPD, CNIL and BfDI as examples. The other three data points (the notification portal, the contact email and the breach form) are addresses and an email that you can consult from the record.

Active or not active

Each authority carries the **Active** tick box, ticked by default. It is the only thing in the record that indicates whether an authority is considered in use. Legal bases also have an active field, but it does not appear on any screen in the module, so you cannot see or change it from the interface.

The two types of legal basis

TYPE	WHAT IT COVERS
Article 6 basis	The bases for processing ordinary personal data.
Article 9 basis	The bases for processing special categories of data.

The balancing test

The **Requires Legitimate Interests Balancing Test** tick box marks the bases that call for that balancing test. It appears in the list, for example, as **Legitimate Interests (Art. 6(1)(f))**, with the article reference in its column. The description of each basis exists in the model, but it does not appear on any screen.

Rules and limits

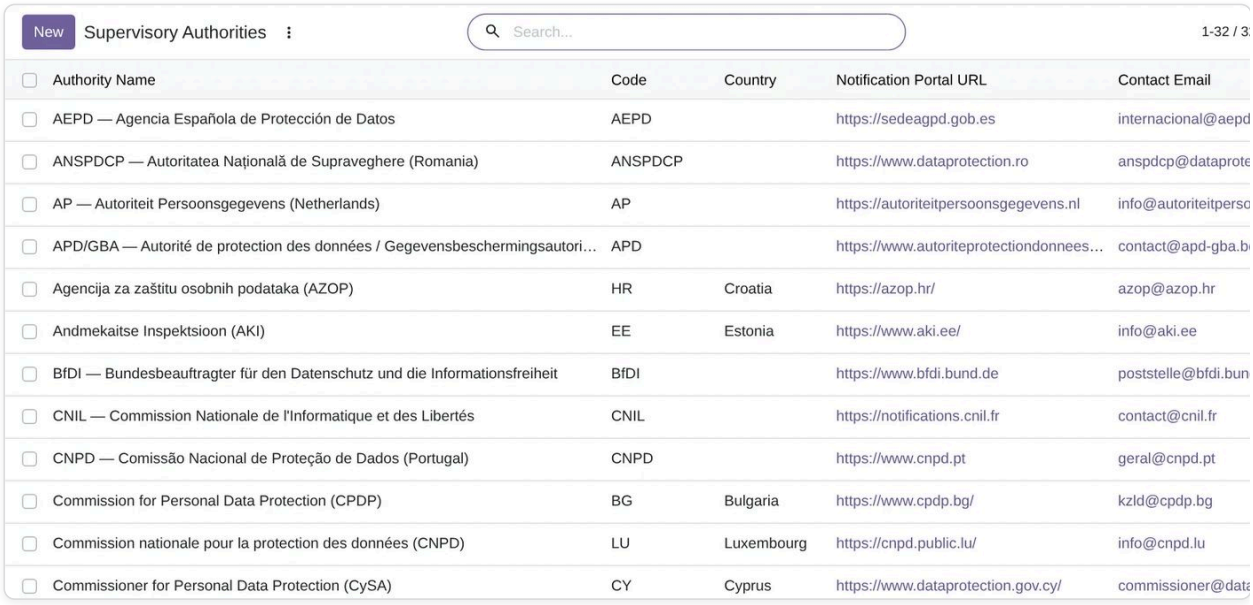
- The authority name and the legal basis name are required.
- The type of basis is required and, if you do not change it, it defaults to an Article 6 basis.
- The lists are loaded at installation. The module does not reload or update them on its own.
- The module does not notify anything to the authority. The portal and the form are addresses for you to notify from outside and record here what you did.

An end-to-end example

1

Open the authorities

Go to **GDPR Toolkit › Configuration › Supervisory Authorities**. The list shows 32 records, with the AEPD among them: its code is AEPD.

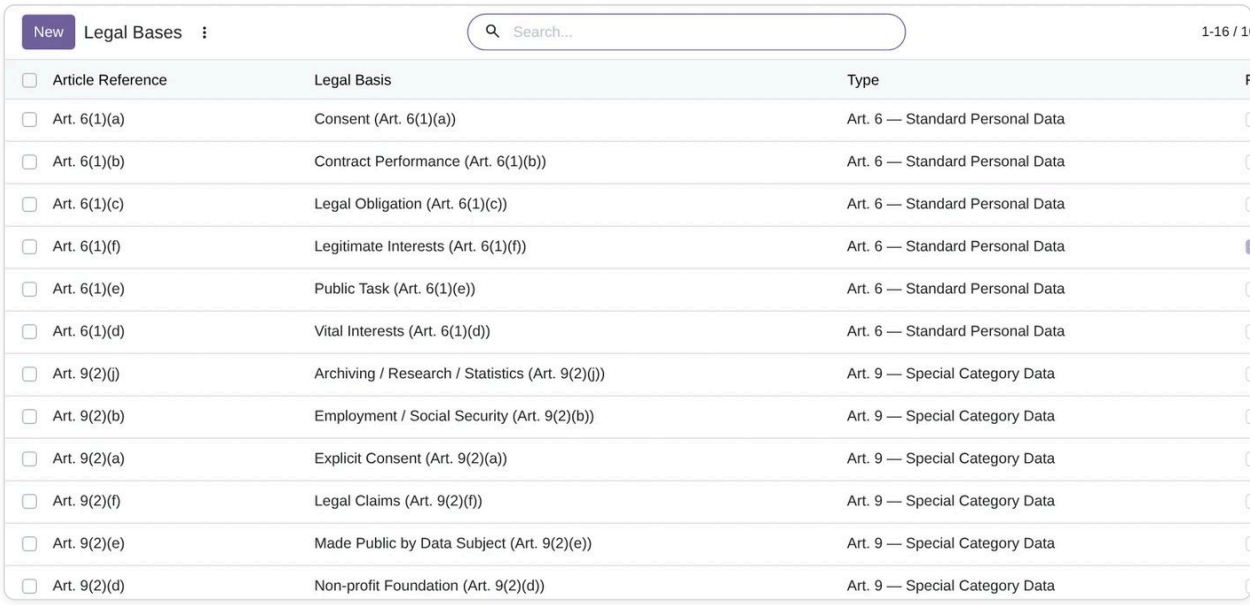


- **Real Odoo 20 screenshot.** The list shows the name, code, country, portal and email of each authority.

2

Open the legal bases

Go to **GDPR Toolkit › Configuration › Legal Bases**. The list shows 16 records. Look for **Consent (Art. 6(1)(a))** and **Legitimate Interests (Art. 6(1)(f))**, which has the balancing test tick box set.



- **Real Odoo 20 screenshot.** The list shows the article reference, the legal basis and its type.

MODULE GUIDE · GDPR COMPLIANCE

15 What goes to FlexigoTech Cloud and what comes back

DATA	DIRECTION	WHEN
The identification of the base: its identifier, its address and its public code, the Odoo version and the names of its modules	From your Odoo to FlexigoTech Cloud	When connecting the base to the service
The acceptance of the terms and of the data processing agreement, with the email of whoever accepts	From your Odoo to FlexigoTech Cloud	When you press **Connect and start the trial** after ticking that you have read the list
The request for the service's permission for the module	From your Odoo to FlexigoTech Cloud	The modules ask on their own; **Check now** asks at that moment
The requests for the monitoring alerts	From your Odoo to FlexigoTech Cloud	Every 6 hours, when the base requests new alerts
The monitoring alerts	From FlexigoTech Cloud to your Odoo	In the next request after a source changes

What the service monitors

FlexigoTech Cloud checks six official sources every day and alerts when one changes. These are the European Union acts amending the GDPR, published in the Publications Office; procedure 2025/0360(COD), known as the digital omnibus, in the European Parliament's Legislative Observatory; the consolidated LOPDGDD, in the BOE; the page of European Commission adequacy decisions; and the guidance and tools pages of the AEPD.

Alerts appear under **Settings › FlexigoTech Cloud** and also arrive in a daily email.

What stays in your Odoo

The record of processing activities, data subject requests, breaches, impact assessments and the audit log stay in your database. The module does not send any of that to FlexigoTech or to any external service. The connection screen says so: your customers, orders, invoices and products are not sent to FlexigoTech Cloud by this connection.

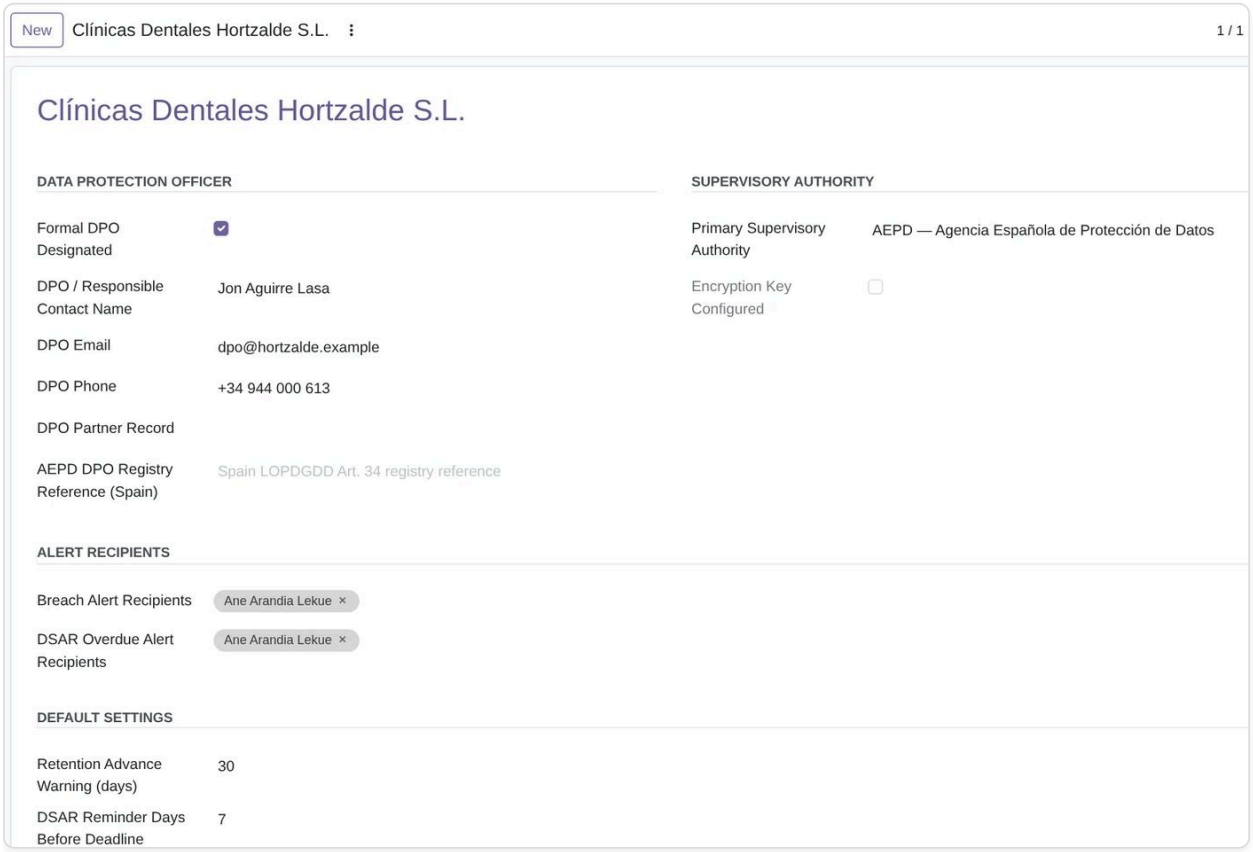
MODULE GUIDE · GDPR COMPLIANCE

16 What happens automatically

TASK	FREQUENCY	WHAT IT DOES
GDPR: DSAR Deadline Reminder	Every day	Sends an email when an open request has reached the number of days set in **DSAR Reminder Days Before Deadline**: to the assigned person or, if they have no email, to the GDPR managers.
GDPR: Breach Countdown Alert	Every hour	In the last 6 hours of the deadline for an open breach that is not marked as notified, it sends an email to the **Breach Alert Recipients** or to the GDPR managers.
GDPR: Retention Expiry Check	Every day	Leaves a reminder activity and sends an email for each active activity whose retention end is approaching and that has not been reviewed in the last 30 days.
GDPR: DSAR Overdue Escalation	Every week	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	Sends an email reminding you that the record of processing activities needs reviewing.

Alerts are sent by email to users with an email address, in each user's language. Frequencies are changed in **Settings › Technical › Automation › Scheduled Actions**, with developer mode activated.

17 Module options and their defaults



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

OPTION	DEFAULT	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 formal DPO has been designated.
AEPD DPO Registry Reference (Spain)	Empty	Stores the reference under which the DPO is registered with the AEPD.
Primary Supervisory Authority	Empty	Chosen 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 requests. If you choose none, the **GDPR Toolkit / Manager** group of the company receives them.
Retention Advance Warning (days)	30	Days in advance of the end of the retention period at which a warning is sent.
DSAR Reminder Days Before Deadline	7	Days before a request's deadline when the reminder is sent.
Art. 30(5) SME Exception Note Acknowledged	Off	You record that you have read the note on the Art. 30(5) exception for companies with fewer than 250 employees.

OPTION	DEFAULT	WHAT IT DOES
Encryption Key Configured	Per server	Read only. Indicates whether the server has an encryption key configured.

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

Legal deadlines (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) and the risk matrix (impact by likelihood) cannot be adjusted, as they belong to the module.

What is done by hand

SCREEN	BUTTONS
RoPA activity	**Set Active** moves the activity from draft to active; it cannot be done if it requires a DPIA and no approved linked one exists. **Archive** archives it. **Set to Draft** returns it to draft. The button to create the DPIA opens an assessment for that activity.
Data subject request	**Verify Identity** records the verification. **Draft Response** moves the request to response drafted. **Extend Deadline (2 months)** adds a two-month extension (Art. 12(3)). **Close — Refused** and **Close — Partial Erasure** close the request with your decision.
Breach	**Mark DPA Notified** records that you have made the notification. **Close** closes the breach. **Archive (Admin Only)** archives it.
DPIA	**Approve** and **Reject** record the decision of the reviewer. **Re-sync Step 1 from RoPA** refills step 1 with the data from the linked activity.
Wizards	**Export RoPA (PDF)** opens a wizard with **Export Format** and **Include Archived Activities**; **Export** generates the report and **Cancel** closes it.

The buttons on requests, breaches and DPIAs are only visible to **GDPR Toolkit / Manager**. Those on the RoPA activity are visible to everyone, but only a manager can use them, because **GDPR Toolkit / User** has read-only access to the record. Only an Odoo administrator can archive a breach.

18 Security and personal data

- The **GDPR Toolkit / User** group has read-only access to the RoPA, can log requests and sees those in **Received** or assigned to them; changing them and using their buttons is a job for **GDPR Toolkit / Manager**.
- The **GDPR Toolkit / Manager** group sees everything and is the only one with the working buttons: verify identity, draft the response, close, approve a DPIA, mark a breach as notified, among others.
- **Archive (Admin Only)**, for breaches, is visible only to the Odoo administrator.
- Each company sees only its own records.
- Requests, breaches and activities are not deleted: they are archived or closed.
- The RoPA history and the audit log cannot be altered.
- The audit summary redacts personal data.
- Internal notes and the justification for a refusal (requests), and the description and consequences (breaches), are stored encrypted only if the server has the GDPR_FERNET_KEY environment variable set. Without it they are stored unencrypted, the server log notes this, and the configuration shows it under **Encryption Key Configured**.
- No requests, breaches, DPIAs or processing activities are sent to FlexigoTech Cloud. Your Odoo data stays in your Odoo. The paid service monitors six official sources and alerts you when one changes.

19 Multiple companies

Each Odoo company has its own GDPR configuration. If nobody has opened the configuration menu, the module creates it with the default values the first time it is needed. The **Dashboard** menu opens the configuration of the active company and creates it if it does not exist.

Each record (activity, request, breach, DPIA) carries its company, and each user sees those of the companies they have access to. Scheduled tasks loop through each company with its own configuration. Alerts go to the recipients that configuration specifies and, if there are none, to the GDPR managers of that company.

The privacy portal creates the request in the company active at the moment the data subject submits it.

The Standard plan costs €29 per month or €290 per year, and Pro costs €58 per month or €580 per year (prices exclude VAT). Each module has its own subscription, for the production database; its trial copies are included.

20 If something goes wrong

A processing activity does not activate and a warning appears that an approved DPIA is missing.	Complete and approve a DPIA linked to the activity. Once it is approved, press **Set Active** again.
A data subject request does not go back to a previous status.	Status only moves forward. If you made a mistake, note it in the internal notes and continue from the current status.

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 justification 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. For breaches, only an Odoo administrator can archive, and 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.

Other warnings you may see

«Only GDPR Managers can submit a DPIA for review.»	Ask a GDPR manager to send it for review.
«Only GDPR Managers (acting as DPO) can approve a DPIA.»	Approval is done by a GDPR manager, who acts as DPO. Ask whoever holds that permission.
«Only GDPR Managers can perform this action.»	The action is reserved for GDPR managers or Odoo administrators. Ask one of them.
«Only Odoo Administrators can archive breach records.»	Ask an administrator to archive the breach. A reason must be given.
«Archive reason is required.»	Write the reason for archiving and confirm again.
«Extension justification is required when extending retention.»	In the retention review, write the justification before saving the extension.
«New retention end date is required when extending retention.»	Enter the new retention deadline in the review before saving it.
«No Odoo contact linked to this DSAR. Please link a res.partner record first.»	Link the contact to the request and repeat the export.
The notice that the data subject's data has already been anonymised and needs manual handling with your DPO.	The contact is already anonymised in Odoo and there is no data to export. Check with your DPO how to respond.
«No processing activities found for this company.»	When exporting the RoPA, check that the active company has activities.

21 Other ways to do it

METHOD	WHAT IT INVOLVES
Manually	Spreadsheets for the processing register, requests and breaches. Deadlines are counted by hand and nobody alerts you when they are approaching.
Odoo alone	Odoo 17, 18, 19 and 20 include the privacy search as standard in Community, in the technical menu of Settings (with developer mode). It lets you find a person's records by name or email, archive or delete them, and keep a privacy log. It does not include a register of processing activities, data subject requests, a breach register or DPIAs.
This module	It adds the register of processing activities, data subject requests with their one-month deadline from receipt and the two-month extension (Art. 12.3), the breach register with the 72-hour countdown from when awareness is established (Art. 33.1), and DPIAs.

To delete or anonymise a person's data, Odoo's privacy search works alongside this module. The module tracks the request and records your decision; deleting or anonymising is done by you in Odoo.

22 Plans and pricing

€9

License per Odoo version.

+ FlexigoTech Cloud

STANDARD

€29/month

or €290 a year

- First response within 1 working day

PRO

€58/month

or €580 a year

- First response within 4 working hours
- Video call if needed

14-day trial, no card

Prices exclude VAT

The module license is per Odoo version. FlexigoTech Cloud is paid monthly or yearly, and the 14-day trial does not require a card.

23 Frequently asked questions

Does it work without FlexigoTech Cloud?

No.

What does the FlexigoTech Cloud subscription provide?

Daily monitoring of six official sources, with an alert when one changes. Alerts appear in **Settings › FlexigoTech Cloud** and in a daily email.

How much does FlexigoTech Cloud cost?

The Standard plan costs €29 per month or €290 per year, and the Pro plan €58 per month or €580 per year, excluding VAT. On top of that, the module license costs €9 per Odoo version.

Which sources does the service monitor?

The European Union acts amending the GDPR, the Digital Omnibus procedure in the European Parliament, the consolidated Spanish LOPDGDD from the BOE, the European Commission's adequacy decisions, and the AEPD's guidance and tools.

What leaves my Odoo for FlexigoTech Cloud?

The identification of the installation (identifier, address, public code, Odoo version and module names), the acceptance of the terms with the email of the person accepting, and the request for the service's permission. The processing register, requests, breaches, DPIAs and audit trail stay in your database.

Does it work on Odoo Online?

No. Odoo Online does not allow installing third-party modules.

Does it need Odoo Enterprise?

No. It only depends on Odoo Community modules (base, mail and portal) and flexigotech_cloud: it works on both Community and Enterprise.

Which Odoo versions is it available for?

There is a branch for each of versions 17, 18, 19 and 20.

What deadline does it calculate for a data subject request, and where does it come from?

One month from receipt of the request, under Art. 12.3 of the GDPR. The **Days Remaining** column counts down to the current deadline.

How is the deadline extended?

With **Extend Deadline (2 months)**, which adds two more months (Art. 12.3) and requires a reason. It only changes the **Current Deadline**; it does not change the request's status.

What happens when a request's deadline expires?

The request appears in the **Overdue** list. Each week, the task **GDPR: DSAR Overdue Escalation** sends a summary of overdue requests to the recipients of those alerts or, if there are none, to the GDPR managers.

How does it count the 72 hours of a breach, and who does it alert?

It counts from the date and time you record that awareness was established, under Art. 33.1. Every hour, the task **GDPR: Breach Countdown Alert** sends an email when 6 hours or less remain, until you mark it as notified.

Does it notify the supervisory authority?

No. You make the notification yourself and record here the status, the date and time, the means and the reference.

Does it communicate anything to those affected by a breach?

No. If the communication under Art. 34 is mandatory, you make it and record it with **Mark Data Subjects Notified**.

Does it delete or anonymise data in an erasure request?

No. **Retention Conflict Check** counts what exists and records your decision. Deleting or anonymising is done by you in Odoo.

Does it send the reply letter to the data subject?

No. You draft it in the response tab from a template and send it yourself. The only email sent automatically to the data subject is the acknowledgement of receipt for a request made through the portal.

What does portability export, and in which formats?

Contact details, order history (with the Sales app) and the employee record (with the Employees app, with explicit confirmation). The formats are JSON or CSV.

What does the portability export need in order to be generated?

A verified identity and a linked Odoo contact on the request. Without these, the wizard refuses.

How does a data subject make a request through the portal, and what do they need?

They go to /my/privacy-rights on your Odoo, which requires signing in, so they need a portal account. The module does not place a link in My Account: you provide the address yourself.

When is a DPIA marked as mandatory?

When two or more of the nine criteria on the **DPIA Criteria** tab are met, or if you force it manually. The two-criteria rule is a general guideline from WP248, not a legal obligation.

What is prior consultation?

The consultation with the supervisory authority under Art. 36. With high or critical residual risk, **Prior Consultation Required (Art. 36)** is ticked automatically. If you submit it, you record here what you did; the module does not submit it.

Can I delete a request, a breach or an activity?

No. Activities, requests and breaches are archived or closed. Only the Odoo administrator can archive a breach, and a reason is required.

What does the audit log record?

The date and time, the user, the operation, the model, the record name and, where available, the IP address of each change. Nobody can modify or delete its entries, not even an administrator.

What is stored encrypted?

Internal notes, the justification for a refusal, and the breach description and consequences, only if the server has the encryption key. Without it, they are stored unencrypted.

Does it work with multiple companies?

Yes. Each company has its own settings, and each user sees only the records of the companies they have access to.

Which languages are the screens in?

The module's screens are in Spanish. In other languages they appear in English; Odoo's menus and buttons appear in each user's language.

Does it suit a company with fewer than 250 employees?

Art. 30.5 of the GDPR exempts organisations with fewer than 250 employees from the obligations in paragraphs 1 and 2, unless the processing is likely to result in a risk to the rights and freedoms of data subjects, is not occasional, or includes special categories of data or data on criminal convictions and offences. The module does not judge whether this applies to you.

How many supervisory authorities and legal bases does it include?

32 supervisory authorities and 16 legal bases, which are loaded on installation. You choose the primary authority in **GDPR Toolkit › Configuration › DPO & Settings**.

What reports and exports does it have?

You can export the RoPA as PDF or Excel. There are also reports on the data subject request history, the breach register and the DPIA status.

What emails does it send?

Five scheduled tasks: the daily reminder of request deadlines, the hourly breach countdown, the daily retention check, the weekly escalation of overdue requests and the annual RoPA review reminder.

What does the Dashboard menu show?

Three buttons that open lists: **View Open DSARs**, **View Active Breaches** and **DPIAs Pending Review**. It shows no figures.

Does it decide for me whether to notify a breach or carry out a DPIA?

No. The final decision rests with the controller or its DPO. The risk matrix, impact by likelihood, belongs to the module, not to the law.

Is this legal advice?

No.

24 Glossary

GDPR	The General Data Protection Regulation, Regulation (EU) 2016/679. It is the European regulation from which the deadlines and obligations in the module derive.
LOPDGDD	The Spanish data protection and digital rights guarantee law. FlexigoTech Cloud monitors its consolidated text in the BOE.
AEPD	The Spanish Data Protection Agency. It is one of the 32 supervisory authorities included in the module.
Supervisory authority	The public authority that oversees data protection in each country. Breaches are notified to it (Art. 33.1). In **Primary Supervisory Authority** you choose yours.
DPO	The data protection officer or, if there is none, the person responsible for privacy. Their details are stored in the settings.
Controller	The party that decides why and how data is processed. Its register of processing activities is the one under Art. 30.1.
Processor	The party that processes data on behalf of the controller. Its register of processing activities is the one under Art. 30.2.
Data subject	The person whose data is processed and who can exercise their rights.
RoPA	The register of processing activities (Art. 30): one record per activity, with its history.
Data subject request	A request made by a data subject: access (Art. 15), rectification (Art. 16), erasure (Art. 17), restriction (Art. 18), portability (Art. 20) or objection (Art. 21).
Current deadline	The date by which a request must be answered: one month from receipt and, if extended, two more months (Art. 12.3).
Portability	The right to receive the personal data the data subject provided in a structured, commonly used and machine-readable format (Art. 20.1). The module exports it in JSON or CSV.
Erasure	The right to have data erased (Art. 17). The module counts what exists and records your decision; you carry out the deletion yourself.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. It must be notified to the supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of it, unless it is unlikely to result in a risk (Art. 33.1).
DPIA	The data protection impact assessment (Art. 35), with five steps.
Residual risk	The risk that remains after applying mitigation measures. Where residual risk is high or critical, prior consultation is flagged.
Prior consultation	Consultation with the supervisory authority before processing where a DPIA shows that the processing would result in a high risk in the absence of measures to mitigate it (Art. 36.1). You submit it yourself.
Lawful basis	The ground that permits the processing of data. The module provides 16: 6 under Art. 6 and 10 under Art. 9.
Special categories	The data covered by Art. 9, such as health data. These have their own lawful bases.

International transfer	The sending of data to a third country. The activity record captures the country and the safeguard that covers it.
Retention	How long the data of each activity is kept, with its estimated deadline and review history.
Audit trail	The list of who made which change, when, and from which IP address. It cannot be modified or deleted.
Monitoring	The FlexigoTech Cloud service that checks six official sources every day and alerts you when one of them changes.

MODULE GUIDE · GDPR COMPLIANCE

25 Checklist and contact

- [ ] You have Odoo 17, 18, 19 or 20 on Odoo.sh or on your own server. Odoo Online does not allow third-party modules to be installed.
- [ ] You have installed the module and its dependency, flexigotech_cloud.
- [ ] You have activated the 14-day FlexigoTech Cloud trial in **Settings › FlexigoTech Cloud** and have read the list of data that is sent.
- [ ] You have opened **GDPR Toolkit › Configuration › DPO & Settings** and filled in the DPO details and the **Primary Supervisory Authority**.
- [ ] You have set the recipients for breach and request notifications.
- [ ] You have given each person the **GDPR Toolkit / Manager** or **GDPR Toolkit / User** group.
- [ ] If you want to encrypt internal notes and breach descriptions, you have set the encryption key on the server and **Encryption Key Configured** confirms it.
- [ ] You have created the RoPA activities with their DPIA criteria and retention period.
- [ ] You have logged a first request and checked its **Current Deadline**.
- [ ] You have given data subjects the /my/privacy-rights address of your Odoo instance.
- [ ] If you wish, you have tested the breach register with a test breach and seen the 72-hour countdown.

If you would like us to set it up with you, get in touch. Every purchase includes 2 months of support: we help you install it, set it up and get it working, by email and video call.

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).