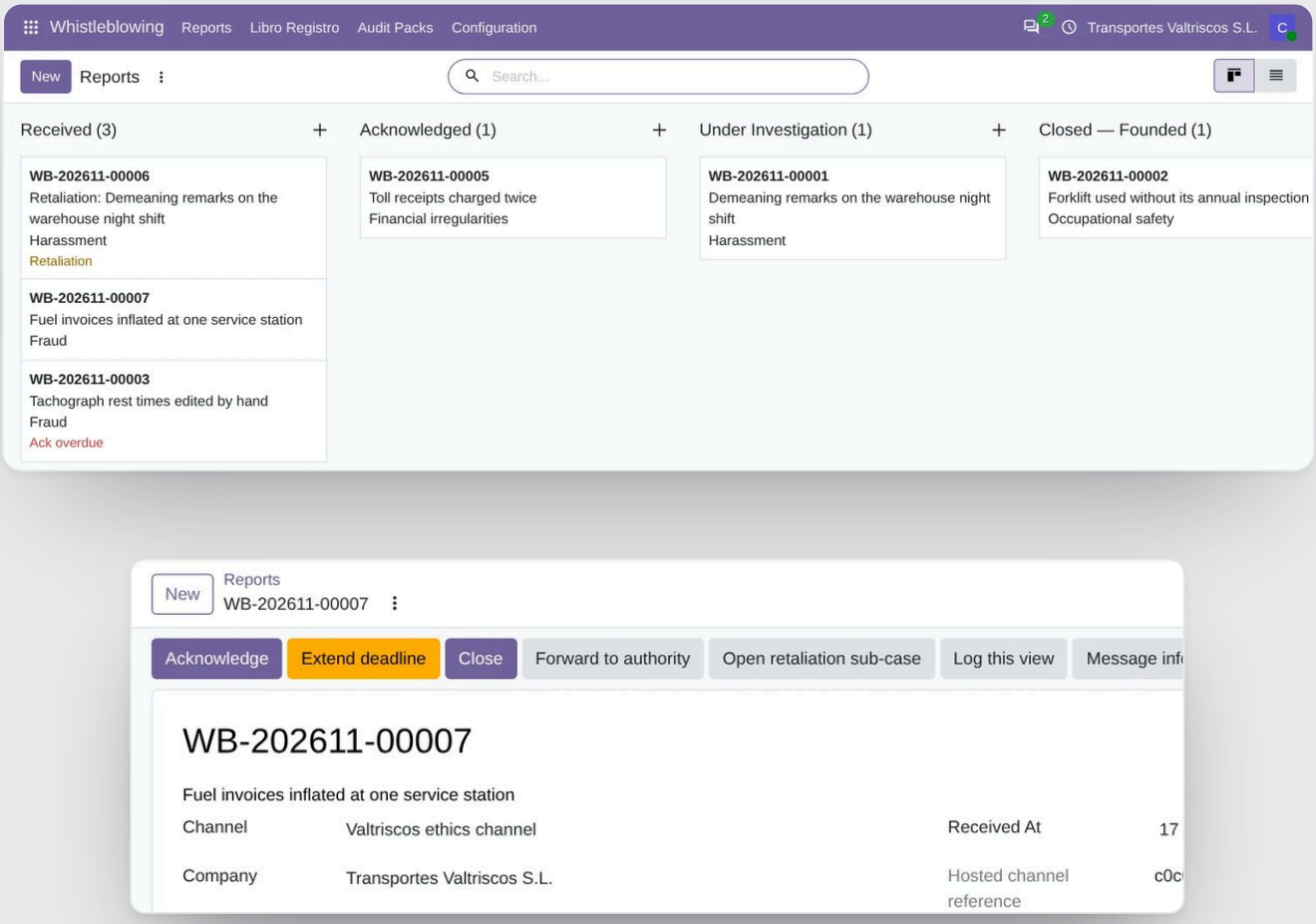
MODULE GUIDE · COMPLIANCE AND REGULATION

Whistleblowing for Odoo

A hosted page to report, anonymously or by name, and in your Odoo the deadlines, the reports register and the encrypted identity.

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



Real Odoo 20 screenshot. This dashboard shows reports by status and the detail view of a report received through the hosted page.

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 starting	6
5	The FlexigoTech Cloud trial	6
6	Connecting your reporting channel step by step	8
7	The channel and its hosted page	10
8	Receiving and handling a report	15
9	The deadlines: acknowledgement, response and extension	18
10	Talking to the informant	20
11	Who sees what: encryption, permissions and access logging	22
12	Closing, forwarding and retaliation	26
13	The register and the audit pack	30
14	Retention, data subject requests and import	33
15	The data that goes out and comes back	36
16	What happens automatically	37
17	The options and their defaults	38
18	Security and personal data	40
19	Several companies and groups of companies	40
20	If something goes wrong	41
21	Other ways of doing it	42
22	Plans and price	43
23	Frequently asked questions	44
24	Glossary	46
25	Checklist and contact	48

This guide describes version 20.0.1.3.12 of the module (Odoo branch 20.0, commit d70a9f16f). Everything in it comes from its published code, the platform's official documentation or real screenshots.

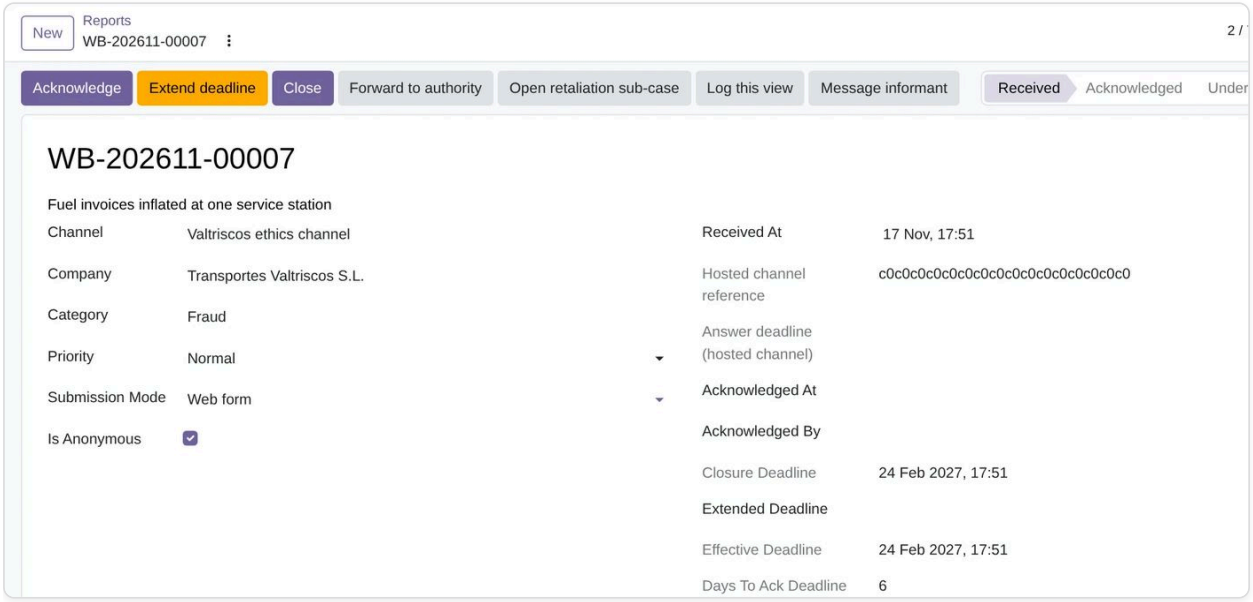
The screenshots come from a test Odoo 20 database, with a made-up company and data and no real connection to FlexigoTech Cloud. The module also has a version for Odoo 17, 18 and 19.

1 Who it is for and what it solves

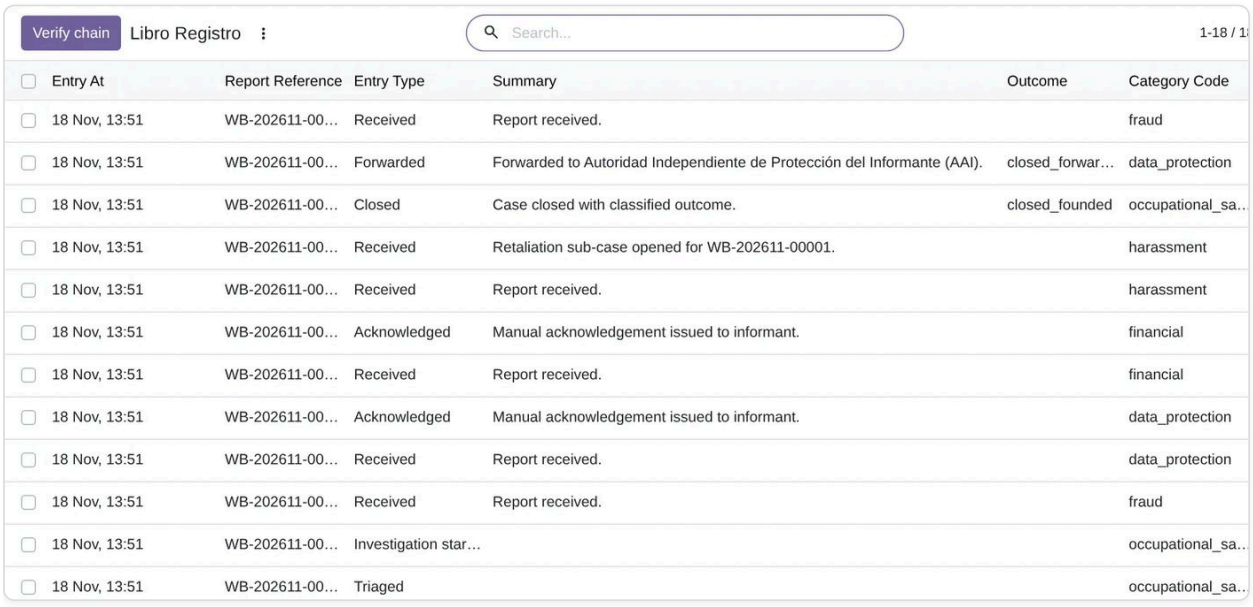
Law 2/2023 requires private-sector companies with fifty or more employees to have an internal information system (art. 10.1.a), and Directive (EU) 2019/1937 requires internal reporting channels for companies with 50 or more workers (art. 8.3). Companies with between 50 and 249 workers may share the system and resources with others (Law 2/2023 art. 12; Directive art. 8.6). The module serves those companies, their System Manager and their data protection officer.

Without a tool, the channel is usually a mailbox: deadlines are counted by hand, the register is a spreadsheet anyone can change, and there is no record of who read what.

With the module, reports arrive through the FlexigoTech Cloud hosted page, anonymous or named, even if your Odoo is down. They arrive sealed with your database key, and your Odoo collects them every 10 minutes and stores the reporter's text and details encrypted. Without the hosted channel, a new installation has no address for reporters.



- **Real Odoo 20 screenshot.** A report received through the hosted page, with its buttons for acknowledgement, deadline extension and closure.



- **Real Odoo 20 screenshot.** The register book with the button to verify the chain.

What changes day to day

- The 7-day acknowledgement deadline and the 3-month response deadline are calculated automatically (Law 2/2023 art. 9.2.c and 9.2.d; Directive art. 9.1.b and 9.1.f), with alerts for overdue items and activities for the System Manager.
- The reporter's identity is stored encrypted, and on screen only the System Responsable can see it. Investigators, HR and Legal cannot see it either.
- With the reporter there is a secure thread through the hosted page, and from a report you can open a retaliation sub-report.
- The register book required by Law 2/2023 art. 26 cannot be changed from Odoo and is chained with SHA-256 fingerprints: the verify-chain button warns if someone altered an entry outside Odoo.
- Each report keeps its event history, and the audit pack gathers the register book and the records for a period into a ZIP file.

What it does not do

- It does not send anything to any authority. The forward button records which authority it was forwarded to, closes the report as forwarded and leaves the entry in the register book; you are the one who sends it.
- It does not investigate or decide: the System Manager classifies, investigates and closes each report. It is not legal advice.
- It does not notify the Independent Authority for the Protection of Whistleblowers of the appointment or dismissal of the Manager (Law 2/2023 art. 8.3): the company ticks that box by hand.
- It does not book in-person meetings through the hosted page, does not record or transcribe verbal communications, and has no screen for writing down a report received verbally.
- It does not apply the law of any country other than Spain: with any other country profile, only the response deadline calculation changes, counted from the acknowledgement, as in the Directive.

MODULE GUIDE · WHISTLEBLOWING

2 The module in figures

4
Odoo versions: 17, 18, 19 and 20

14
days of FlexigoTech Cloud trial

7
days for acknowledgement of receipt

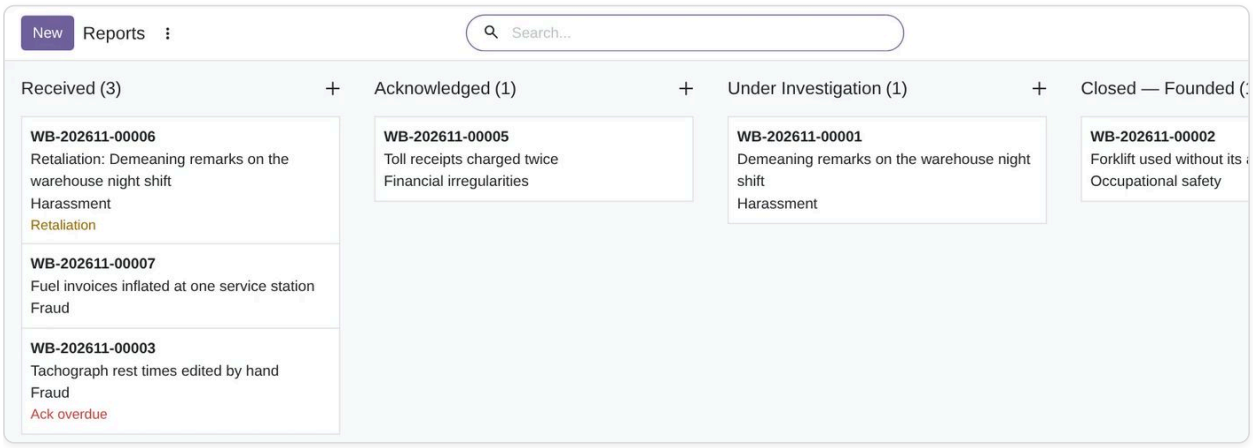
3
months for the response

7
scheduled tasks

195
automated tests

The module works on Odoo 17, 18, 19 and 20. It depends on base, web, mail, website, portal, calendar and flexigotech_cloud.

3 Where you see it in your Odoo



- **Real Odoo 20 screenshot.** The **Reports** dashboard, with the sample reports grouped by status.

Everything hangs off the **Whistleblowing** menu. Almost all of its screens appear in English in every language, including Spanish, and they are written here exactly as you will see them.

Whistleblowing › Reports	The reports, as a status dashboard and as a list. The System Manager and investigators see them; investigators see only the reports they are assigned to.
Whistleblowing › Libro Registro	The register book required by Law 2/2023 art. 26, with a button to verify its chain. The Manager, the data protection officer and the external auditor see it.
Whistleblowing › Audit Packs	The audit packs already generated and, inside it, **Whistleblowing › Audit Packs › Generate Audit Pack** to create a new one. The Responsable and the data protection officer can see them; only the Responsable can generate.
Whistleblowing › Configuration	**Whistleblowing › Configuration › Channels**, **Whistleblowing › Configuration › Categories**, **Whistleblowing › Configuration › Responsables**, **Whistleblowing › Configuration › Policy documents**, **Whistleblowing › Configuration › Privacy notices**, **Whistleblowing › Configuration › DPIA artefacts**, **Whistleblowing › Configuration › External authorities**, **Whistleblowing › Configuration › Retention policies**, **Whistleblowing › Configuration › Import batches**, **Whistleblowing › Configuration › Import legacy reports** and **Whistleblowing › Configuration › GDPR DSAR Assembly**. The Responsable and the Data Protection Officer can see them; the two import menus are visible only to the Responsable.

Outside its own menu, the module comes with seven scheduled tasks, which collect the reports from the hosted page, watch the deadlines, apply retention and expire the per-case permissions, and a **Whistleblowing** section in the Odoo settings. Reports arrive through the FlexigoTech Cloud hosted page, which you activate from the channel.

4 What you need before starting

- Odoo 17, 18, 19 or 20, on Odoo.sh or your own server. It does not work on Odoo Online, which does not allow installing third-party modules.
- Your Odoo must open at an https address: without it, the channel cannot be published.
- The Website app. The module installs it if you do not have it.
- Who will be the System Manager: a person with an Odoo user or a collegiate body. The administration body appoints them (Law 2/2023 art. 8.1 and 8.2).
- Who will act as investigator and who as data protection officer.
- The text of the channel policy and the privacy notice.
- An https address where you publish your legal texts for reporters, and an email address to receive deadline alerts.
- A FlexigoTech Cloud subscription or its 14-day trial.

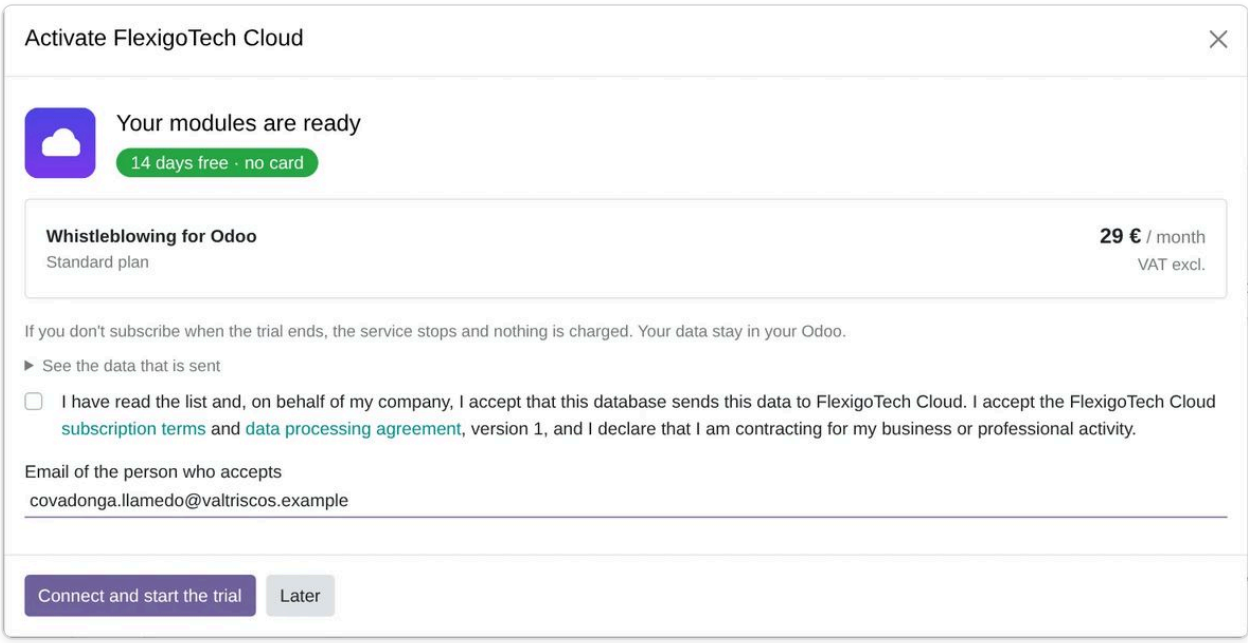
> What the module does not do for you. It does not notify the Independent Authority for the Protection of Whistleblowers of the appointment or dismissal of the Manager: the notification box is ticked by hand once you have done it. It sends nothing to any authority, not even the Public Prosecutor's Office: forwarding to an authority only records which one you forwarded to and keeps a trace. It does not investigate or decide: the Manager classifies, investigates and closes each report with its outcome and measures. And it is not legal advice.

It is installed like any third-party Odoo module, on Odoo.sh or your server. Odoo installs at the same time `flexigotech_cloud`, the connection to FlexigoTech Cloud, and, if you do not have them, the apps it depends on: Website, Discuss and Calendar.

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 free days, no card required.



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

2 **Accept and enter your email**

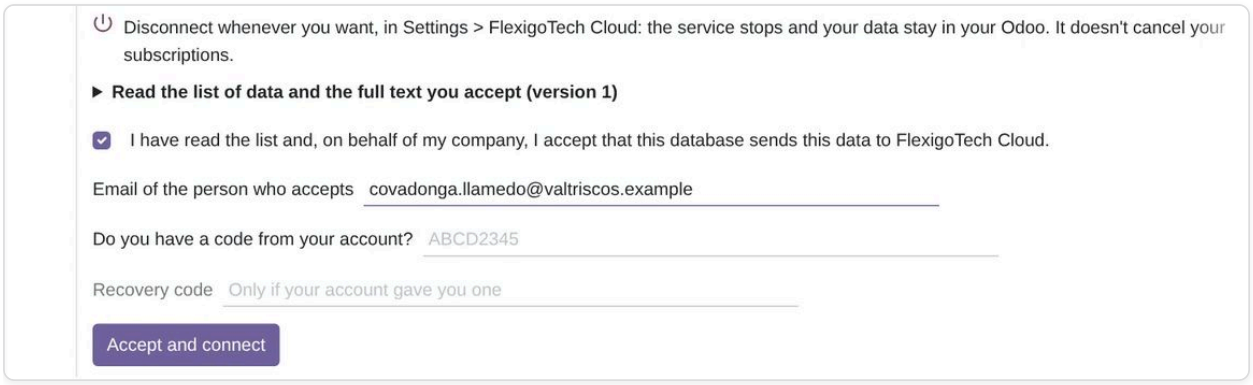
Tick "I have read the list and, on behalf of my company..." (it includes the subscription terms and the data processing agreement) and enter the **Email of the person who accepts**.

3 **Click Connect and start the trial**

Odoo registers the database with FlexigoTech Cloud and the module trial begins. If you want to leave it for later, **Later** closes the window.

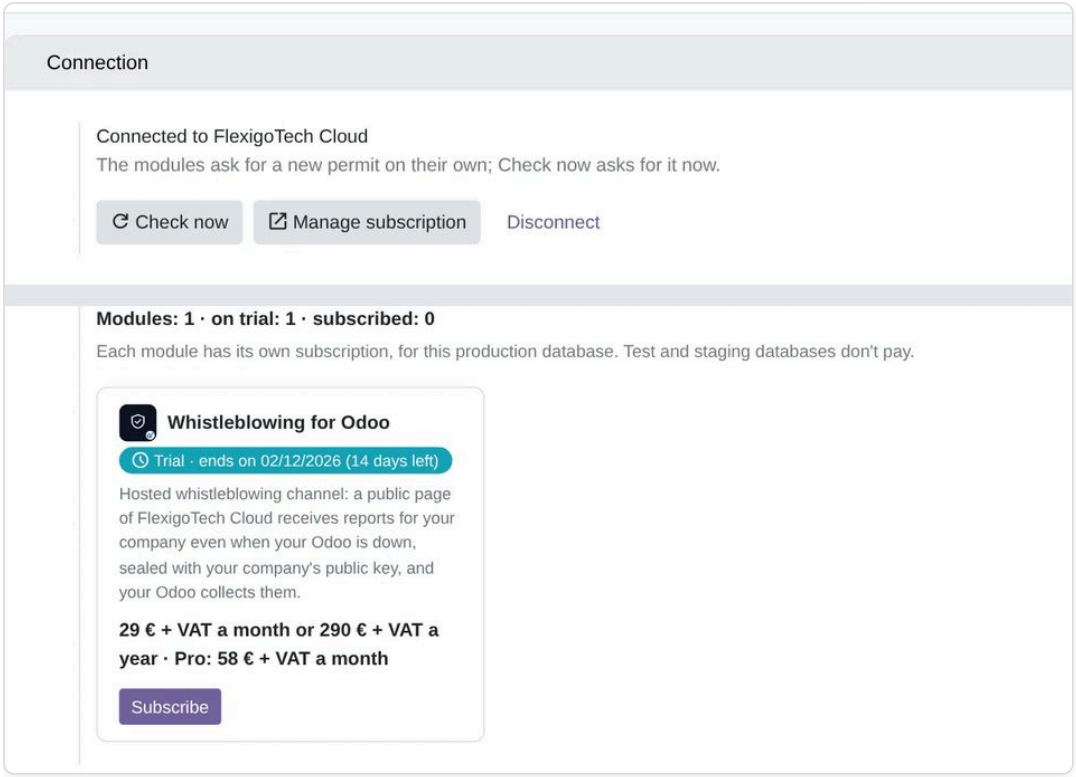
The same, from Settings

Settings › FlexigoTech Cloud has 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 **Do you have a code from your account?** field 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**.

Once the database is 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 the permit immediately (otherwise the module renews it by itself every 6 hours).

> A trial cannot be started 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 · WHISTLEBLOWING

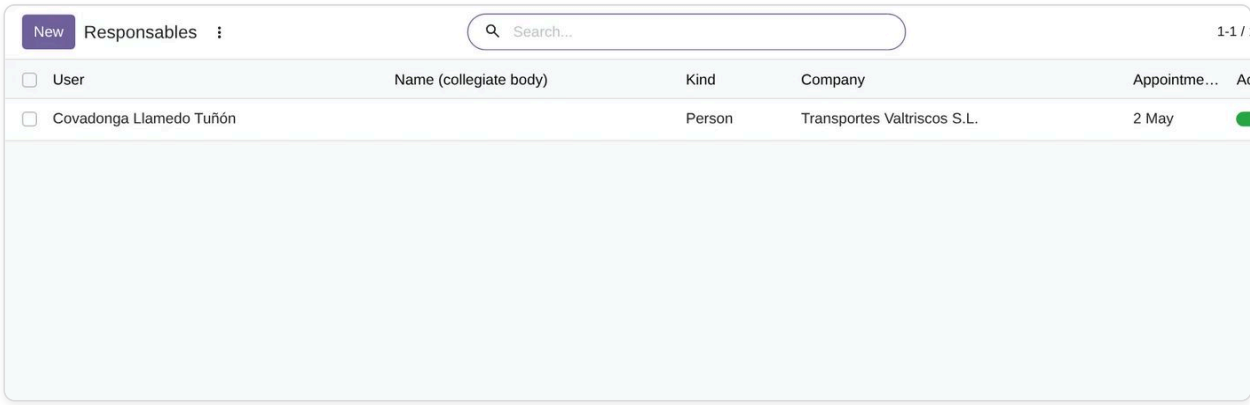
6 Connecting your reporting channel step by step

1. **Give the Manager their group**

   On installation, the module gives none of its groups to anyone, not even the administrator: until someone has one, nobody sees the **Whistleblowing** menu and its lists give an access error. An administrator opens the user record of whoever is going to be the Responsable del Sistema (it can be you) and gives them the **Whistleblowing / Responsable del Sistema** group. That group includes those of investigator, data protection officer, external auditor and Board dashboard.

2. **Create the System Manager**

   Go to **Whistleblowing › Configuration › Responsables** and click **New**. In **Kind** you choose the type: a person carries their user in **User** and a collegiate body carries its name in **Name (collegiate body)**. The appointment date goes in **Appointment Date** and cannot be in the future. In the **AAI notification** group you attach the designation document and, once you have notified the appointment to the Autoridad Independiente de Protección del Informante, you tick **Notified To Aai** yourself and its date. There can only be one active Responsable per company. On saving, their user also receives the group from the previous step.



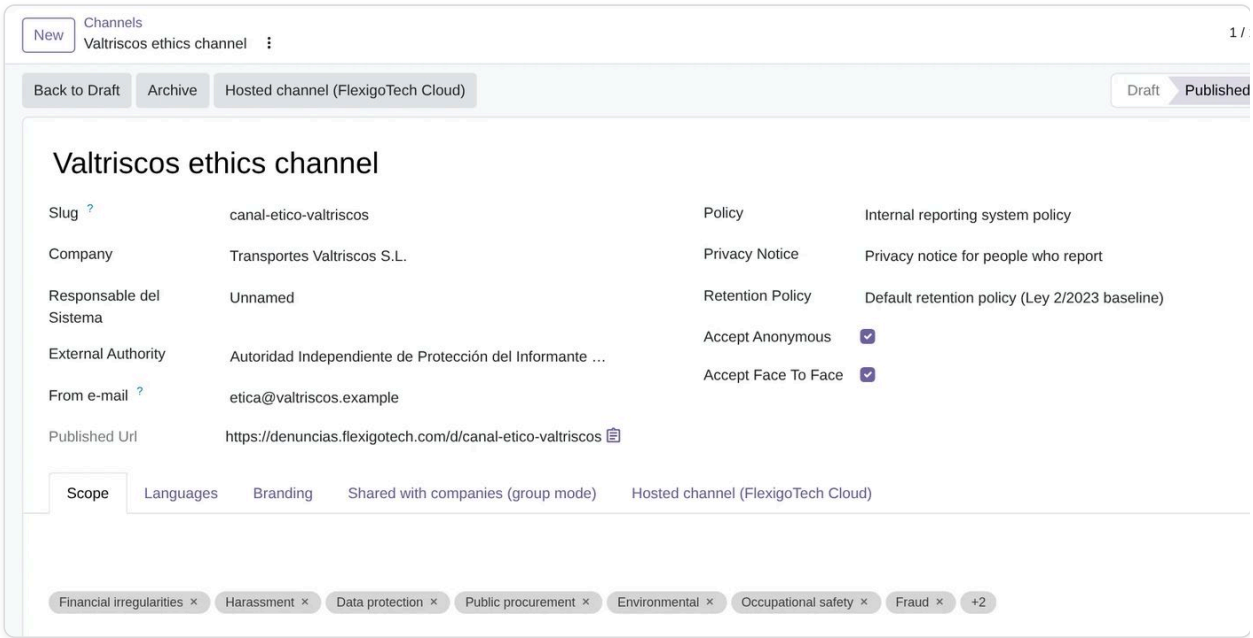
- **Real Odoo 20 screenshot.** The **Responsables** list with the Manager of the sample company.

3 Create the policy and the privacy notice

Write the channel policy in **Whistleblowing › Configuration › Policy documents** and the privacy notice in **Whistleblowing › Configuration › Privacy notices**. The channel needs both in order to be published.

4 Create the channel and publish it

Go to **Whistleblowing › Configuration › Channels** and click **New**. Enter the channel name and its identifier in **Slug**, and choose the **Responsable del Sistema**, the **Policy**, the **Privacy Notice** and the **External Authority**. In the tabs you choose the **Languages** and, in **Scope**, the **Accepted Categories**: these are the languages and categories the channel passes to the hosted page. Then click **Publish**. To publish you need the Responsable, the policy, the privacy notice, and your Odoo address must start with https. In a company in Spain you cannot remove **Accept Anonymous** (Ley 2/2023 art. 7.3).



- **Real Odoo 20 screenshot.** The sample channel, with the **Hosted channel (FlexigoTech Cloud)** button at the top and the address of its hosted page in **Published Url**.

5 Activate the hosted page

On the channel, click **Hosted channel (FlexigoTech Cloud)**; only administrators see it. The wizard explains what is sent to FlexigoTech Cloud before anything is sent. Fill in **Page address** (3 to 40 lowercase letters, digits or hyphens), **Legal texts address (https)** and **Email for deadline alerts**, and if you

wish **Your other reporting channels**. Tick the acceptance box and click **Activate the hosted channel**. A database has only one active hosted channel: activating it on one channel turns off the others.

6 **Give the address to staff**

With the page active, **Published Url** shows its address, at denuncias.flexigotech.com. This is the one reporters will use: put it where your staff can find it.

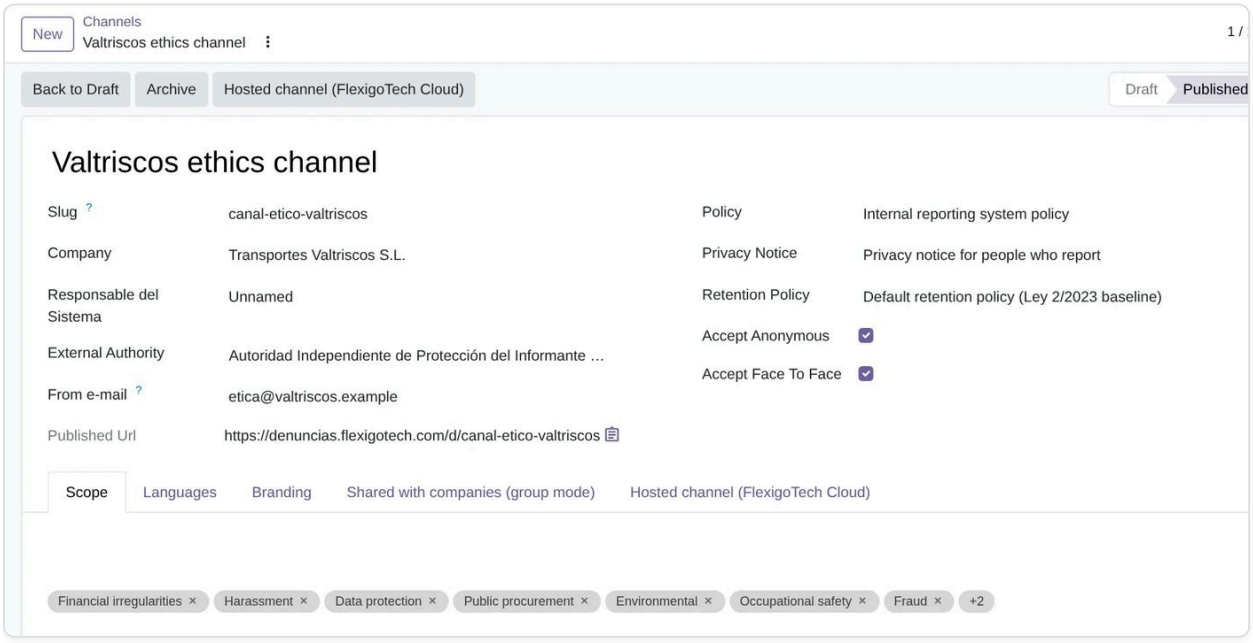
7 **Give the groups to others**

Give each person their group on their user record: **Whistleblowing / Investigator** to whoever investigates, **Whistleblowing / Data Protection Officer** to the data protection officer and **Whistleblowing / External auditor** to the auditor. HR and Legal go through per-case permissions: this is explained in "Giving access to a case".

After activation, the hosted page already receives reports. Your Odoo collects them automatically, every 10 minutes, with the scheduled task **Whistleblowing: hosted channel (FlexigoTech Cloud)**, and stores the reporter's text and details encrypted. Two other tasks monitor deadlines: **Whistleblowing: recompute overdue flags**, every 15 minutes, and **Whistleblowing: deadline reminders**, every hour.

MODULE GUIDE · WHISTLEBLOWING

7 The channel and its hosted page



- **Real Odoo 20 screenshot.** The channel with its buttons, the published address and the tabs.

The channel

Go to **Whistleblowing › Configuration › Channels**. Each channel has a name, an identifier in Odoo (**Slug**) and the company it belongs to. The other fields on the form:

Responsable del Sistema	The person or body that manages the reports of this channel.
Languages and **Accepted Categories**	The channel's languages and the infringement categories it accepts.
Policy and **Privacy Notice**	The channel policy and the privacy notice shown to the reporter.

External Authority	The external authority to which a forwarding is directed.
Accept Anonymous	Whether the channel accepts anonymous reports. In a company in Spain it cannot be removed (Ley 2/2023 art. 7.3): on saving, the warning "Anonymous reporting is mandatory in Spain (Ley 2/2023 art. 7.3); cannot be disabled for a Spanish company channel." appears.
Published Url	The address for reporters. In a new installation it is that of the hosted page, and there is none until you activate it.

Tabs and states

The channel has the tabs **Scope**, **Languages**, **Branding**, **Shared with companies (group mode)** and the hosted channel one. Its state is **Draft**, **Published** or **Archived**. The buttons change according to the state:

Publish	Shown only in draft. Moves the channel to published.
Back to Draft	Shown when the channel is not in draft. Returns it to draft.
Archive	Shown while the channel is not archived. Archives it.

To publish, the channel needs a Responsable del Sistema, a policy and a privacy notice, and the Odoo address (the one Odoo has stored as its web address) must start with https. If anything is missing, Odoo says so in a message in English: "Cannot publish a channel without a Responsable.", "Cannot publish a channel without a Policy.", "Cannot publish a channel without a Privacy Notice." or "Whistleblowing channels require HTTPS. The current web.base.url (...) is plain HTTP. Configure TLS before publishing.".

Activate the hosted page

The hosted page is a public FlexigoTech Cloud page, at denuncias.flexigotech.com/d/ followed by the page address. It receives reports even if your Odoo is down. Without it, a new installation has no address for informants.

1. **Open the wizard**
   In the channel, press **Hosted channel (FlexigoTech Cloud)**. Only administrators see it. The wizard explains what is sent to FlexigoTech Cloud before sending anything.

2. **Fill in the details**
   Page address (3 to 40 lowercase letters, digits or hyphens; the wizard proposes the channel identifier), **Legal texts address (https)** and **Email for deadline alerts** are mandatory. The email is pre-filled with the Responsable user's email or, if they have none, the company's. **Your other reporting channels** is optional.

3. **Accept**
   Tick the acceptance box, which is given on behalf of your company. If you don't tick it, "Tick the box to accept before activating the hosted channel." appears and nothing is activated.

4. **Press Activate the hosted channel**
   If FlexigoTech Cloud accepts the registration, the channel becomes active and stores the accepted text version, who accepted and when. If not, Odoo says why; for example, "That page address belongs to another company: choose another one.".

The **Hosted channel (FlexigoTech Cloud)** tab of the channel shows **Hosted channel active**, **Hosted page** (the page address), **Hosted page address**, **Legal texts address (https)**, **Email for deadline alerts** and **Other reporting**

channels, and on the right **Accepted text version**, **Accepted DPA version**, **Accepted by** and **Accepted on**.

> A database has only one active hosted channel: if you activate the page on one channel, it is switched off on the others, including those of other companies. The page does not store the IP address of the person reporting, either in the application or in its server log.

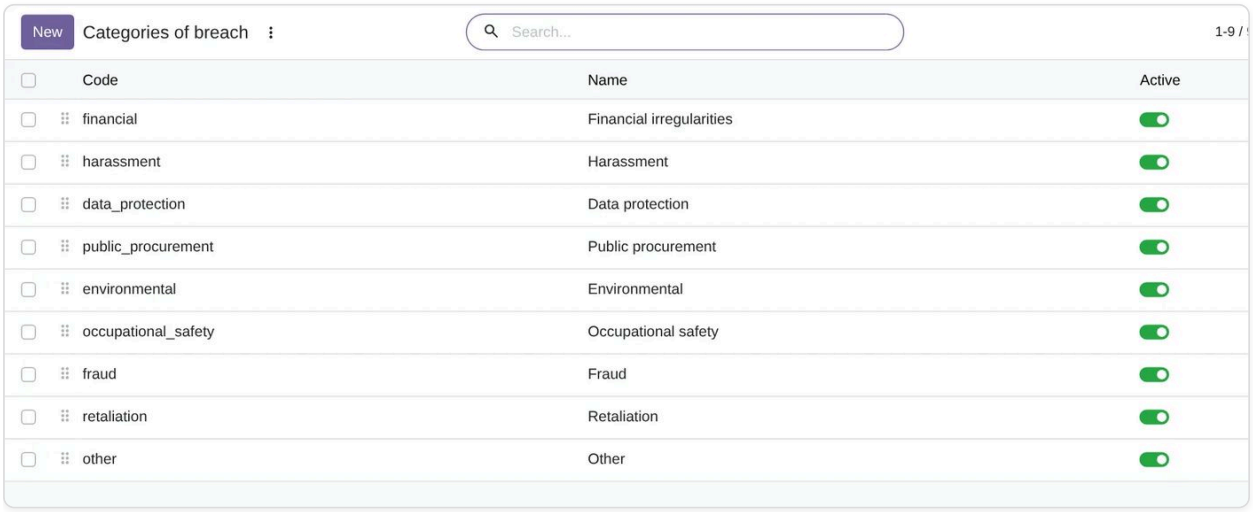
What the informant sees

- The page asks for the category, the subject and the text of the report.
- The informant chooses between reporting anonymously or with a name and email.
- Up to 10 attachments can be uploaded.
- On submission, the page shows once a 26-character tracking code that they do not choose. With that code they return, read the company's messages and reply with messages and attachments.
- The page can appear in Spanish, English, Catalan, Portuguese, French or German. It shows the language of whoever opens it if the channel has it in **Languages**; otherwise the first of those six that the channel has, or English. There is no Italian, Dutch or Polish.

Where reports come from

Reports arrive sealed at FlexigoTech Cloud. The scheduled task **Whistleblowing: hosted channel (FlexigoTech Cloud)** runs every 10 minutes in your Odoo: it collects what has been received, stores encrypted the text and the informant's data, passes on to the informant what the company has written to them, and reads the deadlines of each hosted report.

The categories



- **Real Odoo 20 screenshot.** The 9 categories that the module ships with, in **Categories of breach**.

The module installs 9 categories, in **Whistleblowing › Configuration › Categories**. Each one carries **Code**, **Name** and **Active**.

CODE	NAME
financial	Financial irregularities
harassment	Harassment

CODE	NAME
data_protection	Data protection
public_procurement	Public procurement
environmental	Environmental
occupational_safety	Occupational safety
fraud	Fraud
retaliation	Retaliation
other	Other

> Until an administrator gives a user the **Whistleblowing / Responsable del Sistema** group, nobody sees the **Whistleblowing** menu and its lists give an access error. Nor can the text of a received report be changed by hand: it only comes in through the hosted page.

Channel states and what each one means

STATE	MEANING
Draft	The state a channel is created in. Everything can be edited. To move to published, the publication requirements must be met.
Published	The channel is published. With the hosted page active, the address for informants is that page's.
Archived	The channel is archived. **Back to Draft** returns it to draft.

Rules and conditions

- The channel identifier in Odoo (**Slug**) only accepts lowercase letters, digits and hyphens, 2 to 64 characters. Otherwise "Slug must be lowercase letters, digits and hyphens (2-64 chars)." appears.
- The hosted page address is something else: 3 to 40 lowercase letters, digits or hyphens. The wizard proposes the channel identifier, but it can be changed there.
- In a company with country Spain, **Accept Anonymous** cannot be unticked (Spanish Law 2/2023, art. 7.3).
- To publish, you need a Responsable, a policy, a privacy notice and an Odoo address with https.
- Only administrators see the **Hosted channel (FlexigoTech Cloud)** button. Without ticking the acceptance, the wizard does not activate anything.
- When installing or updating the module, the key with which the cloud seals reports for your database is created before any registration. The private key never leaves your Odoo, and a neutralised copy of the database (staging) does not keep it.

What is sent and what the cloud stores

The wizard sends the cloud what is needed to publish the page: your database's public key, the page address, the channel's categories and languages, the address of your legal texts, the company's country, the alerts email and your other channels. The page shows your company's name as registered in FlexigoTech Cloud. The cloud stores each report sealed with your database's key, without being able to read it, until your Odoo confirms it has it. It also monitors deadlines: it writes to the alerts email on day 5 if there is no acknowledgement and 14 days

before the end of the response deadline, with nothing from the report (only the channel, the reference and the date).

Register fields and tabs

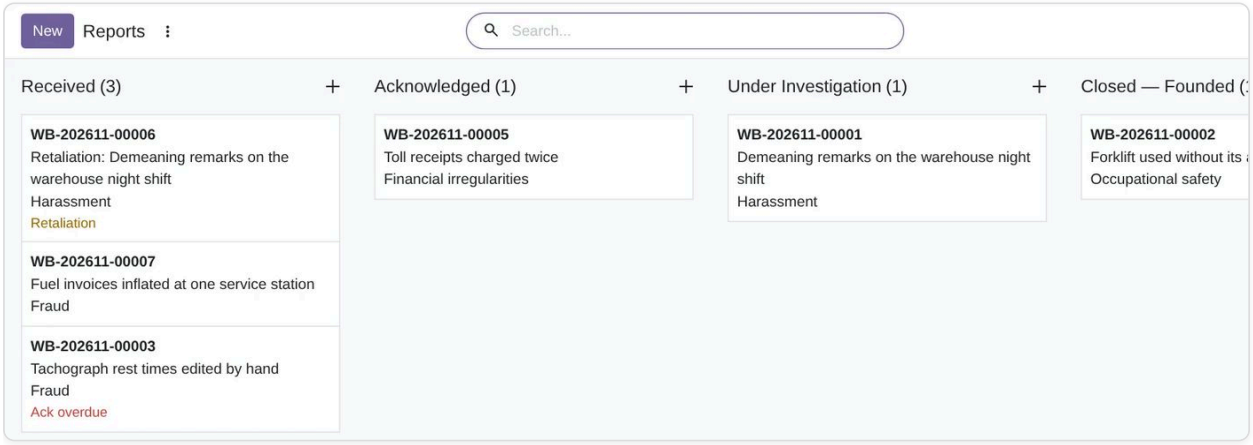
Name, **Slug**, **Company**	Basic channel details. All three are mandatory.
Scope Statement	Free text on the scope of the channel (**Scope** tab, next to the **Accepted Categories**).
Languages	Channel languages (**Languages** tab).
Branding Logo and **Branding Color Primary**	Logo and colour (**Branding** tab).
Retention Policy	The retention policy that applies. It is mandatory and pre-filled.
Shared with Companies (group)	Companies with which the channel is shared (**Shared with companies (group mode)** tab). Spanish Law 2/2023, art. 12 allows sharing means between private-sector companies with 50 to 249 employees.
Accept Face To Face	Ticked by default. On a new installation it changes nothing: the hosted page does not offer to request an in-person meeting, which Spanish Law 2/2023 art. 7.2 provides for at the informant's request within seven days at most.

End-to-end example

The example channel is called Valtriscos ethics channel. It belongs to the company Transportes Valtriscos S.L., refers to the Autoridad Independiente de Protección del Informante (AAI) and its Responsable del Sistema is Covadonga Llamedo Tuñón. Its hosted page is at **https://denuncias.flexigotech.com/d/canal-etico-valtriscos**. The whistleblower goes to that address and submits their report. The task that runs every 10 minutes collects it, and it appears in **Whistleblowing › Reports** under **Received**, with its reference, for example WB-202611-00007. On that record, **Hosted channel reference** shows the report's reference in the cloud and **Answer deadline (hosted channel)** the date calculated by FlexigoTech Cloud.

8 Receiving and handling a report

Whistleblowing › Reports opens the reports on a board by state; there is also a list view. On opening, the **Open** filter is already applied, so closed ones do not appear until you remove it. In the list, those with an overdue deadline appear in red; on the board, their card says **Ack overdue** or **Closure overdue**. In the search there are filters for **Open**, **Closed**, **Overdue acknowledgement**, **Overdue closure** and **Retaliation**, and groupings by **State**, **Category** and **Priority**.

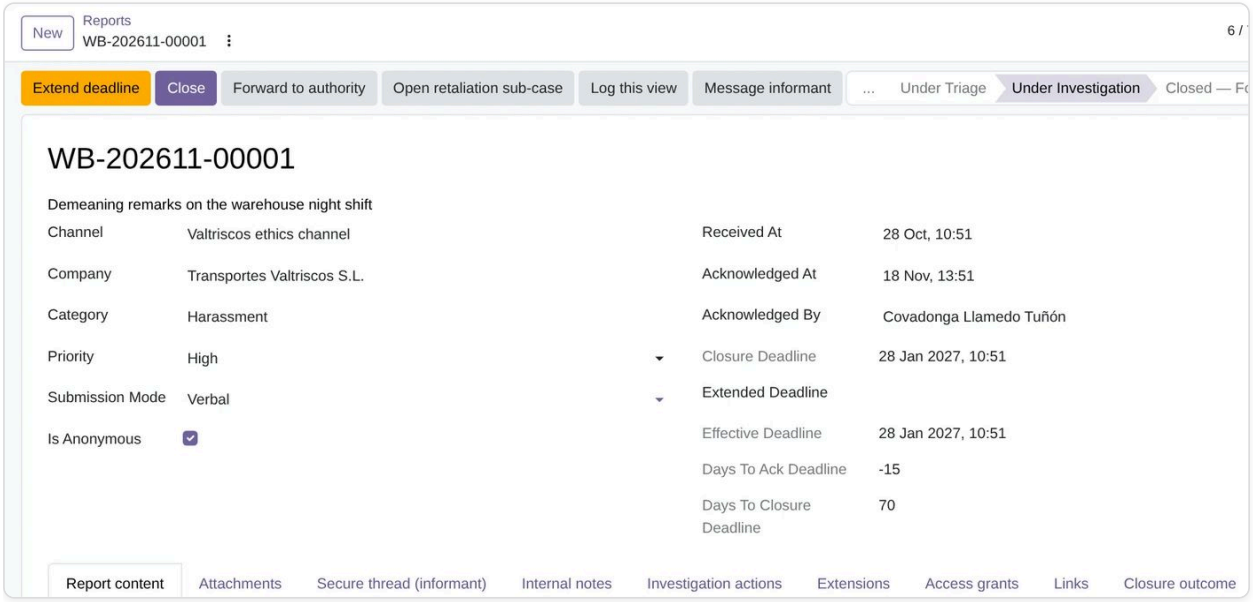


- **Real Odoo 20 screenshot.** The reports board with the reports grouped by state.

Reports from the hosted page are collected only by the task **Whistleblowing: hosted channel (FlexigoTech Cloud)**, every 10 minutes. The report stores its hosted-channel reference in **Hosted channel reference** and the date calculated by FlexigoTech Cloud in **Answer deadline (hosted channel)**. On creation, the module logs the event and the entry in the register book.

The form

At the top appear the report details: **Channel**, **Company**, **Category**, **Priority** (**Normal**, **High** or **Retaliation**), **Submission Mode** (**Web form**, **Verbal** or **Face to face**) and **Is Anonymous**. On the right are the dates: **Received At**, **Acknowledged At** and the deadlines. Below there are tabs for the content, attachments, the secure thread with the whistleblower, internal notes, investigation actions, extensions, per-case permissions, links, closure, events, the access log and meetings.



- **Real Odoo 20 screenshot.** A report under investigation with its buttons and tabs.

Acknowledge	Acknowledges receipt: records who and when, leaves a message for the informant, notes the entry in the register book and, if the informant gave their email, sends them a notice. Only visible with the report in **Received**.
Triage	Moves to **Under Triage**. Only visible with the report in **Acknowledged**.
Start investigation	Moves to **Under Investigation**. Visible in **Acknowledged** and **Under Triage**.
Message informant	Writes to the informant through the secure thread. Only the Responsable del Sistema sees it.
Log this view	Records in the access log that you have read the content. Only the Responsable del Sistema sees it.

Investigators are assigned in **Assigned Investigators**, in the **Access grants** tab; each one sees only the reports they are on. Attachments are not encrypted: they are stored as Odoo attachments, with a limit of 25 MB per file and 100 MB per report. EXIF metadata is removed from images. They are only scanned for viruses if you enable **Anti-virus scanning** and your Odoo server has ClamAV; otherwise they remain unscanned.

> Once the report is closed, **Extend deadline** and **Close** disappear. The **Report content** tab, with the text and the reporter's identity, is visible only to the System Responsable. The reporter, the report text and the assigned investigators can only be changed by the Responsable, or by an assigned investigator who is also an Odoo administrator.

Report states

In the status bar, a closed report shows as **Closed** followed by the outcome chosen when it was closed.

STATE	MEANING
Received	It has come in and receipt has not yet been acknowledged.
Acknowledged	Receipt has already been acknowledged to the informant.
Under Triage	It is being assessed what to do with it.
Under Investigation	It is under investigation.
Closed with Founded	It was closed with the outcome founded.
Closed with Partially founded	It was closed with the outcome partially founded.
Closed with Unfounded	It was closed with the outcome unfounded.
Closed with Inadmissible	It was closed without being admitted for processing.
Closed and forwarded	It was closed after noting which external authority it is forwarded to.
Purged (not pursued)	The retention policy erased its content.
Retained anonymised	Once the policy's years had passed, the informant's data was erased.

Rules of the cycle

- **Acknowledge** is only valid while the report is in **Received**; otherwise Odoo says "Only reports in state 'Received' can be acknowledged."

- **Triage** is only valid from **Acknowledged**: "Only acknowledged reports can move to triage."
- **Start investigation** is only valid from **Under Triage** or **Acknowledged**: "Investigation can only start from 'triaged' or 'acknowledged'."
- On screen, the text and the reporter's identity are visible only to the System Responsable; the DSAR assistant of the Data Protection Officer decrypts the identity to find the reports belonging to whoever requests their data.
- **Forward to authority** requires first choosing the authority: "Select an external authority before forwarding."
- On closure, the outcome and the measures are mandatory: "Outcome and measures summary are mandatory at closure."

Close, forward and retain

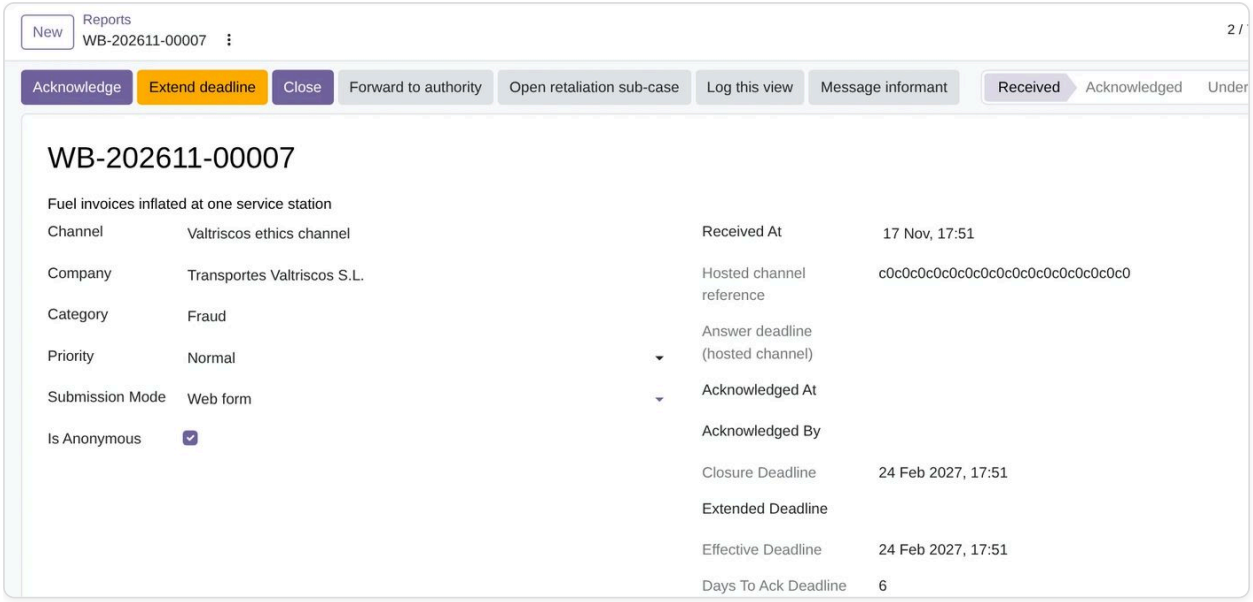
Close asks for the outcome and the measures. **Forward to authority** sends nothing: it records the authority and the date, closes the report as forwarded, and leaves the entry in the register. The sending is done by the company on its own. The task **Whistleblowing: enforce retention** purges reports closed as inadmissible or unfounded 90 days after closure (default value, between 1 and 90). Spanish Law 2/2023, art. 32.4, counts three months from receipt for what was not investigated: an open report that nobody investigates is not purged on its own.

Tabs and fields

Report content	The informant's name and email, **Description of facts** and, after closure, **Outcome (after closure)** and **Measures (after closure)**. Only the Manager sees it.
Attachments	The report's files, unencrypted, with a limit of 25 MB per file and 100 MB per report.
Secure thread (informant)	The messages with the informant and, in **Hosted channel**, how their sending is going. Only the Manager sees it.
Internal notes	The list of internal notes, encrypted, with their date, author and type.
Investigation actions	An editable list of actions, with their type, **Subject**, date and whether they are done.
Extensions	The extension of the deadline, with the new date, who decided it and when.
Access grants	The assigned investigators and the permissions per case.
Links	Links from the report to other Odoo records.
Closure outcome	The authority and date of a forwarding, and the date and author of the closure.
Events and **Access log**	The report's history (date, type and who) and the access log (date, user and action).
Meetings	The list of meetings, with the date each one was requested and the date it took place.

An end-to-end example

WB-202611-00007, about inflated fuel invoices, comes in at **Received**. It has its hosted channel reference and, as there is no acknowledgement yet, its response date counts from when the 7 days expire: 24 Feb 2027. The Manager presses **Acknowledge** and the report moves to **Acknowledged**; with the Spanish profile, the date counts from receipt. Then they press **Triage** and then **Start investigation**. Meanwhile they use **Message informant** to ask for details. On finishing, they press **Close** with the outcome and the measures.



- **Real Odoo 20 screenshot.** A report just collected from the hosted channel, with **Hosted channel reference**.

MODULE GUIDE · WHISTLEBLOWING

9 The deadlines: acknowledgement, response and extension

How they are calculated

- Acknowledgement of receipt: 7 calendar days from receipt (Law 2/2023 art. 9.2.c; Directive (EU) 2019/1937 art. 9.1.b). **Days To Ack Deadline** counts the days left; negative, the days that have passed.
- Response with the Spanish country profile: 3 months from receipt, once acknowledged (Law 2/2023 art. 9.2.d).
- Response with any other profile: 3 months from acknowledgement (Directive (EU) 2019/1937 art. 9.1.f).
- Without acknowledgement, with any profile: 3 months from when the 7 days of the acknowledgement expire (Law 2/2023 art. 9.2.d; Directive art. 9.1.f).
- Days and months are calendar ones: public holidays and weekends are not deducted.

The response date appears in **Closure Deadline**. If there is an extension, the new date goes to **Extended Deadline**, and the one that applies is **Effective Deadline**. **Days To Closure Deadline** counts the days left while the report is open. Changing the country profile does not recalculate dates already set.

The warnings

- When a deadline passes, the report record shows a red warning at the top: "Acknowledgement deadline missed." or "Closure deadline missed (3-month / extended).". In the list, the row appears in red.
- The task **Whistleblowing: recompute overdue flags**, every 15 minutes, recalculates which reports have an expired deadline. The filters **Overdue acknowledgement** and **Overdue closure** gather them.
- The task **Whistleblowing: deadline reminders**, every hour, creates one activity per report and expired deadline on the channel form, for the user of its System Manager. The activity carries the reference and the link to the report, and it is not repeated while the report stays open.

- For reports on the hosted page, FlexigoTech Cloud also writes to the channel's notifications email on day 5 if there is no acknowledgement, and 14 days before the response deadline ends. The email carries the channel, the reference and the date, nothing from the report.
- **Answer deadline (hosted channel)** shows the response date held by FlexigoTech Cloud. The cloud always counts it from receipt: with a profile other than Spain, it may not match **Closure Deadline**.

Requesting the extension

1. **Press Extend deadline**
   It is in the report header while the report is not closed, purged or retained anonymised. The **Motivated Extension** wizard opens.

2. **Choose the new date**
   New Deadline is set to 6 months from receipt, the maximum the module accepts. You may enter an earlier date.

3. **Write the reason**
   The reason goes in the **Justification (mandatory, min 30 chars)** group and needs at least 30 characters; otherwise Odoo warns with "Extension justification must be at least 30 characters (legal requirement).". It is stored encrypted.

4. **Press Apply Extension**
   The date goes to **Extended Deadline** and the extension is recorded in the **Extensions** tab, with who decided it and when. The register notes an **Extended** entry, the informant receives a message on the hosted page and, if they gave their email, an email notice.

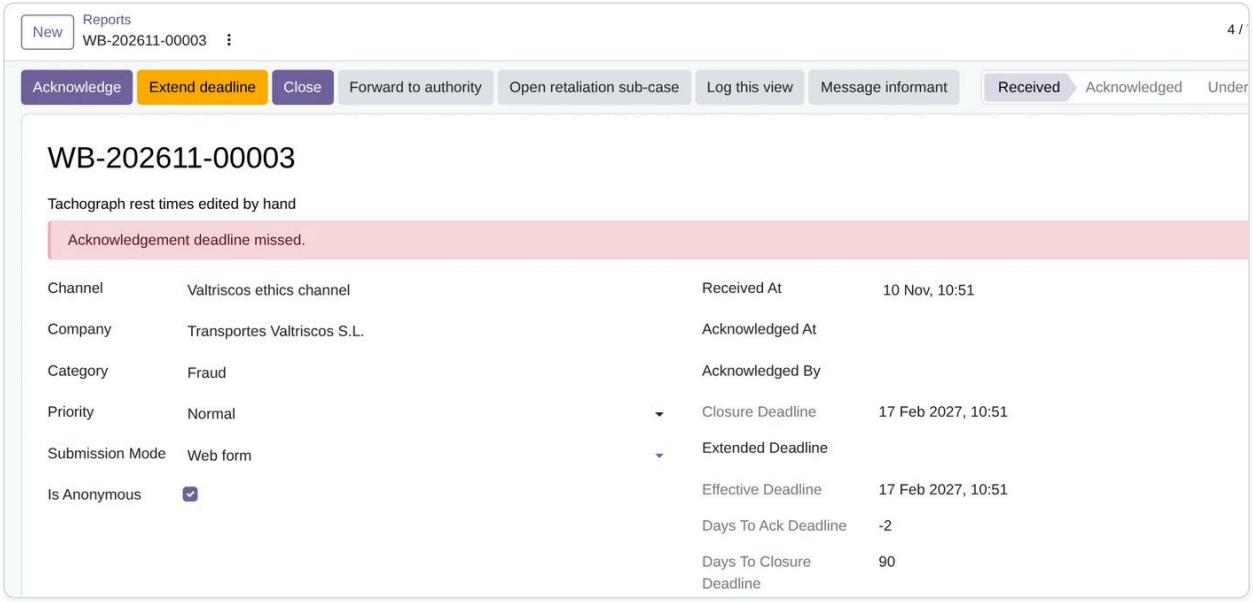
> Only one extension per report is allowed: the second gives "This report already has its motivated extension...". A date more than 6 months after receipt gives "Extension cannot push the deadline beyond 6 months from receipt (Ley 2/2023 art. 9.2.d).". Ley 2/2023 art. 9.2.d only allows extending in cases of special complexity, by up to another three months; deciding whether to extend is a matter for the Responsable.

What the law says

Law 2/2023 art. 9.2.c requires acknowledgement of receipt within seven calendar days of receipt, unless it would jeopardise the confidentiality of the communication. Art. 9.2.d sets the response at three months at most from receipt or, if there was no acknowledgement, from when those seven days expire, and allows extending it by a further three months in cases of particular complexity. Directive (EU) 2019/1937 art. 9.1.b and 9.1.f require acknowledgement within seven days and a response within three months from the acknowledgement, or from the seven days if there was none; for internal channels it provides no extension.

An example

Report WB-202611-00003, about tachograph rest times, came in more than a week ago and nobody has acknowledged receipt. Its record shows "Acknowledgement deadline missed.", **Days To Ack Deadline** is negative and on the board its card says **Ack overdue**. As there is no acknowledgement, its answer date is the date of receipt plus 7 days plus 3 months.



- **Real Odoo 20 screenshot.** Report WB-202611-00003, with the acknowledgement overdue.

MODULE GUIDE · WHISTLEBLOWING

10 Talking to the informant

The law provides for keeping communication with the informant open and, if considered necessary, asking them for additional information (Law 2/2023 art. 9.2.e). The secure thread is where this is done in this module.

Where each piece of data comes from

Messages from the informant and their attachments	They arrive with the scheduled task **Whistleblowing: hosted channel (FlexigoTech Cloud)**, which runs every 10 minutes and collects what the informant has written on the hosted page.
Messages from the company	You write them yourself from the report with **Message informant**, or the module sends them on its own when acknowledging receipt, extending the deadline and closing the report.

Register buttons

Message informant	Opens the wizard of the same name, with the **Body** field. With **Send**, the message is added to the thread and goes out to the hosted page; with **Cancel** it closes without sending anything. If you send it empty, Odoo shows "Reply body is required." Only the System Manager sees it.

How each message travels

Each message for the informant is sealed for them and goes out to FlexigoTech Cloud on the next collection. The **Hosted channel** column of the **Secure thread (informant)** tab shows how it is going: **Pending** while the cloud has not received it, **Sent** once it has accepted it, and **Not accepted** if it has rejected it. If the cloud does not respond, it stays **Pending** and is tried again at the next collection. The informant reads it on the hosted page with their tracking code.

Meetings

The **Meetings** tab is only a list, with the date each meeting was requested and the date it took place. The hosted page does not offer requesting in-person meetings, the module books nothing in the Odoo Calendar, and there is no screen to record or transcribe a verbal communication.

> A verbal report cannot be typed by hand into the module: reports with text come in through the hosted page, and in a report created by hand the subject and the description of the facts are read-only.

What the law requires and what the module provides

Law 2/2023 art. 9.2.e provides for keeping communication with the informant and, if needed, asking them for additional information. That communication is done through the secure thread of each report. The law also admits verbal communication and, at the informant's request, an in-person meeting within a maximum of seven days (Law 2/2023 art. 7.2). The module covers the written thread. For meetings it only keeps a list with their dates.

Rules and conditions

- The message cannot be empty: if you send it without text, Odoo responds "Reply body is required."
- If the informant gave their email, the module also sends them, from your Odoo, an email notice when acknowledging receipt, extending the deadline and closing. The emails carry the report's reference, not its content; the closure one adds the final status with its technical name, for example closed_founded. If they did not give an email, none is sent, and if sending fails, the report's cycle carries on unchanged.
- The informant replies with messages and attachments from the hosted page, using the 26-character tracking code that is shown to them only once when they submit. Their replies enter your Odoo with each 10-minute collection.
- The hosted page does not offer in-person meetings or reports of retaliation.

Register fields and tabs

Secure thread (informant)	Tab of the report with the message thread with the informant and the sending status of each one.
Meetings	Tab with the list of meetings: request date and the date it took place.

What it does not do

- It does not book meetings in the Odoo Calendar, nor does it offer to request them from the hosted page.
- It does not record or transcribe verbal communications, nor does it let you type up the text of a verbal report by hand.
- It does not make decisions for you, nor is it legal advice: what to ask the informant and when is decided by the Responsable del Sistema.

End-to-end example

Report WB-202611-00007, about inflated fuel invoices at a petrol station, arrives through the hosted page and enters your Odoo in **Received**, with the acknowledgement deadline running. The Responsable clicks **Acknowledge** and the informant sees the acknowledgement on the hosted page. They then open **Message informant**, note which documents they need and click **Send**. The message stays in **Pending** and moves to **Sent**

once FlexigoTech Cloud accepts it. The informant replies with a message and an attachment, and the next pickup places them in the **Secure thread (informant)** tab. If more time is needed, **Extend deadline** also sends the informant an extension message.

MODULE GUIDE · WHISTLEBLOWING

11 Who sees what: encryption, permissions and access logging

Law 2/2023 art. 32.1 limits access to the system's personal data to a closed list, within each person's functions: the Responsable del Sistema and whoever manages it directly, the head of human resources only where disciplinary measures may be needed, the head of legal services where legal measures are to be taken, the processors and the data protection officer. Directive (EU) 2019/1937 art. 16.1 requires that the identity of the reporting person not be disclosed, without their consent, to anyone other than authorised staff competent to receive or follow up reports. The module applies this through user groups, assigned investigators and per-case permissions.

On installation, the module gives none of its groups to anyone, not even the administrator. Until an administrator gives a user the Responsable del Sistema group on their Odoo user record, nobody sees the **Whistleblowing** menu and opening its lists gives an access error. Creating the Responsable del Sistema record with a user afterwards also gives them that group.

The Responsable del Sistema

It is created in **Whistleblowing › Configuration › Responsables**. It can be a person with an Odoo user or a collegiate body. Its designation and removal are decided by the entity's administrative or governing body (Ley 2/2023 art. 8.1); a collegiate body delegates the management of the system to one of its members (art. 8.2).

Kind	Person or collegiate body. A person needs a linked user; a collegiate body needs a name in **Name (collegiate body)**.
User	The person's Odoo user.
Appointment Date	Date of appointment. It cannot be in the future.
Revocation Date	Date of dismissal.
Notified To Aai, its date and Designation Attachment	In the **AAI notification** group: the checkbox and date of the notification, which the company marks by hand, and the designation document.
Revoke	Removes the Responsable: it deactivates the record, sets today's date in **Revocation Date** and removes the Responsable group from their user unless they are a Responsable for another company. The button is hidden when the record is no longer active.

> There can be only one active Responsable del Sistema per company. The module does not notify the Independent Authority for the Protection of Whistleblowers of the appointment or dismissal. Law 2/2023 art. 8.3 requires notifying them within ten working days; the company does this on its own and then ticks the checkbox.

Per-case permissions

Investigators see the reports in **Whistleblowing › Reports** where the Responsable has put them in **Assigned Investigators**, in the **Access grants** tab of the report. They do not see the text or the reporter's identity: the **Report content** tab is visible only to the Responsable.

HR and Legal get per-case permissions. In the same tab, the Responsable adds a line with the user, their role in **Role Scope** (**HR Director** or **Legal counsel**) and, if wanted, an expiry date in **Expires At**; to remove access, the Responsable enters a date in **Revoked At**. The user also needs the group **Whistleblowing / HR Director (per-case)** or **Whistleblowing / Legal counsel (per-case)**. The permission does not include the report content or the reporter's identity, and the module gives no menu to those two groups. The other two roles in the list, **Investigator** and **DPO audit**, do not grant access on their own.

A daily task switches off expired permissions. A permission cannot be moved to another case or to another user: it is revoked and a new one is granted. Who granted it and when is recorded.

What is encrypted and what cannot be changed

The facts, the informant's name and email, the outcome, the measures, the reason for an extension, the messages and the internal notes are stored encrypted (AES-GCM) with a key per company. Attachments are not encrypted: they are stored as Odoo attachments.

> If you rename the company after receiving reports, the reports already stored can no longer be read: each company's key depends on its name. Do not rename it. If you need to, write to comercial@flexigotech.com first and we will look at it with you.

The access log and the lifecycle events accept only additions: they cannot be modified or deleted. When you try, Odoo replies "The access log is append-only and cannot be modified.", "The access log is append-only and cannot be deleted.", "Lifecycle events are append-only and cannot be modified." or "Lifecycle events are append-only and cannot be deleted.".

Log this view, in the report header, records in the access log that you have read its content. The access log only records that and GDPR access requests: opening a report is not logged automatically.

> Neither investigators, HR nor Legal can see the reporter's identity: the **Report content** tab is visible only to the System Responsable. The Data Protection Officer cannot see it either: their DSAR assistant decrypts it to find the reports belonging to whoever requests their data and, for closed reports, puts it in the ZIP.

States of the Responsable del Sistema

- Active: it is the current Responsable for the company. Only one can be active per company.
- Dismissed: after clicking **Revoke**, the record is inactive, with today's date in **Revocation Date**, and the button stops showing.

Validity of a per-case permission

- Valid: it has not expired and has not been revoked.
- Expired: its **Expires At** date has passed. The daily scheduled task switches it off.
- Revoked: it has a date in **Revoked At** and no longer applies.

Rules and conditions

SITUATION	WHAT HAPPENS	WHY
You save a person-type Responsable without a user	"A person Responsable requires a linked user."	A person needs an Odoo user.
You save a collegiate-body Responsable without a name	"A collegiate Responsable requires a name."	A collegiate body is identified by its name.
You register a second active Responsable in the same company	"Only one active Responsable del Sistema per company is allowed."	Only one active per company.
You enter a future appointment date	"Appointment date cannot be in the future."	The appointment must already have taken place.
You try to change the case or the user of a permission	"A per-case access grant cannot be moved to another case or user: revoke it and grant a new one."	It is revoked and a new one is granted.
You try to modify or delete an entry in the access log or the events	"The access log is append-only..." or "Lifecycle events are append-only..."	They are add-only records.

What the access log records

The **Access log** tab of the report shows the date, user and action of each entry. Internally, each one is chained with a hash to the previous one. Entries are made when you click **Log this view** and when preparing a GDPR access request; opening the report is not logged automatically.

What the lifecycle events record

The **Events** tab shows the date, type and author of each event. Types include receipt, acknowledgement, triage, start of investigation, extension, closure, forwarding, purge, the informant's reply and reading of the content.

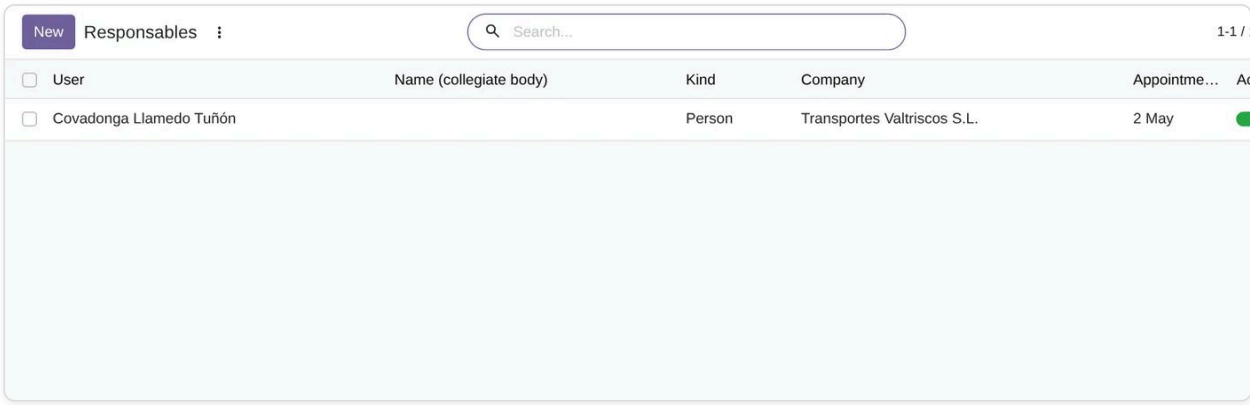
Responsable fields on screen

The Responsable record shows **Kind**, **User** or **Name (collegiate body)** depending on the type, **Company**, **Appointment Date**, **Revocation Date**, **Active** and the **AAI notification** group, with the designation document.

An end-to-end example

1. **Grant the group to the Responsable**
   An administrator opens the Odoo user record of Covadonga Llamedo Tuñón and gives them the **Whistleblowing / Responsable del Sistema** group. Until then nobody sees the **Whistleblowing** menu.

2. **Create the Responsable record**
   In **Whistleblowing › Configuration › Responsables** click **New**, choose the person type, link their user and enter the appointment date, which cannot be in the future.



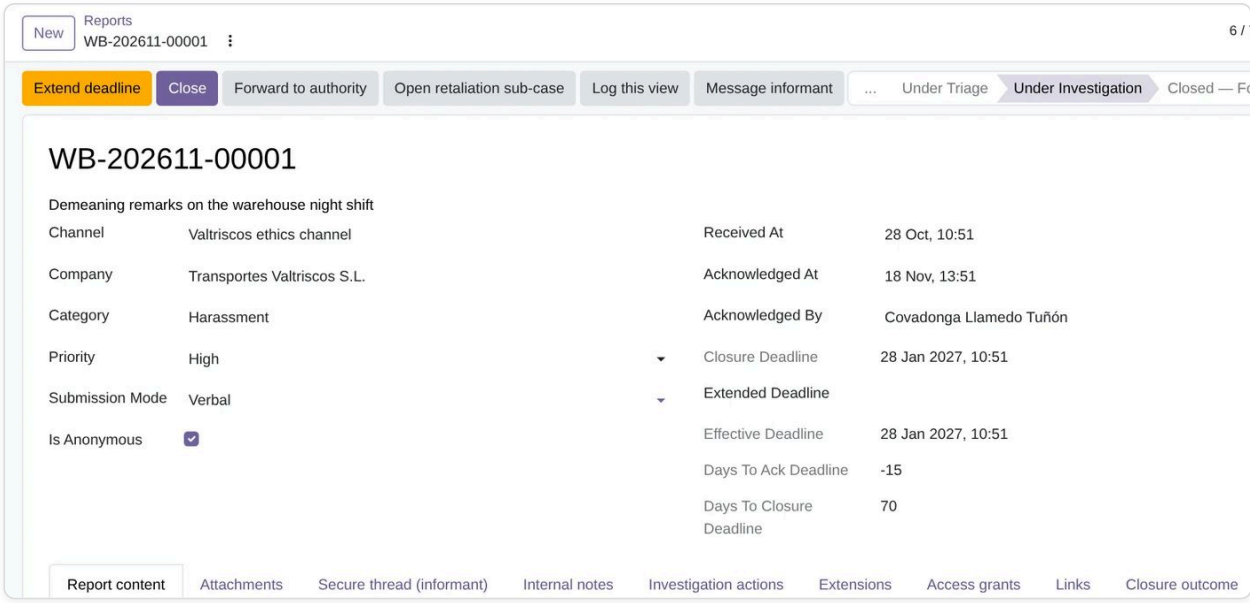
- **Real Odoo 20 screenshot.** The **Responsables** list with the Responsable of Transportes Valtriscos S.L.

3 Attach the designation and tick the notification

In the **AAI notification** group you attach the designation document. Once the company has notified the appointment to the Independent Authority for the Protection of Whistleblowers, you tick **Notified To Aai** and enter its date. The module does not make that notification.

4 Read a case and leave it recorded

Covadonga opens the report under investigation, WB-202611-00001, reads its content and clicks **Log this view**.



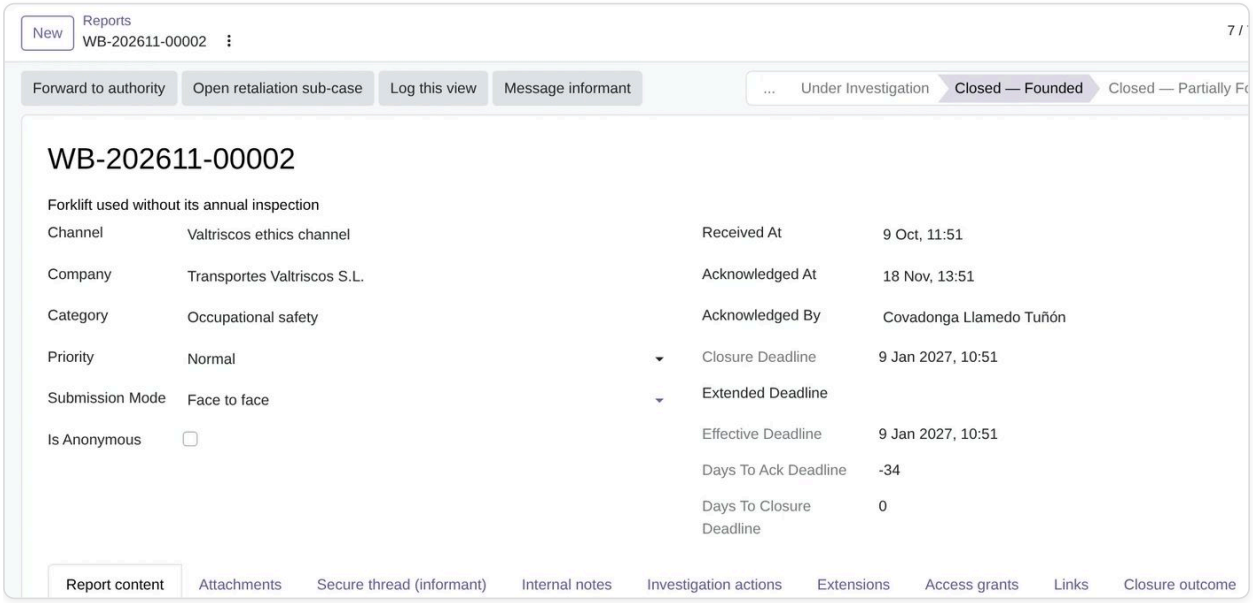
- **Real Odoo 20 screenshot.** Report WB-202611-00001 under investigation, with the buttons in the header.

5 Grant HR a per-case permission.

In the **Access grants** tab, add the HR director with the **HR Director** role and a date in **Expires At**. She also needs the group **Whistleblowing / HR Director (per-case)**. The daily task will switch the permission off on that date. If you chose the wrong case or user, you revoke it with **Revoked At** and grant another.

> The company decides who should have access to each case: Law 2/2023 art. 32.1 limits it to the people who need it for their functions.

12 Closing, forwarding and retaliation



- **Real Odoo 20 screenshot.** A report already closed, with the **Forward to authority** and **Open retaliation sub-case** buttons still visible.

Closing with Close

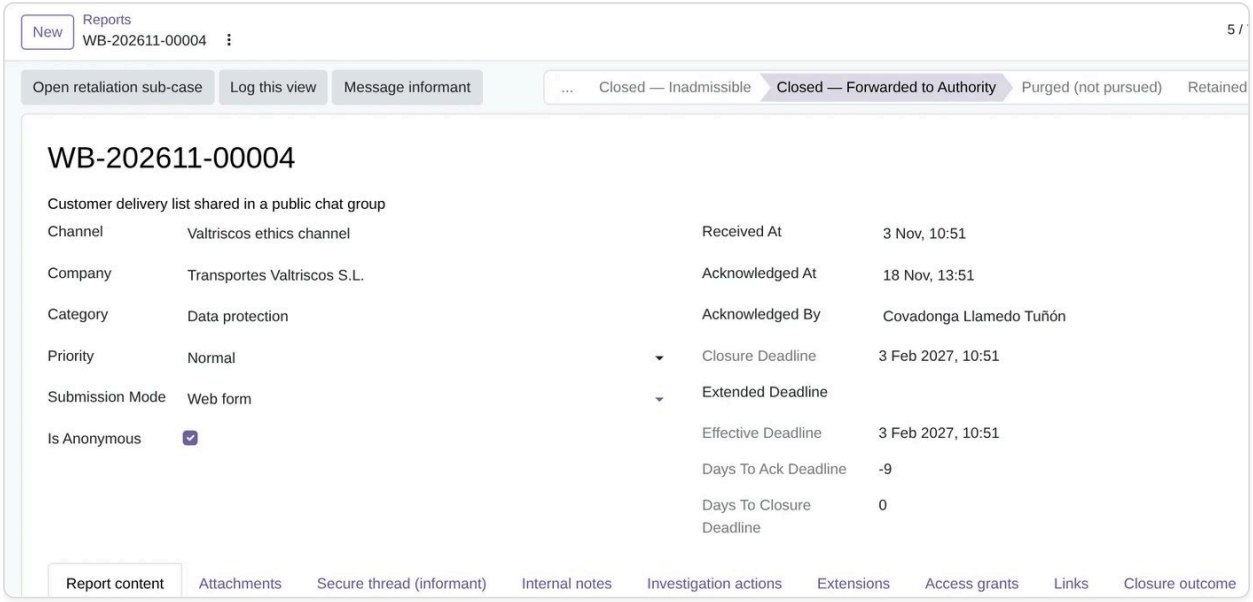
Click **Close** on the report and a wizard opens. The button is hidden when the report is already closed, purged or retained anonymised. In **Outcome State** you choose one of five outcomes: **Founded**, **Partially founded**, **Unfounded**, **Inadmissible** or **Forwarded to authority**. The default is **Unfounded**.

The wizard has two mandatory texts, those of the **Outcome** and **Measures summary** groups. Both are stored encrypted. If either is missing, Odoo warns "Outcome and measures summary are mandatory at closure." When the closure is applied, the informant receives a message with the outcome on the hosted page, the register book records an entry and, if the informant gave their email, a notice with the final status goes to them under its technical name (for example, closed_founded).

Apply Closure	Applies the chosen outcome and closes the report.
Cancel	Closes the wizard without touching the report.

Forwarding to an authority

Before clicking **Forward to authority**, choose the authority in **Forwarded To Authority**, in the **Closure outcome** tab of the report. Without an authority, Odoo replies "Select an external authority before forwarding." The button records the date, closes the report as forwarded and leaves the entry in the register book; it does not write to the informant. It is hidden on reports already forwarded, purged or retained anonymised.

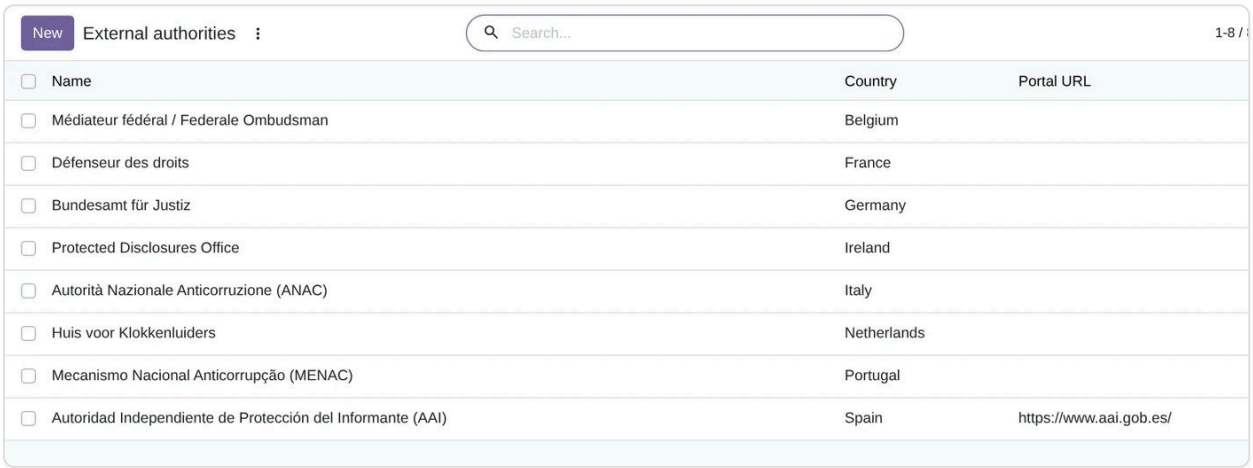


- **Real Odoo 20 screenshot.** A report closed as forwarded to the authority, with **Open retaliation sub-case** in the header.

> The module does not send anything to any authority. Sending is done by your company on its own. This includes the Public Prosecutor's Office, to which Law 2/2023 art. 9.2.j requires that facts which could indicatively be a crime be forwarded immediately.

External authorities

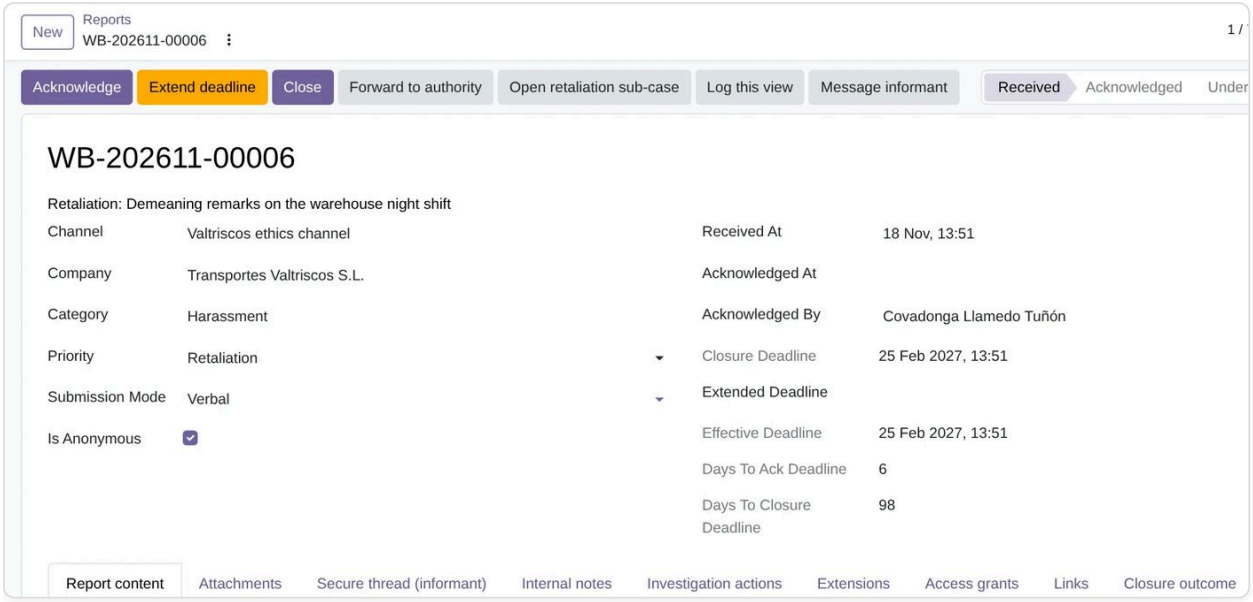
The module comes with 8 authorities, one per country profile: Spain, Portugal, France, Germany, Italy, Belgium, the Netherlands and Ireland. You can add others in **Whistleblowing › Configuration › External authorities**. For each one you store the name, the country and the address of its portal.



- **Real Odoo 20 screenshot.** The **External authorities** list with the 8 authorities the module ships with.

Retaliation sub-report

Open retaliation sub-case creates a new report, in **Received**, with priority **Retaliation**, its own reference and the same content. Its subject starts with the word Retaliation, and the register book records which report it came from; the record does not show a link between the two. The button is visible in any state. Law 2/2023 art. 36.1 prohibits retaliation against anyone who files a report.



- **Real Odoo 20 screenshot.** Sub-report WB-202611-00006, with priority **Retaliation**.

Closure outcomes

Founded	The Responsable del Sistema considers the facts proven.
Partially founded	The facts are proven only in part.
Unfounded	The facts are not proven.
Inadmissible	The report is not admitted for processing.
Forwarded to authority	The report is closed once you record which external authority your company forwards it to.
Purged (not pursued)	Status a report moves to when it is inadmissible or unfounded and the retention purge clears its content.
Retained anonymised	Status for closed reports whose informant data has already been erased.

Rules and error messages

- Outcome and measures: without both boxes filled in, Odoo shows "Outcome and measures summary are mandatory at closure."
- Forwarding: without an authority selected, Odoo shows "Select an external authority before forwarding."
- Protected data: anyone who is neither the System Responsable nor an Odoo administrator receives "Only the Responsable del Sistema can change the informant, the report text or the assigned investigators." if they try to change the informant, the text or the assigned investigators.

Report fields and tabs

Closed At and **Closed By**	The closure date and the user who applied it.
Forwarded To Authority, **Forwarded At** and **Forwarded Reference**	The authority chosen, the date the forwarding was recorded and the reference your company notes.
Closure outcome	The tab where those fields are.

Outcome (after closure) and **Measures (after closure)**	The two encrypted texts written in the wizard, in the **Report content** tab.
Events and **Access log**	Tabs showing what has happened on the report and the recorded reads.

Retention after closure

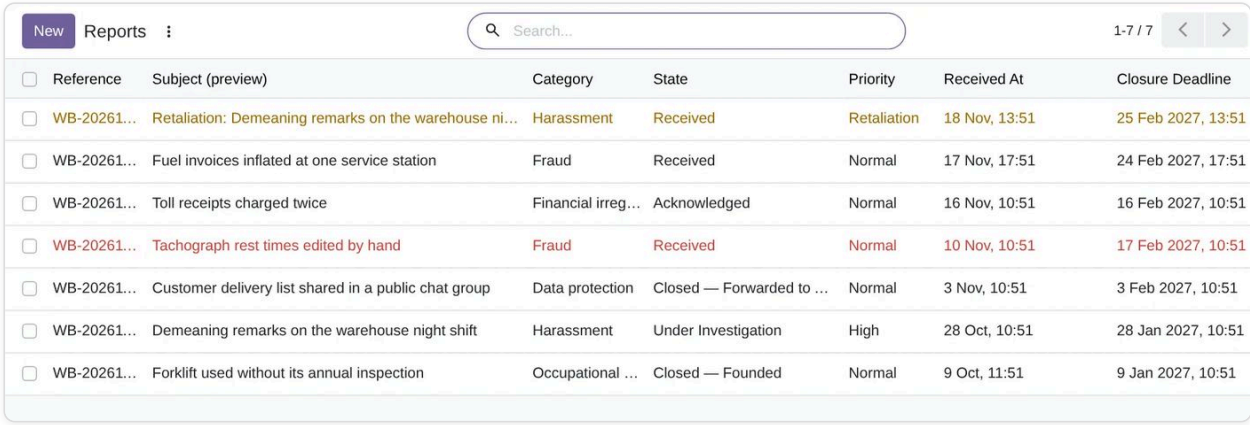
The **Whistleblowing: enforce retention** task runs every day. 90 days after closure, under the standard policy, it purges closed reports that were marked inadmissible or unfounded: it deletes the facts text, the informant's identity, the outcome, the measures, the attachments, the messages and the notes, and records the purge in the register. That period counts from closure. Spanish Law 2/2023 art. 32.4 counts three months from receipt for matters that were never investigated. So an open report that nobody investigates is not purged on its own.

10 years after closure, under the default policy, the same task erases the name, email and contact details of the informant on closed reports marked founded, partly founded, unfounded or forwarded. The facts text is not erased. It also anonymises register entries older than 10 years. Spanish Law 2/2023 art. 26.2 sets that ten-year limit.

End-to-end example

1 Open the report

In **Whistleblowing › Reports**, remove the **Open** filter to also see closed reports, and open WB-202611-00002, the forklift case without the annual inspection, in the Occupational safety category.



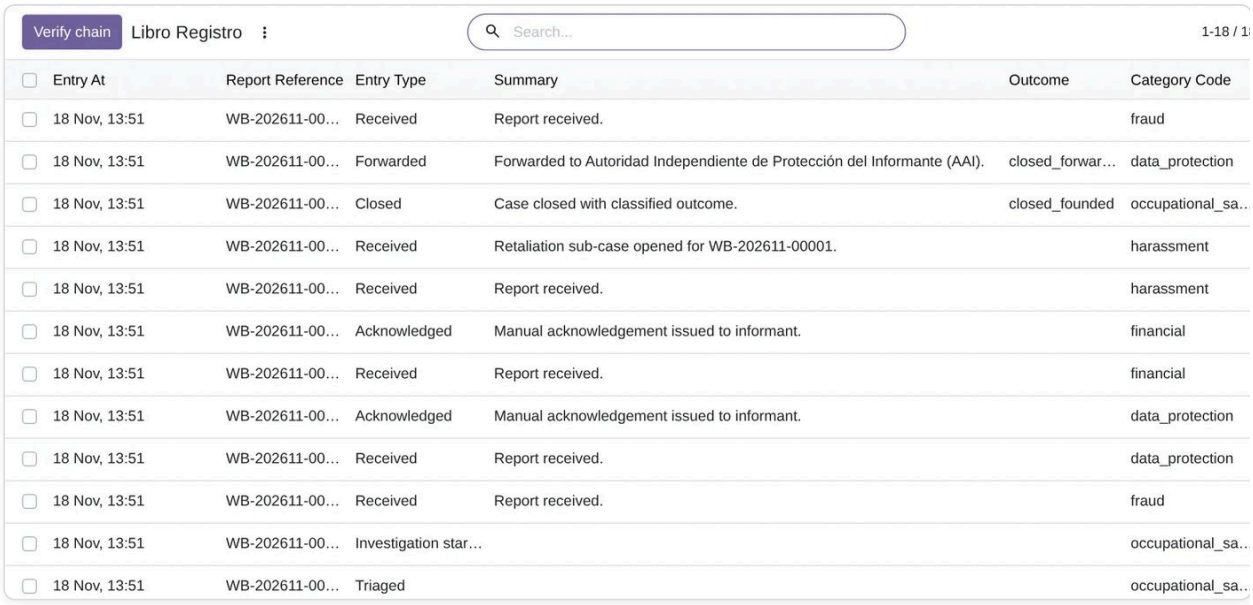
- **Real Odoo 20 screenshot.** The **Reports** list with the sample reports.

2 Close it with Close

In the wizard you choose **Founded**, write the outcome and the measures and click **Apply Closure**. The report is closed as founded, the informant receives a message on the hosted page, and the register records a **Closed** entry with the outcome closed_founded.

3 Check the register

In **Whistleblowing › Libro Registro** you will find that entry, with its summary and the outcome closed_founded.



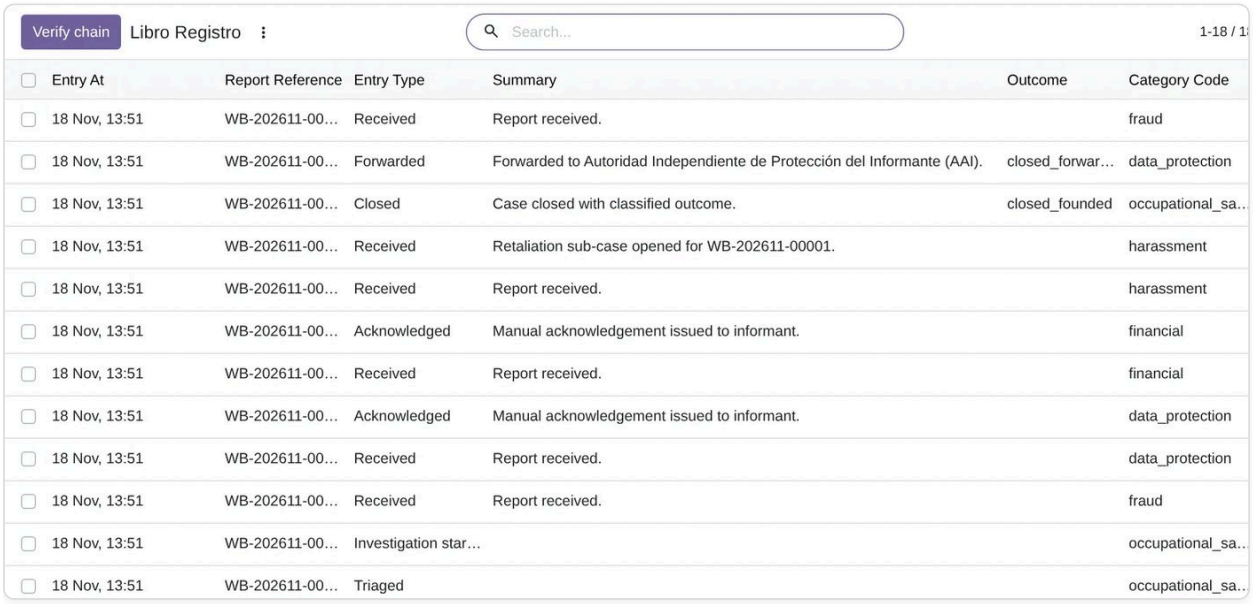
- **Real Odoo 20 screenshot.** The register with the entries from the sample reports.

4 **Forward another report**

In WB-202611-00004, the one about the delivery list shared in a public chat, choose the authority in **Forwarded To Authority** (tab **Closure outcome**) and click **Forward to authority**. The report is closed as forwarded, and the register records that it was forwarded to the Autoridad Independiente de Protección del Informante (AAI). Your company is the one that sends it to the authority.

MODULE GUIDE · WHISTLEBLOWING

13 The register and the audit pack



- **Real Odoo 20 screenshot.** The register list with the chain verification button at the top.

The register

The menu is **Whistleblowing › Libro Registro**. It is the register of reports received and internal investigations required by Spanish Law 2/2023 art. 26.1; Directive (EU) 2019/1937 art. 18.1 calls it the register of reports. Each

entry stores the date and time, the report reference, the type, a summary, the outcome, the category code and whether it is anonymised; it does not store informant data. The entry types the module writes are **Received**, **Acknowledged**, **Triaged**, **Investigation started**, **Extended**, **Closed**, **Forwarded**, **Purged** and **Retention deletion**.

The register only accepts new entries. If you try to modify or delete one, Odoo replies "The libro-registro is append-only and cannot be modified." or "The libro-registro is append-only and cannot be deleted." The only exception is retention, which anonymises entries older than the years in its policy.

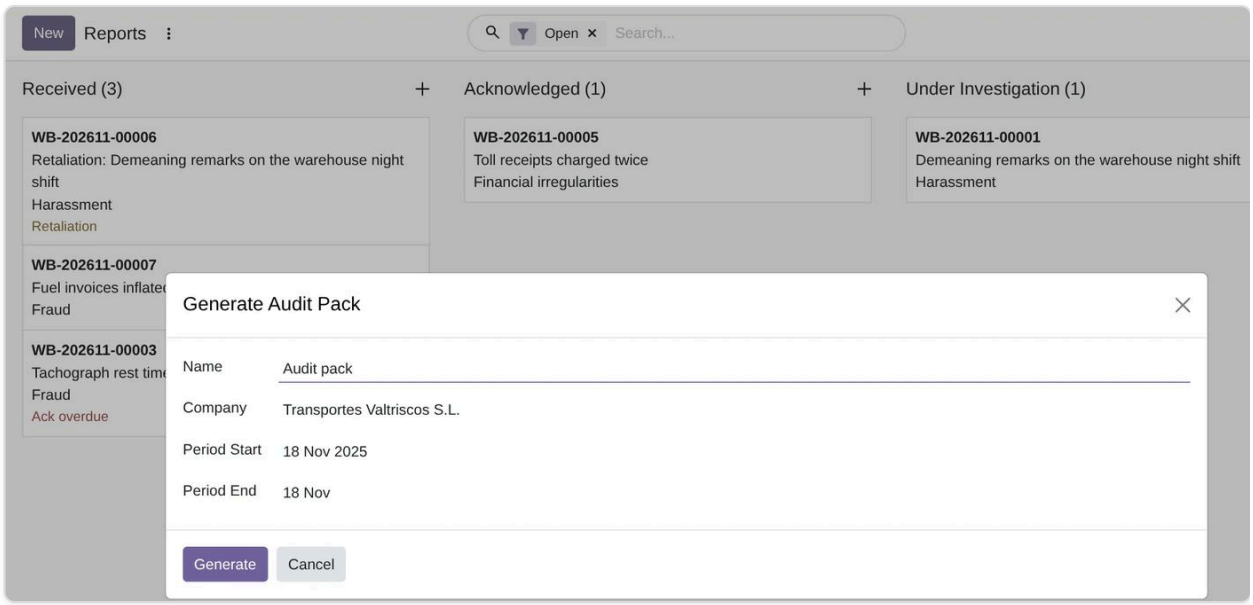
Verifying the chain

Each entry carries a SHA-256 hash chained to the previous one of its company. **Verify chain**, at the top of the list, walks the chain of each company you work in. If everything matches, Odoo reports "Libro-registro: chain intact". If someone changed the reference, type, summary, outcome or category code of an entry outside Odoo, it reports "Libro-registro: chain broken" and says which is the first entry that does not match.

The audit pack

1. ### Open the wizard

   Go to **Whistleblowing › Audit Packs › Generate Audit Pack**.



- **Real Odoo 20 screenshot.** The **Generate Audit Pack** wizard, with the proposed period.

2. ### Set the period

   Fill in **Period Start** and **Period End**. By default they cover the last year up to today. You can change the **Name** and the **Company**.

3. ### Click Generate

   Odoo creates the pack and opens its record, with its status, who generated it and when, and the ZIP in **Pack Attachment**. Odoo also stores its SHA-256 hash. Packs are listed in **Whistleblowing › Audit Packs**.

Generate Audit Pack	Wizard that asks for the period, the company and the name, and generates the pack.
Generate now	Button on a pack's record. It hides when the pack is ready.
Verify chain	Button on the register list. It checks the hash chain.

What the pack contains and where its documents come from

The ZIP contains the register for the period in CSV and PDF, the access log and the retention run log, statistics without personal data, the documents appointing the controller and a README.

Policies and privacy notices are maintained in **Whistleblowing › Configuration › Policy documents** and **Whistleblowing › Configuration › Privacy notices**: each has a name, version, effective date, company and text, and its status is **Draft**, **Published** or **Superseded**. **Publish** only appears on a draft, and **Supersede** on a published document. The DPIA goes in **Whistleblowing › Configuration › DPIA artefacts**, with its version, date and who approved it; its status is **Draft**, **Approved** or **Superseded**, and **Approve** only appears on a draft.

> The register cannot be edited or deleted from Odoo: a mistaken entry stays as it is. When retention anonymises entries older than the years in the policy, it changes their summary and reference, and **Verify chain** will flag them as changed outside Odoo.

Statuses and entry types

The audit pack has three statuses: **Generating** while it is being built, **Ready** when it is done, at which point **Generate now** disappears, and **Failed** if generation failed, with **Generate now** available to retry it.

With **Publish**, a policy or privacy notice moves from **Draft** to **Published**; with **Supersede**, from **Published** to **Superseded**. With **Approve**, the DPIA moves from **Draft** to **Approved** and records who approved it.

Rules and conditions

- The register cannot be modified or deleted from Odoo. The error messages are "The libro-registro is append-only and cannot be modified." and "The libro-registro is append-only and cannot be deleted."
- The exception is retention, which anonymises the summary and reference of entries older than the years in its policy.
- **Verify chain** walks the chain company by company and points to the first entry that does not match.
- **Publish** only appears on a draft and **Supersede** on a published document. **Approve** only appears on a draft DPIA.
- **Generate now** hides when the pack is ready.

Register retention periods

Spanish Law 2/2023 art. 26.2 says the personal data in the register is kept only for as long as necessary and proportionate, and never more than ten years. Art. 32.4 requires that communications without an investigation started be deleted three months after receipt, and those not processed may only be kept anonymised. Retention policies are maintained in **Whistleblowing › Configuration › Retention policies**. When you talk about the purge, there are two different counts: the module counts from the closure of the report, while the law counts three months from receipt of what was not investigated.

Register fields and tabs

Company	The company the entry belongs to.
Entry At	The date and time of the entry.
Report Reference	The reference of the report it refers to.

Entry Type	The type of entry.
Summary and Outcome	A summary of what happened and the outcome, if there is one.
Category Code	The code of the infringement category.
Anonymised	Whether retention has already anonymised the entry.

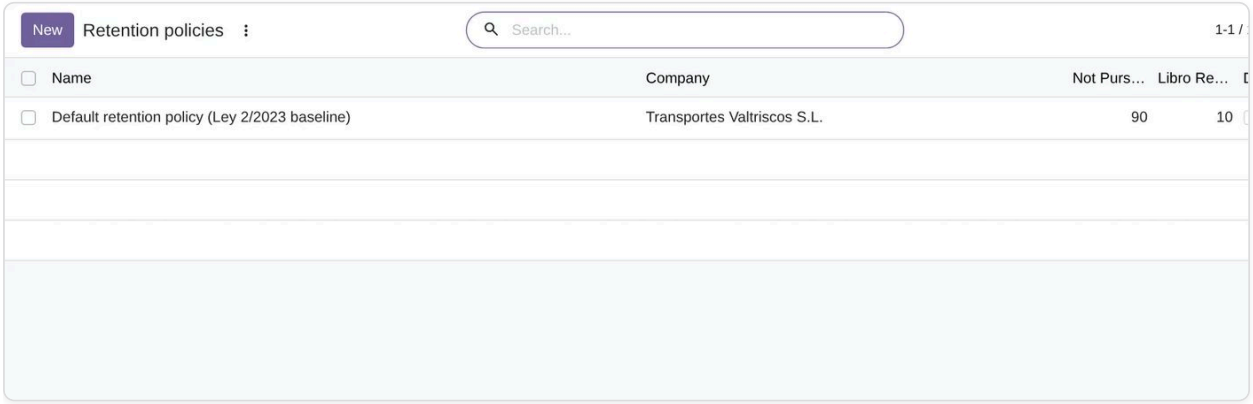
The forms have a group with the text: **Policy body** on policies, **Notice body** on notices and **DPIA body** on the DPIA.

End-to-end example

When you open **Whistleblowing › Libro Registro**, 18 entries appear. One of type **Received**, for WB-202611-00007, has the summary "Report received.". Another of type **Forwarded**, for WB-202611-00004, carries the outcome closed_forwarded and, in the summary, the name of the authority. There is also a **Closed** entry for WB-202611-00002, with the outcome closed_founded, and a **Received** entry for WB-202611-00006, the retaliation sub-report of WB-202611-00001. You click **Verify chain** to check the chain. Then you open **Whistleblowing › Audit Packs › Generate Audit Pack**, keep the period it suggests, the last year up to today, and click **Generate**. The pack appears in **Whistleblowing › Audit Packs** with its ZIP.

MODULE GUIDE · WHISTLEBLOWING

14 Retention, data subject requests and import



- **Real Odoo 20 screenshot.** The list of retention policies with the company's default policy.

The retention policy

You find it in **Whistleblowing › Configuration › Retention policies**. A default policy comes with the installation. The scheduled task **Whistleblowing: enforce retention** runs every day and applies it.

Name	The name of the policy.
Company	The company it applies to.
Not Pursued Purge Days	Days after closure after which a report closed as inadmissible or unfounded is purged. The default is 90 and the allowed range is 1 to 90.
Libro Registro Retention Years	Years after closure after which the informant's data is erased, and years after which register entries are anonymised. The default is 10 and the allowed range is 1 to 10.

Dry Run	Checkbox for test mode: the task counts what it would delete but deletes nothing.

What is purged and what is kept

90 days after a report closed as inadmissible or unfounded, the task deletes the facts text, the informant's identity, the outcome and measures, the attachments, the messages, the notes and the case key. The report moves to **Purged (not pursued)** and the register records the purge. Spanish Law 2/2023 art. 32.4 counts differently: three months from receipt for matters that were not investigated. The module counts from closure, so an open report that nobody investigates is not purged on its own.

10 years after closure, the task erases the name, email and contact details of the informant on closed reports marked founded, partly founded, unfounded or forwarded, and moves them to **Retained anonymised**. The facts text is not erased. It also anonymises register entries older than 10 years. Spanish Law 2/2023 art. 26.2 sets a maximum of ten years for keeping the personal data of reports and investigations.

With **Dry Run** on, the task deletes nothing: it only counts how many reports it would have purged or anonymised. Each run is logged with its date, its company and those counts. That log has no screen of its own: it goes into the audit pack.

GDPR access requests

They are handled from **Whistleblowing › Configuration › GDPR DSAR Assembly**.

1. **Identify the person**
   Enter their email in **Subject email** or their name in **Subject name**. At least one of the two is required.

2. **Choose how you verify their identity**
   In **Verification Mode** choose **Verified email**, **Signed PDF** or **In-person ID check**. With **Verified email** you need the person's email. With **Signed PDF** or **In-person ID check**, record the proof in **Verification Note**.

3. **Click** Assemble DSAR
   The wizard reviews the company's reports, decrypts the whistleblower's data, searches for matches with the person and prepares a ZIP with the data found, the list of what has been redacted and a README. In the **Result** group you see **Result Attachment** and **Matched Report Count**. The request is logged in the access register of each report that matches.

If the request is for erasure, tick **Right-to-be-forgotten request (art. 17)**. The ZIP then includes a refusal letter based on the retention obligation in Ley 2/2023 art. 32. Review the letter before sending it: the module does not provide legal advice.

> Only the Controller and the Data Protection Officer can see the wizard, and only for their own companies. With another company, Odoo shows "You can only answer data subject requests of your own companies."

Importing reports from another tool

Whistleblowing › Configuration › Import legacy reports reads a CSV with three columns: the subject (subject or title), whether it is anonymous (anonymous) and the date received (received_at). Each row creates a report in **Received** in the **Channel** you choose, with its original received date: if it is more than 7 days old, it appears with the acknowledgement already overdue. Each import is recorded as a batch in **Whistleblowing › Configuration › Import batches**, as **Done** or, if any row failed, as **Failed**, with the number of errors.

The **Vendor** you choose (Whispli, EQS Integrity Line, WhistleB, Whistlelink, FaceUp, SpeakUp or other) is only recorded; it does not change how the file is read. The facts text, the whistleblower's identity, the status, the messages and the attachments are not imported.

> The purge only acts on reports closed as inadmissible or unfounded. An open report is not purged. The module's deadlines are counted in calendar days, excluding public holidays.

Deadlines and their limits

The policy accepts between 1 and 90 days for not-pursued or unfounded reports and between 1 and 10 years for the register book. Odoo does not let you save values outside those ranges and shows "Not-pursued purge days must be between 1 and 90 (Ley 2/2023 art. 32 cap)." or "Libro-registro retention must be between 1 and 10 years (Ley 2/2023 art. 26.2 cap)."

The module counts the 90 days from closure. The law (Ley 2/2023 art. 32.4) refers to three months from receipt for matters not investigated. These are two different counts, and a report that nobody investigates and stays open is not purged automatically. The ten-year period for the register book comes from Ley 2/2023 art. 26.2.

What the daily task does, step by step

- Once the policy's days have passed since closure, it purges reports closed as inadmissible or unfounded: it deletes the facts text, the whistleblower's identity, the outcome, the measures, the attachments, the messages and the notes, and records the purge in the register book.
- Once the policy's years have passed since closure, it deletes the whistleblower's name, email and contact details on reports closed as founded, partly founded, unfounded or referred, but keeps the facts text.
- It anonymises the register book entries older than those years.

Dry-run mode and execution log

With the dry-run checkbox (**Dry Run**) ticked, the task only counts what it would delete. Use it to see the effect before letting it delete. Each run's log records when it ran, for which company, whether it was a dry run, how many reports it purged and how many it anonymised, how many register book entries it anonymised, and the text of any error. It has no screen: it is included in the audit package.

GDPR access request: rules and conditions

SITUATION	WHAT HAPPENS
You fill in neither email nor name	Odoo shows "Provide at least an email or a name."
Email verification mode without the person's email	Odoo shows "Email verification mode requires the subject email."
Verification by signed PDF or in-person check, without a note	Odoo shows "Document the verification proof in the verification note."
A company that is not yours	Odoo shows "You can only answer data subject requests of your own companies."

If you tick the art. 17 checkbox, the wizard produces a refusal letter citing the retention obligation in Ley 2/2023 art. 32.

Importing from another tool

- The wizard reads the subject, whether it is anonymous and the date received.
- Each report is placed in **Received** in the chosen channel, with its original date: if it is more than 7 days old, it appears with the acknowledgement already overdue.
- The batch is recorded with its status and the number of errors.
- If it fails completely, Odoo shows "Import failed: ...", with the reason for the failure in place of %s.

An end-to-end example

In the sample data, the company Transportes Valtriscos S.L. has a default policy with 90 days and 10 years. A person requests access to their data. You open **GDPR DSAR Assembly**, enter their email, leave the verification mode as email and click **Assemble DSAR**. The wizard goes through the reports, decrypts the whistleblower's data and counts the matches in **Matched Report Count**. The ZIP is left in **Result Attachment**. If the same person also asks for their data to be erased, you tick the art. 17 box and click **Assemble DSAR** again to get the refusal letter.

MODULE GUIDE · WHISTLEBLOWING

15 The data that goes out and comes back

DATA	DIRECTION	WHEN
Identification of the database	Your Odoo to FlexigoTech Cloud	When the database is connected to FlexigoTech Cloud.
Request for service permission	Your Odoo to FlexigoTech Cloud	When the hosted channel is activated from the wizard's **Hosted channel (FlexigoTech Cloud)** button.
Channel settings: the database's public key, the page address, the channel's categories and languages, the address of the legal texts, the company's country, the notification email and other channels	Your Odoo to FlexigoTech Cloud	When the channel is activated.
Contract acceptance: who accepts, when and which version	Stays in your Odoo, on the hosted channel tab	When the hosted channel is activated with the acceptance checkbox.
Confirmation of what was collected	Your Odoo to FlexigoTech Cloud	In a pass after the one that saved the reports, never in the same pass.
Your messages to the whistleblower, sealed	Your Odoo to FlexigoTech Cloud	You write them with **Message informant** and they go out on the next collection.
Request for the deadlines	Your Odoo to FlexigoTech Cloud	On each collection.
Reports, attachments and whistleblower messages, sealed with your database's key	FlexigoTech Cloud to your Odoo	Your Odoo collects them every 10 minutes.

DATA	DIRECTION	WHEN
Deadlines	FlexigoTech Cloud to your Odoo	On each collection.

Your database's private key never leaves your Odoo. FlexigoTech Cloud cannot read what is sealed with the public key and only stores it until your Odoo confirms it has it. The hosted page does not store the IP address of the person reporting, either in the application or in its server log.

Stays only in your Odoo: the open encrypted reports, the internal notes, the register book, the access and event logs and the audit packages. The register book, the access log and the events cannot be modified or deleted.

MODULE GUIDE · WHISTLEBLOWING

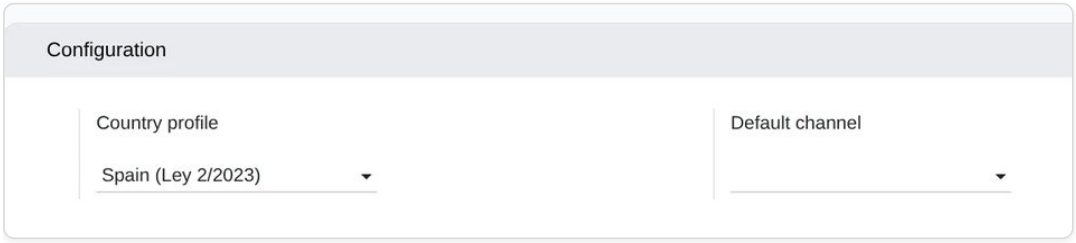
16 What happens automatically

TASK	FREQUENCY	WHAT IT DOES
Whistleblowing: hosted channel (FlexigoTech Cloud)	Every 10 minutes	Collects what has arrived at the hosted page, confirms what was collected in an earlier pass, sends the whistleblower the pending messages and reads the deadlines.
Whistleblowing: recompute overdue flags	Every 15 minutes	Recalculates which reports have an overdue acknowledgement or response deadline.
Whistleblowing: deadline reminders	Every hour	Creates one activity per overdue deadline for the System Manager, on the channel record. It does not repeat an identical one while it remains open.
Whistleblowing: enforce retention	Every day	Applies the retention policy: purges reports closed as inadmissible or unfounded and, once the policy's years have passed, deletes the whistleblower's data.
Whistleblowing: recompute per-case access validity	Every day	Switches off per-case permissions whose expiry date has passed.

All seven are active. The other two, which also start with Whistleblowing, have nothing to do on a new installation. To change a task's frequency, activate developer mode and go to **Settings › Technical › Automation › Scheduled Actions**. They are listed there under the English names you see here.

Separately from your Odoo, FlexigoTech Cloud monitors the deadlines of each report on the hosted page. It emails the channel's notification address on day 5 if there is no acknowledgement and 14 days before the end of the response deadline. The alert only carries the channel, the reference and the date, nothing from the content of the report.

17 The options and their defaults



- **Real Odoo 20 screenshot.** The **Whistleblowing** section of the settings, with its **Configuration** block.

OPTION	DEFAULT	WHAT IT DOES
Country profile (settings)	**Spain (Ley 2/2023)**	Only changes when the response deadline starts counting: with the Spain profile, from receipt; with any other, from the acknowledgement of receipt. No profile applies another country's law.
Default channel (settings)	Empty	Currently changes nothing: no part of the module uses it.
Anti-virus scanning (settings)	Off	With the box ticked and ClamAV installed on your Odoo server, attachments are scanned for viruses. Otherwise, they are left unscanned.
Accept Anonymous (channel)	On	Accepts anonymous reports. For a company in Spain it cannot be switched off (Ley 2/2023 art. 7.3).
Languages (channel)	Empty	The languages the channel passes to the hosted page. If you choose none, the language of whoever activates it is used.
Accepted Categories (channel)	Empty	The infringement categories the channel passes to the hosted page. They are maintained in **Whistleblowing › Configuration › Categories**.
Not Pursued Purge Days (retention policy)	90	Days from closure after which reports closed as inadmissible or unfounded are purged. Accepts 1 to 90.
Libro Registro Retention Years (retention policy)	10	Years from closure after which the informant's data is deleted, and years after which the register entries are anonymised. Accepts 1 to 10.
Dry Run (retention policy)	Off	Test mode: the retention task counts what it would delete and deletes nothing.

The acknowledgement and response deadlines are not adjusted: they are 7 days and 3 months (Spanish Law 2/2023 art. 9.2.c and 9.2.d). The extension can be requested once per report and the new date cannot go past 6 months from receipt. Days and months are calendar days and months, without public holidays.

What is done by hand

SCREEN	BUTTONS
The report	**Acknowledge** gives the acknowledgement of receipt. **Extend deadline** extends the deadline with a reason, once per report. **Close** closes with outcome and measures, both mandatory. **Forward to authority** asks you to choose the authority first, records the date, closes the report as forwarded to the authority and leaves the entry in the register; you send it yourself, on your own account. **Open retaliation sub-case** opens a sub-report for retaliation. **Log this view** records that you have opened the report. **Message informant** writes in the secure thread with the informant.

SCREEN	BUTTONS
The channel	**Publish** moves the channel to published. **Back to Draft** returns it to draft. **Archive** archives it. **Hosted channel (FlexigoTech Cloud)** opens the wizard that asks for consent before activating the hosted channel.
The register	**Verify chain** walks the chain of entries and warns you if it finds an inconsistency.
The wizards	**Generate Audit Pack** generates the ZIP audit pack for a period. **Import legacy reports** imports a CSV with the subject, whether it is anonymous and the receipt date of each report.

Log this view and **Message informant** are only visible to the Responsable del Sistema, and the hosted channel button only to an Odoo administrator. Until an administrator gives a user the Responsable del Sistema group on their user record, nobody sees the **Whistleblowing** menu.

18 Security and personal data

- The module has seven user groups: Responsable del Sistema, Investigator, HR Director (per-case), Legal counsel (per-case), Data Protection Officer, External auditor and Board dashboard. Spanish Law 2/2023 art. 32.1 limits access to personal data to a closed list of people, within their functions.
- On installation, the module gives no group to anyone, including the administrator. Until an administrator gives a user the Responsable del Sistema group, nobody sees the **Whistleblowing** menu and its lists show an access error.
- The facts, the informant's name and email, the outcome, the measures, the messages and the notes are stored encrypted with AES-GCM, with one key per company. Attachments are not encrypted.
- On screen, the content and the reporter's identity are visible only to the System Responsable. The Data Protection Officer cannot see them either: their DSAR assistant decrypts the identity to find the reports belonging to whoever requests their data.
- Investigators see only the reports they are assigned to. HR and Legal's per-case permission is limited to one report, does not include the reporter's identity and gives them no menu.
- The access log, the event log and the register cannot be changed or deleted from Odoo. Register entries are chained with SHA-256, and the verify-chain button checks it per company.
- Each company sees only its own reports, channels, responsables and register entries.
- Retention is automatic. A daily task purges the reports closed as inadmissible or unfounded once 90 days have passed since closure. Ley 2/2023 art. 32.4 counts three months from receipt for anything that was never investigated. At 10 years after closure, the same task deletes the whistleblower's data and anonymises the old entries in the register book.
- FlexigoTech Cloud cannot read the reports: the hosted page stores each one sealed with your database's public key until your Odoo confirms it has it, and the private key never leaves your Odoo.

19 Several companies and groups of companies

Each report, channel, responsable and register entry carries its company, and each user sees those of the companies they belong to. There can be only one active Responsable del Sistema per company: if you activate a second, Odoo warns with "Only one active Responsable del Sistema per company is allowed.". The encryption key is also one per company.

> If you rename the company after receiving reports, the reports already stored can no longer be read: each company's key depends on its name. Do not rename it. If you need to, write to comercial@flexigotech.com first and we will look at it with you.

In a group of companies you can share the channel with other companies from the channel itself. The other companies see the channel, not its reports. Spanish Law 2/2023 art. 11.2 allows a group of companies to have a single internal reporting system, and art. 12 allows private companies with between fifty and two hundred and forty-nine workers that so decide to share the system and the resources to handle reports. EU Directive 2019/1937 art. 8.6 allows those with between 50 and 249 workers to share resources for receiving reports and carrying out investigations. In all cases the confidentiality and reply-to-the-reporter obligations still apply.

A database has only one active hosted channel, even if it has several companies: activating it on one channel turns it off on the others. FlexigoTech Cloud offers the Standard plan at €29 a month or €290 a year and the Pro

plan at €58 a month or €580 a year, excluding VAT. The trial is 14 days free and requires no card.

20 If something goes wrong

You cannot see the Whistleblowing menu	On installation nobody has the module's groups. An administrator has to give you the **Whistleblowing / Responsable del Sistema** group on your user record.
The channel does not publish	This happens if the Responsable, the policy or the privacy notice is missing, or if your Odoo address is http. Complete what is missing on the channel record. For the address, set up https before publishing.
The hosted channel wizard rejects the address or asks you to accept	The page address accepts 3 to 40 lowercase letters, digits or hyphens, without the words flexigo or odoo, and it cannot be another company's. Also tick the acceptance box before activating.
A cycle button does not move forward	Each step requires coming from a specific state: acknowledging only from **Received**, moving to triage only from **Acknowledged**, and investigating from **Acknowledged** or **Under Triage**. Check the state of the report.
The deadline extension is rejected	It asks for a reason of at least 30 characters. Only one is granted per report, and the new date cannot go past 6 months from receipt.
The closure does not complete	You must fill in the outcome and the summary of the measures. Without both, Odoo does not close the report.
Forwarding to the authority does not proceed	First choose the authority on the **Closure outcome** tab and press **Forward to authority** again.
A second Responsable cannot be left active	Only one Responsable del Sistema can be active per company. Deactivate the previous one with **Revoke**.
Someone cannot see the content of a report	On screen, the text and the reporter's identity are visible only to the System Responsable, in the **Report content** tab. Investigators, HR and Legal cannot see them.

Warnings appear in English, as the module writes them, for example "Cannot publish a channel without a Responsable." or "Only reports in state 'Received' can be acknowledged.". If you see a warning that is not listed here, copy the full text before looking it up.

Other warnings you may see

"Only one active Responsable del Sistema per company is allowed."	Deactivate the previous Responsable of that company with **Revoke** or edit the one that is already active.
"Provide at least an email or a name."	In a GDPR access request, fill in at least the person's email or name.
"Email verification mode requires the subject email."	If you verify by email, enter the email of the person making the request.
"Document the verification proof in the verification note."	Note in the verification note how you checked the identity.
"Reply body is required."	Write the message to the informant before sending it.

"Select an external authority before forwarding."	Choose the authority on the report and forward again.
"Appointment date cannot be in the future."	Enter an appointment date of today or earlier.
"A per-case access grant cannot be moved to another case or user: revoke it and grant a new one."	Revoke the permission and grant a new one to the correct user or case.

MODULE GUIDE · WHISTLEBLOWING

21 Other ways of doing it

OPTION	WHAT IT INVOLVES
By hand: a mailbox or a spreadsheet	Acknowledgement and response deadlines are counted by hand, with no due-date alerts. The file, the messages and the attachments are spread across email and the case handler's files.
Odoo alone	Odoo 17, 18, 19 and 20 do not ship a whistleblowing channel as standard: no manifest for Odoo Community or Enterprise names "whistleblow" or "denuncia".
A separate whistleblowing platform	Another system and another account outside Odoo. The reports live there and what is done in Odoo has to be carried over by hand.
This module	The channel works inside Odoo. Reports come in through the FlexigoTech Cloud hosted page, anonymous or named, and your Odoo collects them every 10 minutes and stores them encrypted. Each report follows its cycle with buttons and deadlines (7 days for acknowledgement, 3 months for response, reasoned extension capped at 6 months from receipt), with warnings and activities for the Responsable del Sistema. It adds the secure thread with the informant, the chained register and the audit pack.

22 Plans and price

€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 annually, and the 14-day trial does not require a card.

23 Frequently asked questions

Does it work without FlexigoTech Cloud?

No.

Does it work on Odoo Online?

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

Does it need Odoo Enterprise?

No. Its dependencies (base, web, mail, website, portal, calendar and the FlexigoTech Cloud module) include no Enterprise module.

Which Odoo versions does it work on?

Odoo 17, 18, 19 and 20.

Who is obliged to have an internal channel?

Private-sector companies with fifty or more workers (Law 2/2023 art. 10.1.a; Directive (EU) 2019/1937 art. 8.3).

Does it accept anonymous reports?

Yes. In the hosted page the informant chooses between reporting anonymously or with a name and email. In a Spanish company, the option to accept anonymous reports cannot be unticked (Law 2/2023 art. 7.3).

How does a report reach my Odoo?

The informant sends it through the FlexigoTech Cloud hosted page. It arrives sealed and your Odoo collects it every 10 minutes with the **Whistleblowing: hosted channel (FlexigoTech Cloud)** task and stores it encrypted.

Can FlexigoTech read the reports?

No. Each report arrives sealed with your database's public key, and the private key never leaves your Odoo.

Does it store the whistleblower's IP address?

No. The hosted page does not store it, either in the application or in its server log. To curb abuse, it only uses an in-memory fingerprint of the IP that changes every day.

Which deadlines does it calculate, and where do they come from?

The acknowledgement of receipt, within seven calendar days (Law 2/2023 art. 9.2.c; Directive art. 9.1.b), and the response, within three months (Law 2/2023 art. 9.2.d; Directive art. 9.1.f). With the Spain profile the response period runs from receipt; with any other profile, from the acknowledgement.

How is the deadline extended, and up to when?

With the **Extend deadline** button: a reasoned extension for the report, of up to three further months (Law 2/2023 art. 9.2.d), never beyond 6 months from receipt. The justification must be at least 30 characters long.

What happens when a deadline expires?

The report form flags it in red, and the System Manager receives an activity on the channel form. Scheduled tasks recalculate expired deadlines every 15 minutes and create the activities every hour. For reports submitted through the hosted page, FlexigoTech Cloud also sends an email to the alerts address.

Which languages does the hosted page come in?

Spanish, English, Catalan, Portuguese, French or German, depending on the channel's languages. There is no Italian, Dutch or Polish.

How does the company communicate with the whistleblower?

Through the secure thread of each report: the message travels sealed to the hosted page. The whistleblower reads it with their tracking code and replies with messages and attachments.

Does it book in-person meetings?

No. The **Meetings** tab is only a list showing the request date and the date each meeting took place.

Can a verbal report be recorded?

The text of a verbal report cannot be typed in by hand. The module does not record or transcribe verbal communications either.

Who can read a report?

On screen, the text and the reporter's identity are visible only to the System Responsable; the DSAR assistant of the Data Protection Officer decrypts the identity to find the reports belonging to whoever requests their data. Neither the assigned investigators, nor HR, nor Legal can see them. Spanish Law 2/2023 art. 32.1 limits access to personal data to a closed list of persons.

How is access granted to HR or Legal?

With a per-case permission, in the **Access grants** tab of the report, with the role **HR Director** or **Legal counsel**, and with the per-case group of each. It can expire and be revoked, and it does not include the reporter's identity. Those two groups have no menu in the module.

Does it send the report to the authority?

No. **Forward to authority** records which authority you forwarded it to, closes the report as forwarded, and leaves the entry in the register book. You do the actual sending.

Does it notify the A.A.I. of the appointment of the System Manager?

No. The notification (Law 2/2023 art. 8.3) is made by the company, after which you tick the **Notified To Aai** box.

What is the register book, and how is it verified?

It is the register book under art. 26 of Law 2/2023. It only accepts new entries, and each one carries a chained SHA-256 hash. The **Verify chain** button walks through the chain and points to the first inconsistency.

What does the audit pack contain?

A ZIP for the period you choose, containing the register book in CSV and PDF, the access and retention logs, statistics without personal data, the System Manager's appointment documents, and a README. It is created with **Generate Audit Pack** and is kept under **Whistleblowing › Audit Packs**.

What does it delete automatically, and when?

At 90 days after closure it purges the inadmissible or unfounded reports. The law (art. 32.4) counts three months from receipt for anything that was not investigated, so an open report that nobody investigates does not purge itself. At 10 years it deletes the whistleblower's identity from the closed ones and anonymises the old register book (Ley 2/2023 art. 26.2).

How is a GDPR access request answered?

With **Whistleblowing › Configuration › GDPR DSAR Assembly**: you identify the person, choose how to verify their identity, and the wizard prepares a ZIP with what it finds.

Does it import reports from another tool?

From a CSV it imports only the subject, whether the report is anonymous, and the date of receipt. It does not import the facts text, the whistleblower's identity, the status, the messages or the attachments.

Does it work for a group of companies?

Yes: the channel can be shared with other companies. Law 2/2023 art. 12 and Directive art. 8.6 allow companies with between 50 and 249 employees to share resources.

Does it work outside Spain?

The country profile only changes the starting point of the response deadline: with the Spain profile, from receipt; with the others, from the acknowledgement of receipt, as in the Directive. The module does not apply other countries' national laws, and the hosted page has no Italian, Dutch or Polish.

Which languages do the screens come in?

Almost all screens are in English in every language, including Spanish.

Is it legal advice?

No. The module does not investigate or decide either: that is done by the System Manager.

MODULE GUIDE · WHISTLEBLOWING

24 Glossary

Internal reporting system	The set of channel, manager, procedure and records through which a company receives and processes reports. Law 2/2023 requires private-sector companies with fifty or more employees to have one (art. 10.1.a). Directive (EU) 2019/1937 requires it in its art. 8.3.
Internal channel	The route by which the whistleblower reports to the company itself. In this module it is the FlexigoTech Cloud hosted page.
External channel	The route for reporting to a public authority. The module only records which external authority you forwarded a report to, using **Forward to authority**.
System Manager	The person or collegiate body that manages reports. Appointed by the administrative body (Law 2/2023 art. 8.1).
Whistleblower	The person who makes the report, either named or anonymous.

Person concerned	The person named in the report. If the report gives their name, it appears in the facts text, which is stored encrypted.
Acknowledgement of receipt	The notice to the whistleblower that their report has been received. It must be given within seven calendar days of receipt (Law 2/2023 art. 9.2.c).
Response deadline	Three months to report on the actions taken. With the Spain profile it runs from receipt (Law 2/2023 art. 9.2.d). With any other profile, from the acknowledgement (Directive art. 9.1.f).
Reasoned extension	A justified extension of the response deadline, of up to three further months (Law 2/2023 art. 9.2.d). The module limits it to one per report and to 6 months from receipt.
Register book	The register of information received and internal investigations (Law 2/2023 art. 26.1). It only accepts new entries.
SHA-256 chain	The hash that links each register book entry to the previous one. **Verify chain** walks through it and points to the first inconsistency.
Audit pack	A ZIP generated for a period with **Generate Audit Pack**. Its hash is stored.
Retaliation	Any act causing detriment to the person who reports, which Law 2/2023 prohibits (art. 36.1). From a report you can open a retaliation sub-case with **Open retaliation sub-case**.
A.A.I.	The Independent Authority for Whistleblower Protection. The appointment of the System Manager must be notified to it (Law 2/2023 art. 8.3). The module does not notify it.
Data protection officer	The person who looks after personal data. They have their own group. They do not open the reports: their DSAR assistant decrypts the reporter's identity to find the reports of whoever requests their data.
Per-case permission	Access to one specific report for one specific user, with an optional expiry date and revocable at any time.
Access log	The record of each report's activity (who, when and what they did), which cannot be changed or deleted. It is written when **Log this view** is pressed and when a GDPR access request is prepared.
Purge	The deletion of the content of a report closed as inadmissible or unfounded 90 days after closure. The law (art. 32.4) counts three months from receipt for anything that was not investigated.
Anonymisation	The deletion of data that identifies the whistleblower in resolved reports, after the policy's number of years from closure (10 by default). Law 2/2023 art. 26.2 sets a maximum of ten years.
Hosted page	The public FlexigoTech Cloud page where the whistleblower submits their report. It is enabled from the channel.
Tracking code	A 26-character code that the page shows the whistleblower only once. With it they can read messages again and reply.
Seal	Encryption with your database's public key. FlexigoTech Cloud cannot read what is sealed: only your Odoo opens it.

25 Checklist and contact

- [ ] You have Odoo 17, 18, 19 or 20 on Odoo.sh or on your own server, with the Website app.
- [ ] You have installed the module.
- [ ] You have started the 14-day FlexigoTech Cloud trial, without a card.
- [ ] You have given the **Whistleblowing / Responsable del Sistema** group to whoever will be the System Manager, and created their record in **Whistleblowing › Configuration › Responsables**, with their appointment document.
- [ ] You have uploaded the channel policy and the privacy notice.
- [ ] You have published the channel with the **Publish** button. Your Odoo needs an https address.
- [ ] You have enabled the hosted page from the channel, with the **Hosted channel (FlexigoTech Cloud)** button.
- [ ] You have given the page's address to the staff.
- [ ] You have given the module's groups to whoever needs them.
- [ ] You have submitted a test report, seen it in **Whistleblowing › Reports**, and pressed **Acknowledge**.
- [ ] In **Whistleblowing › Libro Registro** you have clicked **Verify chain** and the chain checks out.

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. While you're subscribed, support for the service stays included.

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/canal-denuncias-odoo.html

On Odoo Apps

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

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