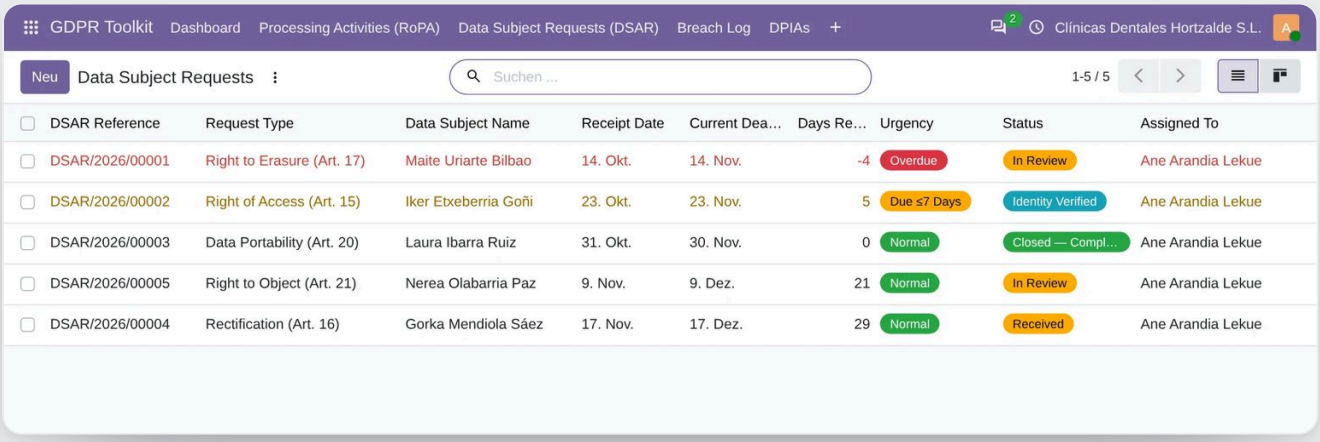
MODUL-LEITFADEN · DATENSCHUTZ

GDPR Compliance für Odoo

Das Verzeichnis der Verarbeitungstätigkeiten, die Anfragen mit ihrer Frist, die Verstöße mit ihren 72 Stunden und die DSFA, direkt in Odoo.

Odoo 17 · 18 · 19 · 20 | 14 Tage Testphase, ohne Karte | Ausgabe vom 19-11-2026





Echter Screenshot aus Odoo 20. Die Liste der Anfragen mit ihrer Frist und Dringlichkeit sowie eine Verletzung mit dem 72-Stunden-Countdown.

Inhalt

Rechts die Seite, auf der jedes Kapitel beginnt. Menüs und Schaltflächen heißen wie im deutschen Odoo. Die Menüs und Schaltflächen des Moduls selbst sind auf Englisch: Das Modul ist noch nicht ins Deutsche übersetzt.

1	Für wen es ist und was es löst	3
2	Das Modul in Zahlen	4
3	Wo Sie es in Ihrem Odoo sehen	5
4	Was Sie vor dem Start brauchen	6
5	Die Testphase von FlexigoTech Cloud	6
6	Schritt für Schritt einrichten	8
7	Das Verzeichnis der Verarbeitungstätigkeiten	10
8	Anträge betroffener Personen und ihre Fristen	14
9	Portabilität, Löschung und das Datenschutzportal	20
10	Das Vorfallregister und die 72 Stunden	23
11	Die Datenschutz-Folgenabschätzungen (DSFA)	26
12	Die Aufbewahrung und ihre Überprüfungen	30
13	Berichte, Exporte und Audit-Protokoll	34
14	Aufsichtsbehörden und Rechtsgrundlagen	37
15	Was an FlexigoTech Cloud geht und was zurückkommt	40
16	Was automatisch geschieht	41
17	Die Moduloptionen und ihre Voreinstellungen	42
18	Sicherheit und personenbezogene Daten	44
19	Mehrere Unternehmen	44
20	Wenn etwas schiefgeht	45
21	Andere Möglichkeiten	46
22	Tarife und Preis	47
23	Häufig gestellte Fragen	48
24	Glossar	51
25	Checkliste und Kontakt	53

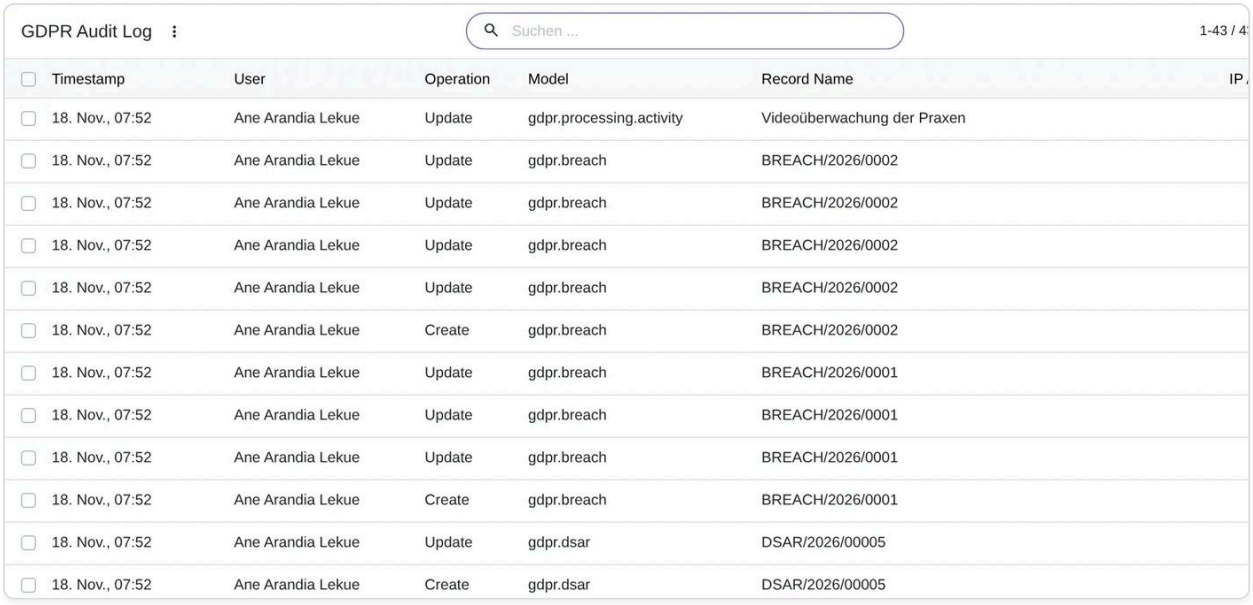
Dieser Leitfaden beschreibt Version 20.0.1.1.13 des Moduls (Odoo-Branch 20.0, Commit e15afc58d). Alles darin stammt aus dem veröffentlichten Code, aus der offiziellen Dokumentation der Plattform oder aus echten Screenshots.

Die Screenshots stammen aus einer Odoo-20-Testdatenbank mit erfundener Firma und erfundenen Daten, ohne echte Verbindung zu FlexigoTech Cloud. Das Modul gibt es auch für Odoo 17, 18 und 19.

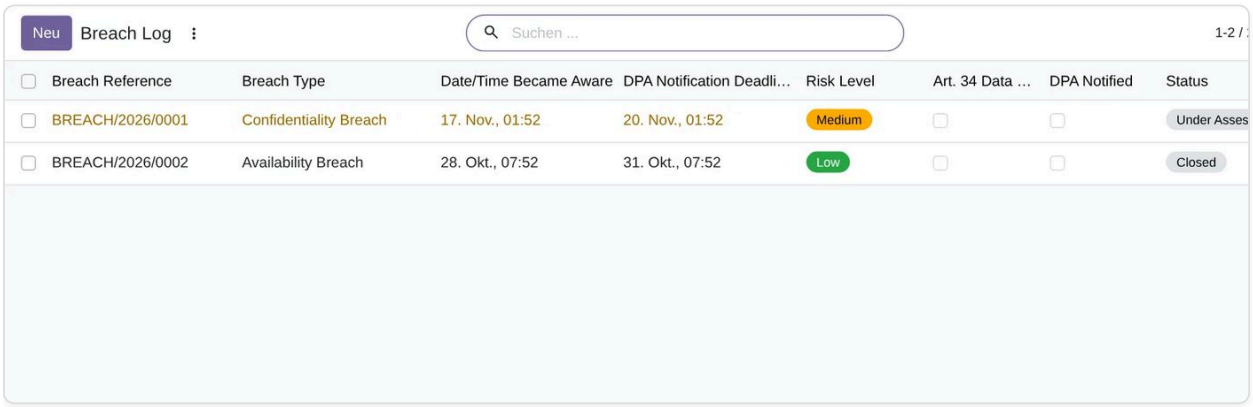
1 Für wen es ist und was es löst

Ohne das Modul liegt das Verzeichnis der Verarbeitungstätigkeiten meist in losen Tabellen. Die Fristen der Anfragen werden von Hand gezählt, und niemand wird rechtzeitig gewarnt, wenn sie näher rücken. Es gibt keine Historie darüber, wer was wann geändert hat. Bei einer Verletzung führt niemand Buch über die Stunden seit Kenntniserlangung.

Mit dem Modul ist all das in Odoo, mit sichtbaren Fristen und einem nicht veränderbaren Audit-Log.



- **Echter Screenshot aus Odoo 20.** Das **GDPR Audit Log** mit Datum, Benutzer und Vorgang jeder Änderung.



- **Echter Screenshot aus Odoo 20.** Die Liste **Breach Log** mit der 72-Stunden-Meldefrist jeder Verletzung.

Was sich im Alltag ändert

- Jede Verarbeitungstätigkeit wird mit ihren Zwecken, Rechtsgrundlagen, Datenkategorien und Betroffenenkategorien, Empfängern und Aufbewahrungsfrist erfasst, und jede Änderung wird in ihrem Verlauf gespeichert.
- Die Anfragen der Betroffenen haben eine Frist von einem Monat ab Eingang, mit einer Verlängerung um zwei weitere Monate, falls nötig, und begründet (Art. 12 Abs. 3). Es gibt Listen der überfälligen Anfragen und derer, die diese Woche fällig werden.
- Eine Verletzung beginnt 72 Stunden zu laufen, sobald Sie den Zeitpunkt der Kenntniserlangung erfassen (Art. 33 Abs. 1). In ihren letzten 6 Stunden warnt das Modul stündlich per E-Mail, solange Sie sie nicht als gemeldet markieren.

- Eine Tätigkeit, die zwei Kriterien der WP248-Leitlinien erfüllt, wird mit **DPIA Required** markiert, und das Modul lässt sie erst aktivieren, wenn eine genehmigte DSFA vorliegt. Die DSFA (Art. 35) hat fünf Schritte und markiert die vorherige Konsultation, wenn das Restrisiko es verlangt (Art. 36).
- Der Betroffene mit Portalkonto sendet seine Anfrage über /my/privacy-rights und erhält eine Eingangsbestätigung per E-Mail.

Was es nicht tut

- Es löscht oder anonymisiert keine Daten in Odoo. Die Löschprüfung zählt, was vorhanden ist, und hält Ihre Entscheidung fest; das Löschen oder Anonymisieren nehmen Sie selbst vor.
- Es meldet nichts an die Aufsichtsbehörde und informiert keine Betroffenen. Hier halten Sie fest, was Sie getan haben: den Status, Datum und Uhrzeit, die Methode und die Referenz.
- Es versendet das Antwortschreiben an den Betroffenen nicht. Sie verfassen es im Reiter der Antwort anhand einer Vorlage und senden es selbst.
- Es entscheidet nicht für Sie, ob eine Verletzung gemeldet werden muss oder ob eine DSFA nötig ist. Die Risikomatrix (Auswirkung mal Wahrscheinlichkeit) und ihre Schwellen stammen aus dem Modul, nicht aus der DSGVO oder den Leitlinien des Europäischen Datenschutzausschusses; die endgültige Entscheidung liegt beim Verantwortlichen oder seinem DSB.
- Es ist keine Rechtsberatung.

MODUL-LEITFADEN · GDPR COMPLIANCE

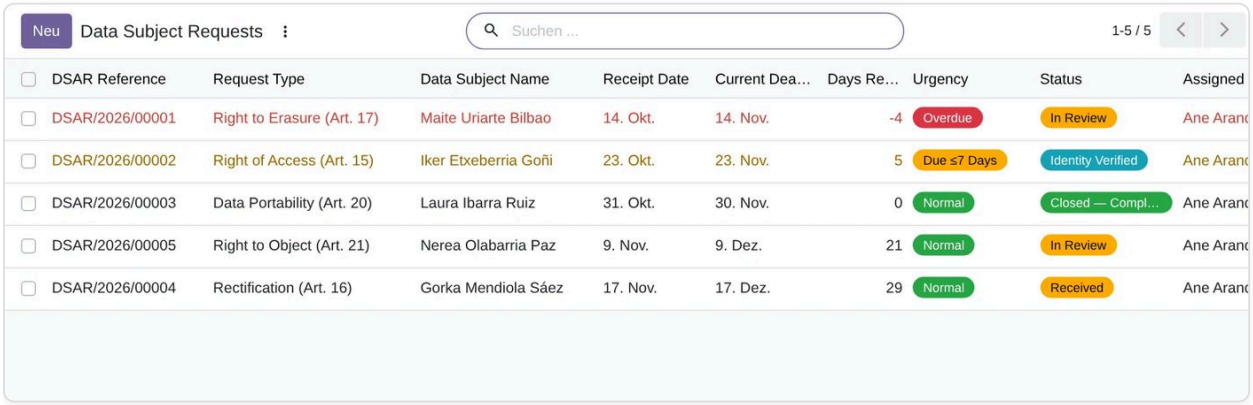
2 Das Modul in Zahlen

155 automatisierte Tests	**7.013** Codezeilen in Odoo Apps (Zweig 20.0)	**32** Aufsichtsbehörden	**16** Rechtsgrundlagen
5 geplante Aufgaben	**14** Testtage von FlexigoTech Cloud		

Es hängt nur von Odoo-Community-Modulen (base, mail und portal) und von `flexigotech_cloud` ab, funktioniert also in Community und Enterprise. Es gibt eine Version des Moduls für Odoo 17, 18, 19 und 20.

> Wie es getestet wurde: Das Modul bringt in seiner Version für Odoo 20 155 automatisierte Tests mit. Das Team von FlexigoTech hat es unter Odoo 17, 18, 19 und 20 getestet, auf Community-Datenbanken und auf Odoo.sh, und seine Fristen mit dem auf EUR-Lex veröffentlichten Text der DSGVO abgeglichen (Artikel 12 Abs. 3, 33 Abs. 1, 35 und 36). Keine Behörde hat das Modul geprüft, und es ist keine Rechtsberatung: die endgültige Entscheidung liegt bei Ihnen oder Ihrem DSB.

3 Wo Sie es in Ihrem Odoo sehen



- **Echter Screenshot aus Odoo 20.** Die Liste **Data Subject Requests** mit der geltenden Frist, den verbleibenden Tagen und der Dringlichkeit jeder Anfrage.

Dashboard	Drei Schaltflächen, die Listen öffnen. Weiter unten erklärt.
Processing Activities (RoPA)	**All Activities** und **DPIA Required**.
Data Subject Requests	**All Requests**, **Overdue** und **Due This Week**.
Breach Log	**All Breaches** und **Active Incidents**. Nur **GDPR Toolkit / Manager** sieht es.
DPIA	**All DPIAs** und **Awaiting DPO Review**. Nur **GDPR Toolkit / Manager** sieht es.
Retention Management	**Retention Schedule** und **Review History**. Nur **GDPR Toolkit / Manager** sieht es.
Reports	**Export RoPA (PDF)**, **Export RoPA (Excel)**, **DSAR History Report**, **Breach Log Report** und **DPIA Status Report**. Nur **GDPR Toolkit / Manager** sieht es.
Configuration	**DPO & Settings**, **Supervisory Authorities**, **Categories of Data**, **Categories of Data Subjects**, **Categories of Recipients**, **Legal Bases** und **Audit Log**. Nur **GDPR Toolkit / Manager** sieht es.

Das Menü **Dashboard** öffnet die Firmenkonfiguration mit drei Schaltflächen: **View Open DSARs**, **View Active Breaches** und **DPIAs Pending Review**. Jede Schaltfläche öffnet eine Liste. Es werden keine Zahlen oder Kennzahlen angezeigt.

Außerhalb seines Menüs fügt das Modul in Ihrem Odoo das Datenschutzportal unter der Adresse /my/privacy-rights hinzu, für Personen mit Portalkonto. Das Modul setzt keinen Link auf der Seite Mein Konto des Portals: die Adresse geben Sie dem Betroffenen selbst. Fünf geplante Aufgaben versenden E-Mail-Warnungen: die tägliche Erinnerung an die Frist der Anfragen, die Countdown-Warnung bei Verletzungen, die tägliche Prüfung des Ablaufs der Aufbewahrung, die wöchentliche Eskalation der überfälligen Anfragen und die jährliche Erinnerung an die Überprüfung des VVT.

4 Was Sie vor dem Start brauchen

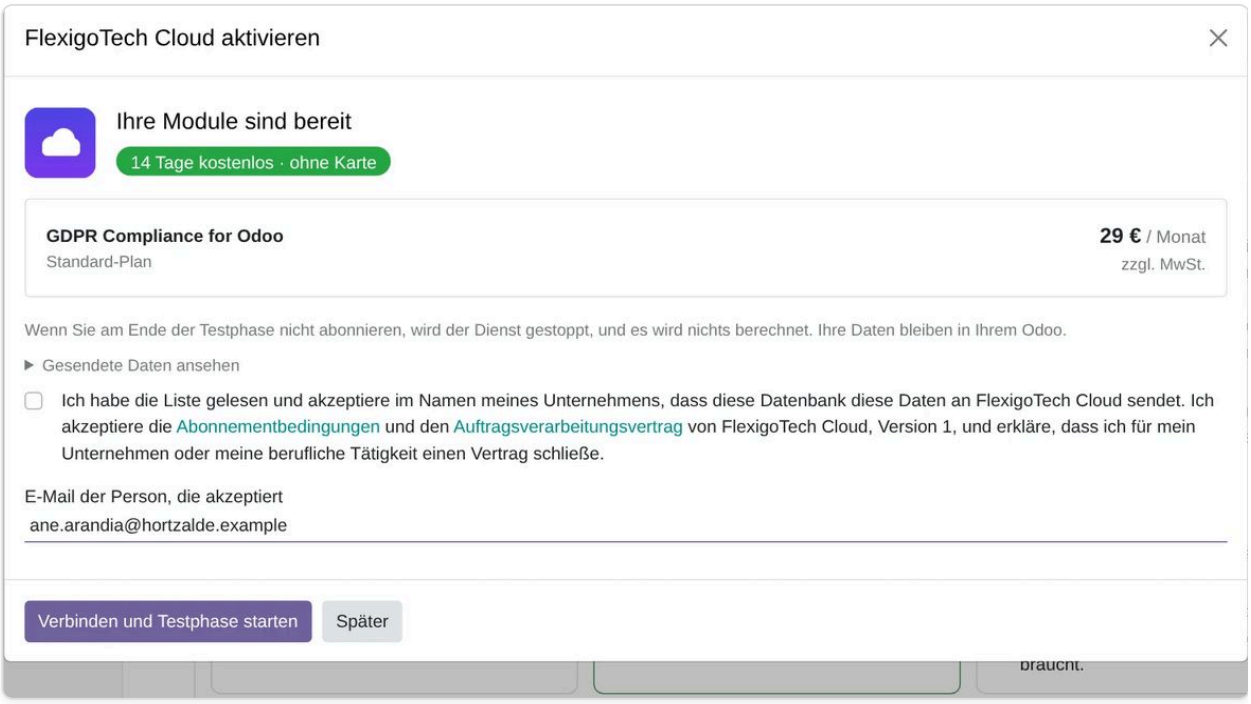
- Odoo 17, 18, 19 oder 20, auf Odoo.sh oder auf Ihrem eigenen Server. Odoo Online funktioniert nicht, da dort keine Module von Drittanbietern installiert werden können.
- Wer **GDPR Toolkit / Manager** und wer **GDPR Toolkit / User** sein wird. Bei der Installation des Moduls wird der Administrator zum **GDPR Toolkit / Manager**.
- Die Daten des DSB oder, falls keiner benannt ist, der für Datenschutz verantwortlichen Person: Name, E-Mail und Telefon.
- Die federführende Aufsichtsbehörde. Sie wählen sie in der Konfiguration unter den Behörden aus, die das Modul mitbringt.
- Wenn interne Notizen, die Begründung einer Ablehnung sowie Beschreibung und Folgen von Verletzungen verschlüsselt gespeichert werden sollen, die Variable GDPR_FERNET_KEY auf dem Server. Sie wird von der Person gesetzt, die den Server betreut. Ohne sie werden diese Texte unverschlüsselt gespeichert, und **Encryption Key Configured** zeigt das an.
- Damit Verkaufs- oder Mitarbeiterdaten in den Export für das Recht auf Datenübertragbarkeit aufgenommen werden, müssen die Apps Verkauf und Mitarbeiter installiert sein.
- Das Abonnement von FlexigoTech Cloud oder seine 14-tägige Testphase. Damit werden täglich sechs offizielle Quellen überwacht, und es kommt eine Benachrichtigung, wenn sich eine davon ändert.

> Das Modul löscht oder anonymisiert keine Daten: die Löschprüfung zählt, was vorhanden ist, und hält Ihre Entscheidung fest. Es meldet auch nichts an die Aufsichtsbehörde und informiert keine Betroffenen: Sie halten fest, was Sie getan haben. Es versendet das Antwortschreiben an den Betroffenen nicht. Die endgültige Entscheidung liegt beim Verantwortlichen oder seinem DSB, und das Modul ist keine Rechtsberatung.

Die Installation erfolgt wie bei jedem Drittanbieter-Modul für Odoo, auf Odoo.sh oder auf Ihrem Server. Odoo installiert gleichzeitig `flexigotech_cloud`, die Verbindung zu FlexigoTech Cloud, und die Odoo-Apps, von denen es abhängt: Discuss und das Portal.

5 Die Testphase von FlexigoTech Cloud

1. **Klicken Sie oben in der Leiste auf Aktivieren**
   Das erscheint, sobald Sie das Modul installieren. Es öffnet sich das Fenster **FlexigoTech Cloud aktivieren**, mit dem Tarif Standard und seinen 14 Tagen kostenlos, ohne Kreditkarte.



- **Echter Screenshot aus Odoo 20.** Das Aktivierungsfenster: Lesen Sie die Liste der Daten, setzen Sie das Häkchen und geben Sie Ihre E-Mail-Adresse ein.

2 **Akzeptieren und E-Mail eingeben**

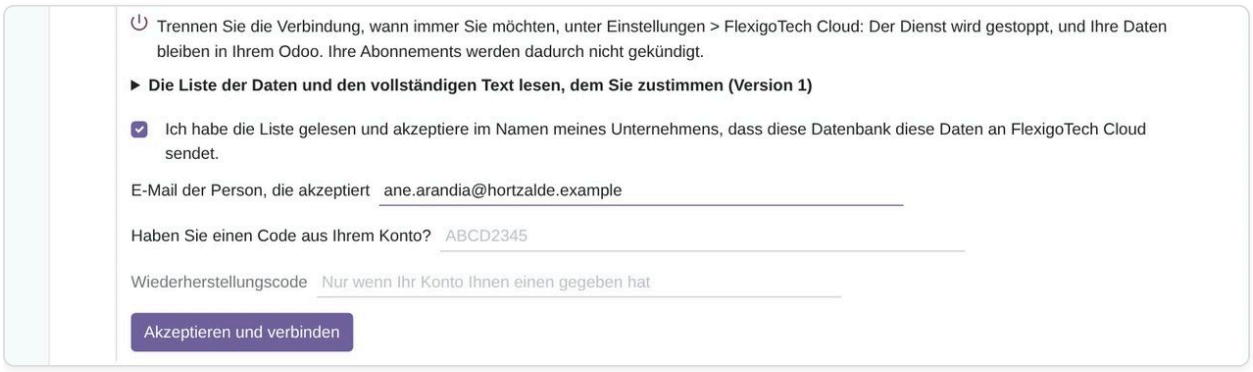
Setzen Sie das Häkchen bei „Ich habe die Liste gelesen und akzeptiere im Namen meines Unternehmens…“ (es umfasst die Bedingungen des Abonnements und den Auftragsverarbeitungsvertrag) und geben Sie die **E-Mail der Person, die akzeptiert** ein.

3 **Klicken Sie auf Verbinden und Testphase starten**

Odoo registriert die Datenbank bei FlexigoTech Cloud und startet die Testphase des Moduls. Wenn Sie das später erledigen möchten, schließt **Später** das Fenster.

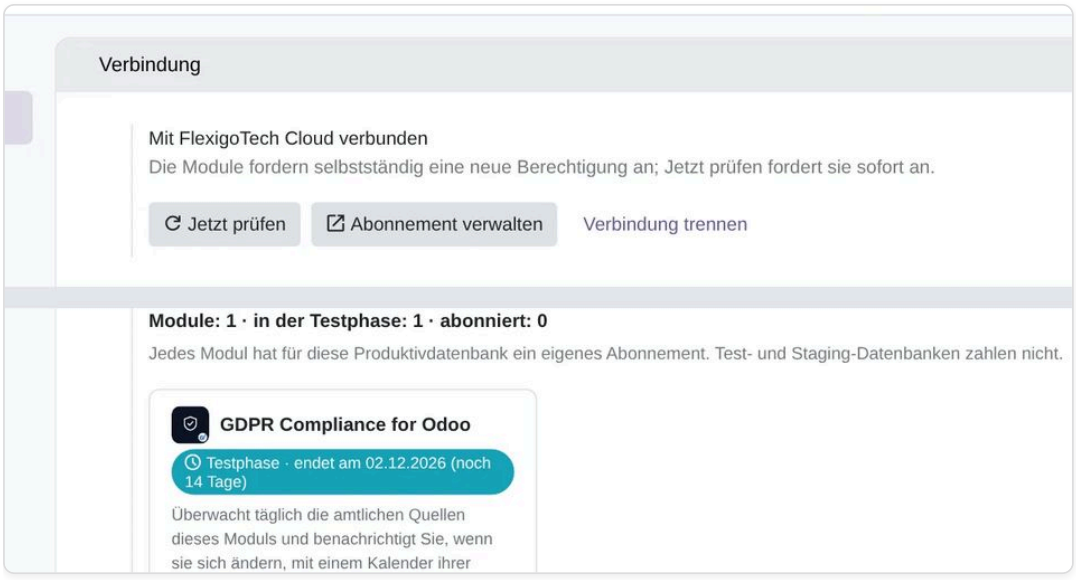
Dasselbe über die Einstellungen

Unter **Einstellungen › FlexigoTech Cloud** steht die vollständige Liste dessen, was die Datenbank sendet. Setzen Sie das Häkchen, geben Sie die E-Mail-Adresse ein und klicken Sie auf **Akzeptieren und verbinden**. Wenn Sie bereits ein Konto auf app.flexigotech.com haben, verknüpft das Feld **Haben Sie einen Code aus Ihrem Konto?** die Datenbank mit diesem Konto (der Code ist 10 Minuten gültig).



- **Echter Screenshot aus Odoo 20.** Einstellungen › FlexigoTech Cloud vor dem Verbinden: das gesetzte Häkchen, die E-Mail-Adresse und **Akzeptieren und verbinden**.

Ist die Datenbank verbunden, zeigt der Block **Module** jedes Modul mit seinem Status: **Testphase** und das Datum des Endes, **Abonniert** usw. Von dort wählen Sie den Tarif (Standard oder Pro, monatlich oder jährlich) und klicken auf **Abonnieren**: die Zahlung erfolgt auf der Seite von Stripe, außerhalb von Odoo.



- **Echter Screenshot aus Odoo 20.** Einstellungen › FlexigoTech Cloud mit verbundener Datenbank und dem Modul in der Testphase.

Preise ohne MwSt. Wenn Sie nach Ende der Testphase kein Abonnement abschließen, wird der Dienst angehalten und nichts berechnet; Ihre Daten bleiben in Ihrem Odoo. **Jetzt prüfen** fordert die Berechtigung sofort an (andernfalls erneuert das Modul sie selbstständig alle 6 Stunden).

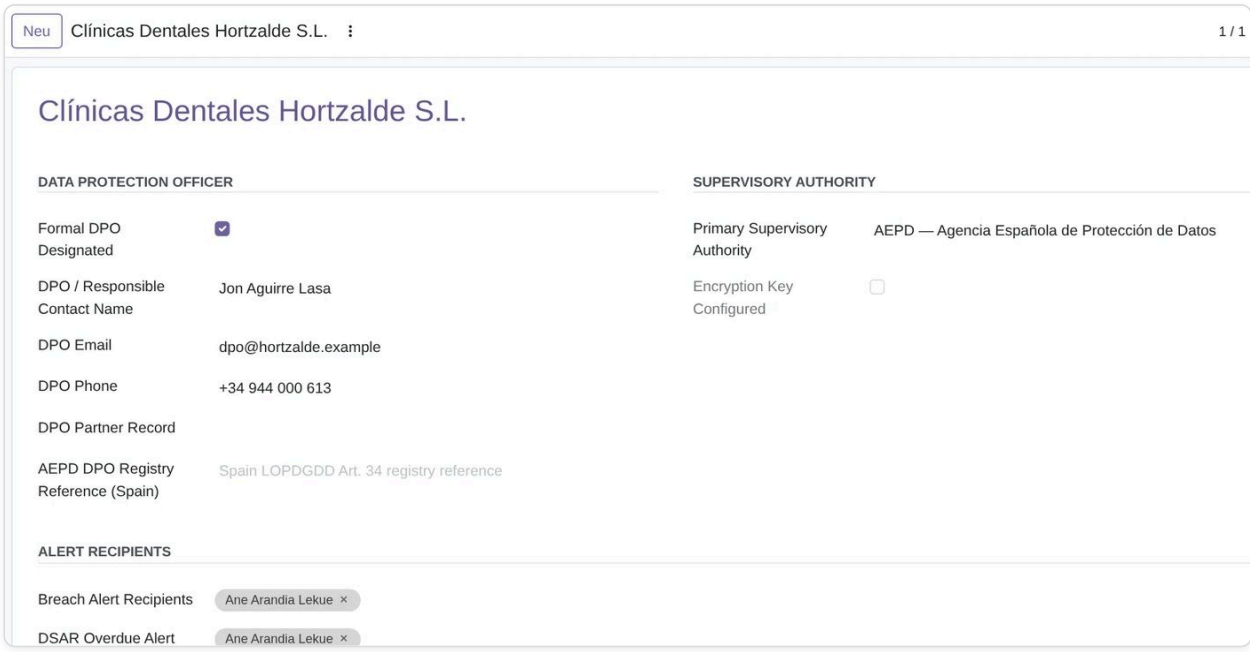
> In einer neutralisierten Kopie (Staging) oder in einer Datenbank mit Demodaten lässt sich keine Testphase starten: Die Einstellungen melden dies mit «Diese Datenbank ist eine neutralisierte Kopie oder enthält Demodaten, daher können hier keine Testphasen gestartet werden.»

MODUL-LEITFADEN · GDPR COMPLIANCE

6 Schritt für Schritt einrichten

1. **Die Konfiguration öffnen**

   Gehen Sie zu **GDPR Toolkit › Configuration › DPO & Settings**. Es öffnet sich die DSGVO-Konfiguration Ihres Unternehmens; falls es noch keine gibt, erstellt Odoo sie mit den Standardwerten.



- **Echter Screenshot aus Odoo 20.** Die DSGVO-Konfiguration des Unternehmens mit den Daten des DSB, der Aufsichtsbehörde und den Empfängern der Warnungen.

2 **Die Daten des DSB ausfüllen**

Füllen Sie **DPO / Responsible Contact Name**, **DPO Email** und **DPO Phone** aus. Wenn kein DSB benannt ist, entfernen Sie das Häkchen bei **Formal DPO Designated**.

3 **Die Aufsichtsbehörde wählen**

Wählen Sie die **Primary Supervisory Authority**.

4 **Festlegen, wer die Warnungen erhält**

Füllen Sie **Breach Alert Recipients** und **DSAR Overdue Alert Recipients** aus. Wenn Sie niemanden eintragen, gehen die Warnungen an alle, die im Unternehmen **GDPR Toolkit / Manager** sind.

5 **Die Vorlaufzeiten anpassen**

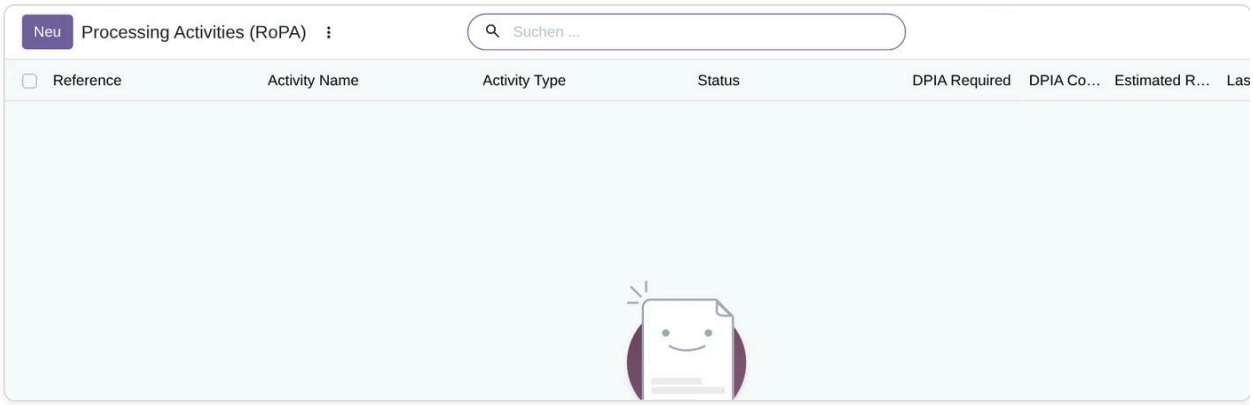
Prüfen Sie **Retention Advance Warning (days)**, das mit 30 voreingestellt ist, und **DSAR Reminder Days Before Deadline**, das mit 7 voreingestellt ist.

6 **Die Gruppen zuweisen**

Weisen Sie **GDPR Toolkit / Manager** und **GDPR Toolkit / User** den Personen zu, die sie brauchen.

7 **Die erste Tätigkeit anlegen**

Gehen Sie zu **GDPR Toolkit › Processing Activities (RoPA) › All Activities**. Anfangs ist die Liste leer. Klicken Sie auf **Neu** und füllen Sie die Tätigkeit aus.



- **Echter Screenshot aus Odoo 20.** Die Liste der Verarbeitungstätigkeiten, noch ohne Einträge.

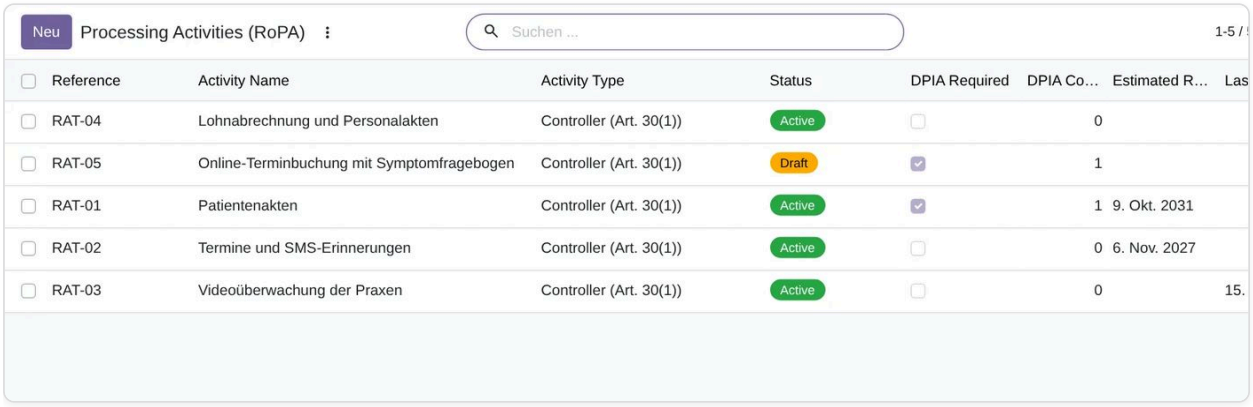
8 Die Adresse des Portals weitergeben

Wenn die Betroffenen über das Portal anfragen sollen, geben Sie jedem Betroffenen mit Portalkonto die Adresse /my/privacy-rights Ihres Odoo. Das Modul setzt keinen Link auf der Seite Mein Konto.

Danach arbeiten die geplanten Aufgaben selbstständig. Jeden Tag werden die Erinnerungen an bald fällige Anfragen versendet und das Ende der Aufbewahrung geprüft. Jede Stunde, in den letzten 6 Stunden der Frist einer Verletzung, erscheint deren Warnung. Jede Woche kommt die Übersicht der überfälligen Anfragen und einmal im Jahr die Erinnerung, das Verzeichnis der Verarbeitungstätigkeiten zu überprüfen. Die Erinnerung an eine Anfrage geht an die zugewiesene Person; die übrigen Warnungen gehen an die von Ihnen eingetragenen Empfänger oder, falls keine eingetragen sind, an die DSGVO-Manager des Unternehmens.

MODUL-LEITFADEN · GDPR COMPLIANCE

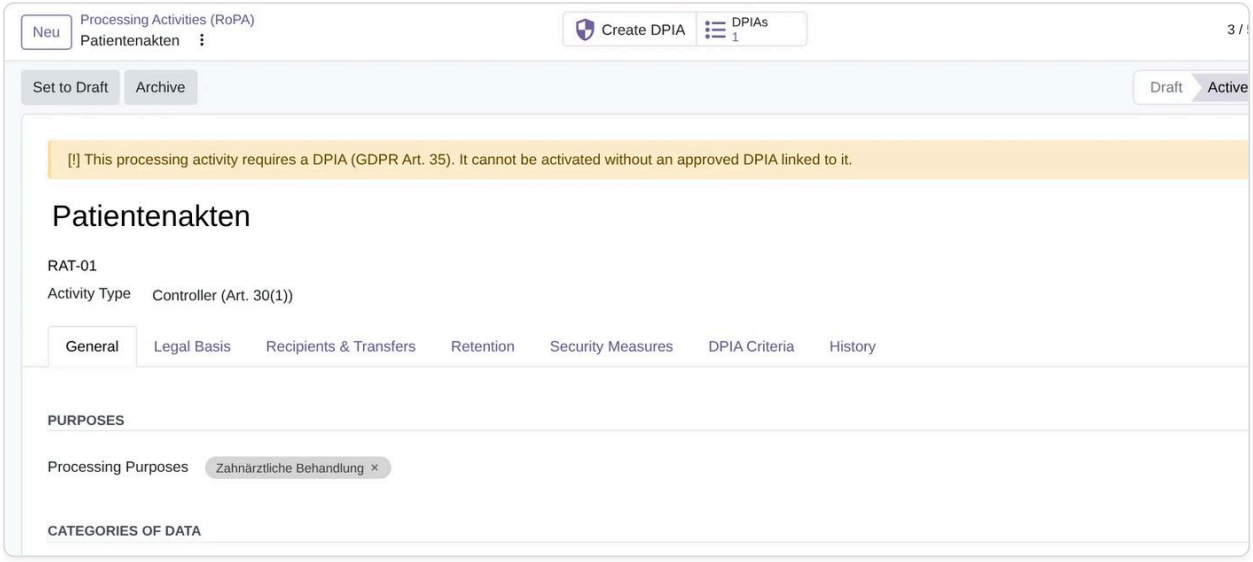
7 Das Verzeichnis der Verarbeitungstätigkeiten



- **Echter Screenshot aus Odoo 20.** Die Liste **Processing Activities (RoPA)** mit ihren fünf Tätigkeiten.

Jeder Eintrag enthält, was Art. 30 Abs. 1 verlangt, wenn Sie als Verantwortlicher handeln, oder Art. 30 Abs. 2, wenn Sie als Auftragsverarbeiter handeln. Das wählen Sie unter **Activity Type**. Sie füllen Zwecke, Kategorien von Betroffenen, Datenkategorien und Empfängerkategorien aus, die Rechtsgrundlage nach Art. 6 und die nach Art. 9, Übermittlungen an Drittländer mit ihrer Garantie, die Aufbewahrung und die Sicherheitsmaßnahmen.

Die Datenkategorien, Betroffenenkategorien und Empfängerkategorien wählen Sie aus den Listen unter **GDPR Toolkit › Configuration › Categories of Data**, **GDPR Toolkit › Configuration › Categories of Data Subjects** und **GDPR Toolkit › Configuration › Categories of Recipients**. Die Zwecke legen Sie an, indem Sie sie direkt im Eintrag schreiben. Die **Reference** vergibt Odoo beim Anlegen der Tätigkeit, und sie lässt sich nicht bearbeiten.



- **Echter Screenshot aus Odoo 20.** Der Eintrag einer Tätigkeit mit seinen Reitern.

Set Active	Setzt die Tätigkeit auf **Active**. Sie wird nicht angezeigt, wenn sie bereits aktiv ist.
Set to Draft	Setzt die Tätigkeit zurück auf **Draft**. Diese Schaltfläche erscheint nur, wenn die Tätigkeit aktiv ist.
Archive	Setzt die Tätigkeit auf **Archived**. Sie wird nicht angezeigt, wenn sie bereits archiviert ist.

Status

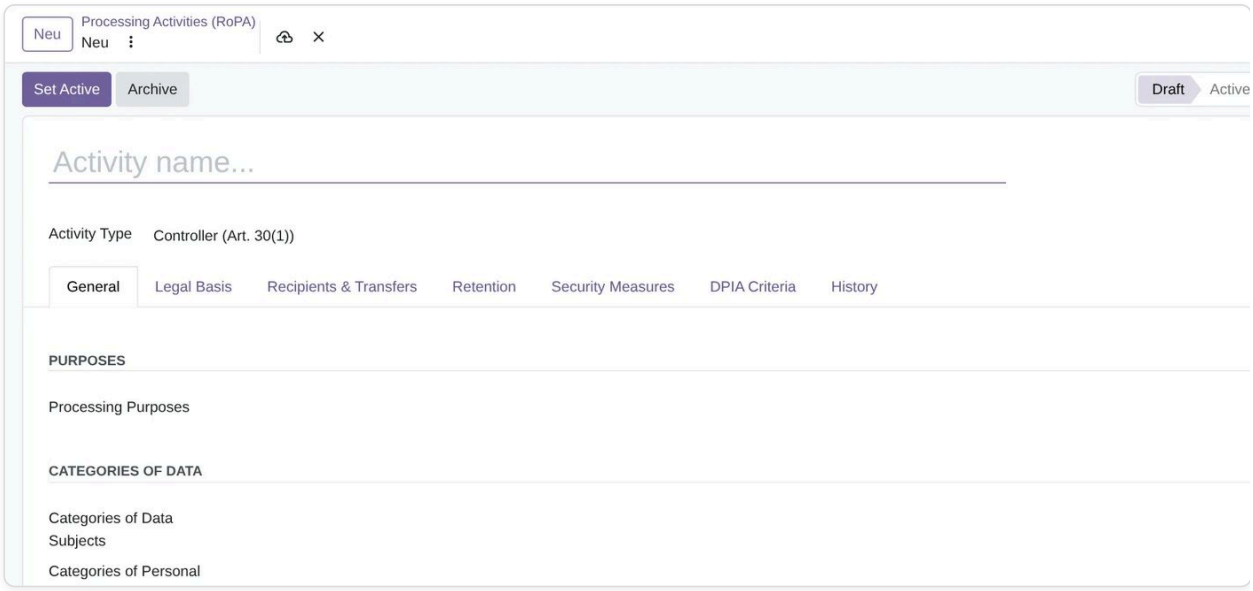
- **Draft**: der Status, mit dem die Aktivität angelegt wird.
- **Active**: die Aktivität, die gültig ist.
- **Archived**: die Aktivität, die nicht mehr verwendet wird. Sie bleibt im Verzeichnis.

Verlauf

Jedes Mal, wenn die Aktivität angelegt oder eine Änderung gespeichert wird, fügt das Modul dem Verlauf einen Eintrag hinzu, der auf dem Reiter **History** zu sehen ist. Diese Einträge lassen sich weder ändern noch löschen.

Eine Aktivität anlegen

1. **Legt die Aktivität an**
   Drücken Sie in der Liste **Processing Activities (RoPA)** auf **Neu**.



- **Echter Screenshot aus Odoo 20.** Das Formular einer neuen Aktivität im Status **Draft**.

2 **Füllen Sie die Reiter aus**

Vervollständigen Sie **General**, **Legal Basis**, **Recipients & Transfers**, **Retention** und **Security Measures**.

3 **Aktivieren Sie sie**

Drücken Sie auf **Set Active**.

> Eine Aktivität wird nicht gelöscht: Das Modul verhindert dies, um den Prüfpfad zu erhalten. Sie muss mit **Archive** archiviert werden. Außerdem lässt sich eine Aktivität, die eine DSFA erfordert, nicht aktivieren, solange keine genehmigte DSFA verknüpft ist.

Was jeder Status bedeutet

Draft	Anfangsstatus. Sie können das Blatt ausfüllen und korrigieren, solange Sie es vervollständigen.
Active	Die Aktivität ist gültig. Um hierhin zu gelangen, muss bei Erforderlichkeit einer DSFA eine genehmigte DSFA verknüpft sein. Von hier aus bringt **Set to Draft** sie zurück in **Draft**.
Archived	Die Aktivität wird außer Gebrauch genommen, ihr Blatt und ihr Verlauf bleiben jedoch erhalten. Das ist der einzige Weg, sie zu entfernen, denn löschen lässt sie sich nicht.

Wann das Modul eine Aktion nicht zulässt

- Eine Aktivität mit **DPIA Required** ohne verknüpfte genehmigte DPIA aktivieren: Es erscheint «Cannot activate processing activity "...": a DPIA is required but no approved DPIA is linked. Please complete and approve a DPIA first.»
- Eine Aktivität löschen: Es erscheint «Processing activity records cannot be deleted to preserve the audit trail. Please archive the record instead.»
- Einen Verlaufseintrag ändern oder löschen: Es erscheinen «History records are immutable and cannot be deleted. They are part of the GDPR audit trail.» und «History records are immutable.»

Wann die DSFA verpflichtend ist

DPIA Required wird automatisch gesetzt, wenn zwei oder mehr Kriterien des Reiters **DPIA Criteria** erfüllt sind, oder wenn sie manuell mit **DPIA Required (Manual Override)** erzwungen wird. Diese Zwei-Kriterien-Regel stammt aus den WP248-rev.01-Leitlinien und ist eine allgemeine Richtlinie, keine gesetzliche Pflicht. Die Kriterien sind **Systematic profiling**, **Automated decisions with legal effects**, **Systematic monitoring**, **Special categories at large scale**, **Large-scale processing**, **Data matching / combining**, **Vulnerable data subjects**, **New technology** und **Prevents exercise of rights**. **DPIA Criteria Met** zeigt, wie viele erfüllt sind, und **DPIA Requirement Reason** enthält die Begründung.

Reiter und Felder des Blatts

General	**Activity Name**, **Activity Type**, die Gruppen **Purposes** und **Categories of Data** sowie die Angaben zum Auftragsverarbeiter, die in einer eigenen Gruppe stehen: **Processor Details (Art. 30(2))**.
Legal Basis	**Legal Basis (Art. 6)** und **Special Category Legal Basis (Art. 9)**.
Recipients & Transfers	**Categories of Recipients**, **Third-Country Transfer**, **Third Countries**, **Transfer Safeguard** und **Safeguard Notes**.
Retention	**Retention Duration**, **Retention Unit** und **Retention Reference Point**, außerdem **Reference Date (fixed)**, **Last Transaction Date**, **Estimated Retention End Date** und **Last Retention Review**.
Security Measures	**Technical & Organisational Security Measures**.
History	**Version History**: ein Eintrag für jede Änderung.

Die Optionen von **Transfer Safeguard** lauten **Adequacy Decision**, **Standard Contractual Clauses (SCC)**, **Binding Corporate Rules (BCR)**, **EU-US Data Privacy Framework (DPF)**, **Other Safeguard** und **No Safeguard (document justification)**. Unter **Safeguard Notes** wird die Referenz der SCC, die Zertifizierungsnummer des DPF oder die Begründung vermerkt. **Retention Reference Point** akzeptiert **From End of Contract**, **From Last Transaction**, **From Withdrawal of Consent**, **Fixed Date** und **Other**.

Filter und verknüpfte Listen

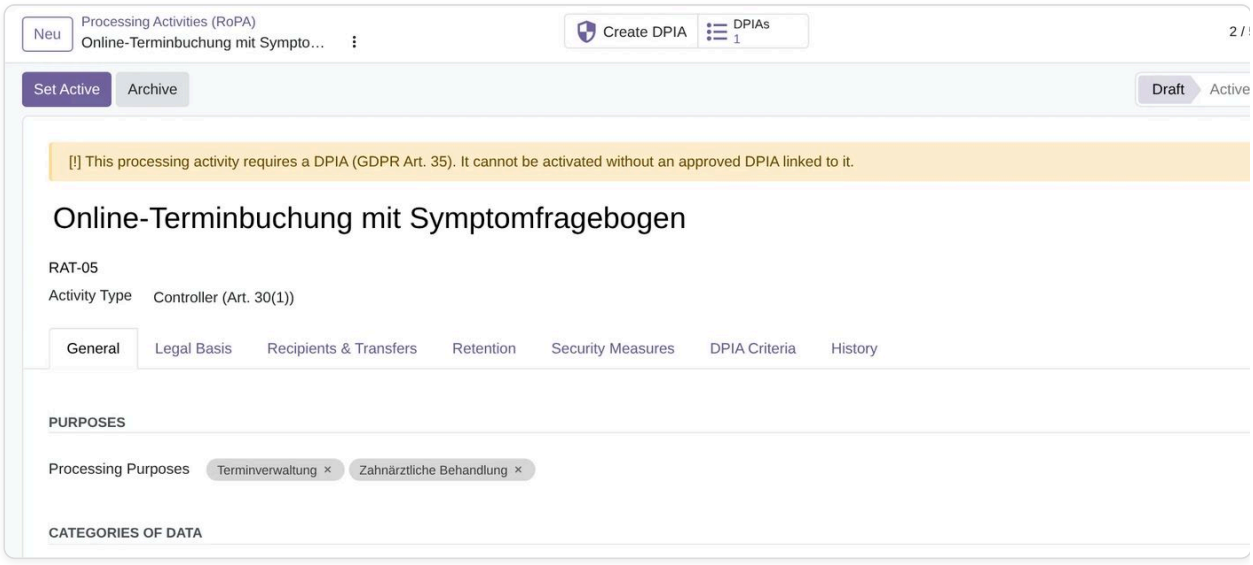
Die Suche bietet die Filter **Active**, **Draft** und **DPIA Required** sowie die Gruppierungen **By Type** und **By Status**. Das Menü **GDPR Toolkit › Processing Activities (RoPA) › DPIA Required** öffnet die Aktivitäten, die eine DPIA benötigen. Das Menü **GDPR Toolkit › Retention Management › Retention Schedule** öffnet die Aktivitäten, für die eine Aufbewahrungsfrist hinterlegt ist.

Ein Beispiel von Anfang bis Ende

Die Beispielbildschirme zeigen eine Zahnklinik mit fünf Aktivitäten. Eine davon, die Patientenakte, ist aktiv und erfordert eine DSFA. Eine andere, die Online-Terminbuchung mit Symptomfragebogen, befindet sich weiterhin in **Draft** und erfordert ebenfalls eine DSFA.

1. **Anlegen und ausfüllen**

   Sie drücken auf **Neu**, geben den Namen ein und füllen Zwecke, betroffene Personen, Daten, Rechtsgrundlage, Aufbewahrung und Sicherheitsmaßnahmen aus.



- **Echter Screenshot aus Odoo 20.** Die Aktivität in **Draft**, mit dem Hinweis, dass sie eine DSFA erfordert.

2 **Aktivieren versuchen**

Sie drücken auf **Set Active**. Solange keine genehmigte DSFA verknüpft ist, verhindert das Modul dies, und die Fehlermeldung erscheint.

3 **Die DSFA klären**

Die Schaltfläche zum Anlegen der DSFA oben im Aktivitätsblatt öffnet eine neue DSFA, die bereits mit ihr verknüpft ist. Nach der Genehmigung können Sie die Aktivität aktivieren.

4 **Den Verlauf prüfen**

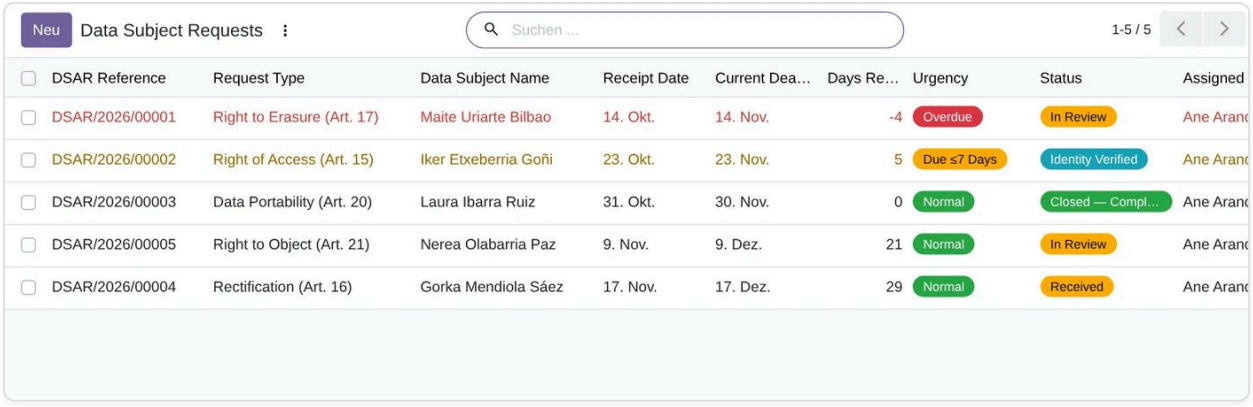
Jede Änderung wird auf dem Reiter **History** festgehalten.

MODUL-LEITFADEN · GDPR COMPLIANCE

8 Anträge betroffener Personen und ihre Fristen

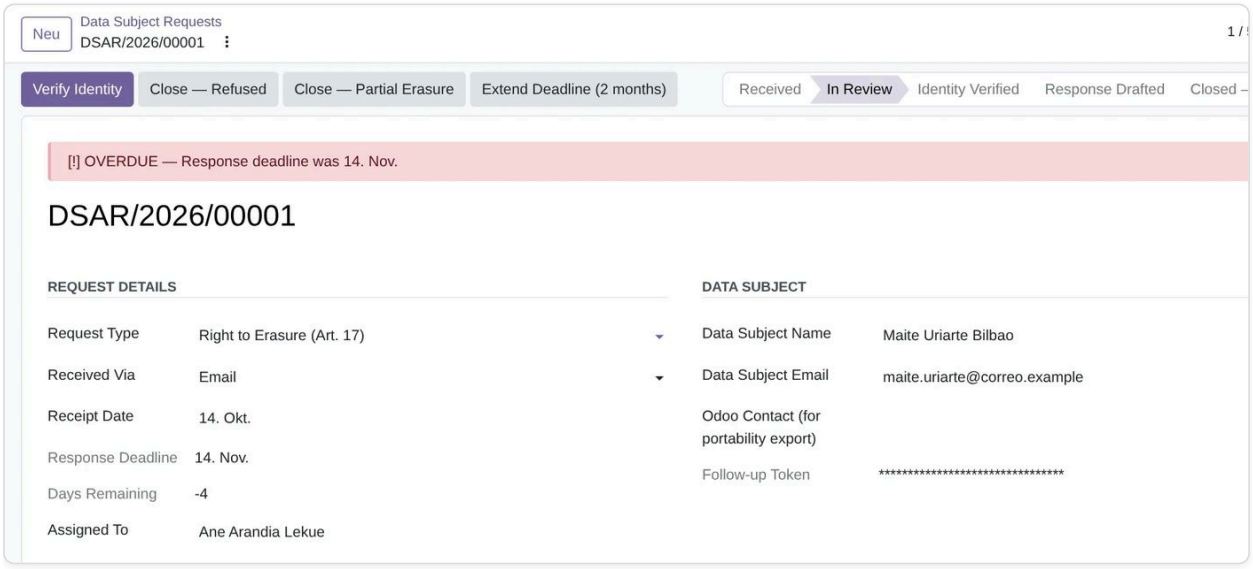
Es gibt sechs Antragsarten: **Right of Access (Art. 15)**, **Rectification (Art. 16)**, **Right to Erasure (Art. 17)**, **Restriction of Processing (Art. 18)**, **Data Portability (Art. 20)** und **Right to Object (Art. 21)**. Der **Received Via** kann **Portal Submission**, **Email**, **Letter**, **Phone** oder **Manual Entry** sein.

Die **Response Deadline** beträgt einen Monat ab dem **Receipt Date** (Art. 12 Abs. 3 DSGVO). Bei Bedarf kann sie um weitere zwei Monate verlängert werden, ebenfalls gemäß Art. 12 Abs. 3, und dann wird die **Current Deadline** zur verlängerten Frist. Die Spalte **Days Remaining** zählt bis zu dieser aktuell geltenden Frist.



- **Echter Screenshot aus Odoo 20.** Die Liste der Anträge mit ihrer aktuell geltenden Frist, den verbleibenden Tagen, der Dringlichkeit und der zugewiesenen Person.

Die Liste **Overdue** zeigt offene Anträge, deren Frist bereits abgelaufen ist, und die Liste **Due This Week** diejenigen, die in sieben Tagen oder weniger fällig werden. Die Spalte **Urgency** unterscheidet diese beiden Fälle vom Rest, der als **Normal** erscheint.



- **Echter Screenshot aus Odoo 20.** Ein Antrag mit dem Hinweis auf Fristüberschreitung und den Schaltflächen seines Status.

Die Person, die einen Antrag bearbeitet, steht unter **Assigned To**. Der Reiter **Identity Verification** speichert Methode, Datum und die verifizierende Person. Auf dem Reiter **Response** befindet sich der **Response Letter**: **Load Response Template** füllt ihn mit der allgemeinen Vorlage aus, und **Draft Response** setzt den Antrag auf **Response Drafted**. **Generate Refusal Letter** erstellt das Ablehnungsschreiben, ohne den Status zu ändern. Das Schreiben wird vom Modul nicht versendet.

Zum Ablehnen verlangt der Reiter **Refusal** die **Refusal Legal Basis** und die **Refusal Justification**. Ohne Begründung lässt sich der Antrag nicht als abgelehnt schließen.

Schaltflächen des Datensatzes

Start Review	Setzt den Antrag von **Received** auf **In Review**.
Verify Identity	Setzt ihn von **In Review** auf **Identity Verified**.
Draft Response	Setzt ihn von **Identity Verified** auf **Response Drafted** und lädt die Vorlage.
Close — Completed	Schließt einen Antrag mit der erstellten Antwort.

Close — Refused	Sichtbar bei Antragsprüfung, verifizierter Identität oder erstellter Antwort.
Close — Partial Erasure	Nur bei Löschanträgen, in denselben Status.
Extend Deadline (2 months)	Sichtbar, solange der Antrag offen und nicht verlängert ist. Verlangt die Begründung.

Status

Die Status sind **Received**, **In Review**, **Identity Verified** und **Response Drafted**. Ein Antrag wird als abgeschlossen, als abgelehnt oder mit partieller Löschung geschlossen. Die Status schreiten nur voran: Ein früherer Status lässt sich nicht wieder aufrufen.

Erinnerungen

Die Aufgabe **GDPR: DSAR Deadline Reminder** läuft täglich und sendet eine E-Mail, wenn für einen offenen Antrag noch die Tage übrig sind, die unter **DSAR Reminder Days Before Deadline** festgelegt sind: an die zugewiesene Person; hat sie keine E-Mail, an die DSGVO-Verantwortlichen; und falls auch das nicht möglich ist, an die E-Mail-Adresse des Unternehmens. Erreicht niemand die Nachricht, wird dies im Antrag vermerkt. Die Aufgabe **GDPR: DSAR Overdue Escalation** läuft wöchentlich und sendet die Übersicht der überfälligen Anträge an die **DSAR Overdue Alert Recipients** oder, falls keine hinterlegt sind, an die DSGVO-Verantwortlichen.

> Ein Antrag wird nicht gelöscht, sondern archiviert. Ein früherer Status lässt sich ebenfalls nicht wiederherstellen. Nur DSGVO-Verantwortliche können die Schaltflächen des Antrags verwenden.

Die Status im Einzelnen

- **Received**: Der Antrag ist gerade eingegangen. Nur **Start Review** ist sichtbar.
- **In Review**: Jemand prüft ihn. Man kann **Verify Identity** ausführen, als abgelehnt schließen, mit partieller Löschung schließen (falls es ein Löschantrag ist) oder die Frist verlängern.
- **Identity Verified**: Es steht fest, wer die betroffene Person ist. Man kann **Draft Response** ausführen und von hier aus ebenfalls als abgelehnt schließen oder die Frist verlängern.
- **Response Drafted**: Das Antwortschreiben ist vorbereitet. Sie können die Anfrage mit **Close — Completed** abschließen oder als abgelehnt schließen.
- Als abgeschlossen geschlossen: beantwortet und geschlossen.
- Als abgelehnt geschlossen: geschlossen mit ihrer Rechtsgrundlage und Begründung.
- Mit partieller Löschung geschlossen: nur bei Löschungen, wenn etwas aufbewahrt wird.
- Mit verlängerter Frist geschlossen: hat keine Schaltfläche. Die Verlängerung der Frist lässt den Antrag in seinem Status und ändert die **Current Deadline**.

Regeln und Bedingungen

- Der Status geht nicht zurück. Wenn Sie es versuchen, meldet Odoo «DSAR status cannot be moved backwards. The audit trail must be append-only.»
- Beim Verlängern der Frist muss eine Begründung eingetragen werden. Sonst erscheint «Extension reason is required when extending the deadline.»
- Zum Schließen als abgelehnt ist eine Begründung nötig. Fehlt sie, erscheint «Refusal justification is required before closing as refused.»

- **Generate Portability Export** erscheint nur bei Auskunfts- und Portabilitätsanfragen mit verifizierter Identität. Wer es ohne Verifizierung versucht, erhält «Identity must be verified before generating a portability export.»
- **Retention Conflict Check** gibt es nur bei Löschanfragen. Bei einem anderen Typ erscheint «Retention conflict check only applies to erasure requests.»
- Eine Anfrage lässt sich nicht löschen: Es erscheint «DSAR records cannot be deleted. Archive them instead (GDPR Manager / Admin only).»
- Die Schaltflächen funktionieren nur mit der Gruppe GDPR-Manager oder als Administrator. Sonst erscheint «Only GDPR Managers can perform this action.»
- **Load Response Template** auf dem Reiter **Response** tut dasselbe wie **Draft Response**: Es lädt die allgemeine Vorlage und setzt den Antrag auf **Response Drafted**, auch wenn er noch auf **Received** oder **In Review** steht. Verwenden Sie es, wenn Sie die Identität bereits verifiziert haben.

Die Löschprüfung

Retention Conflict Check zählt die veröffentlichten Rechnungen, die Mitarbeiterakten (mit der App Mitarbeiter) und die Verkaufsaufträge (mit Verkauf) des Kontakts im Antrag. Sie können für jede Gruppe wählen, ob sie aufbewahrt oder gelöscht wird, und mit **Record Decision & Close DSAR** wird Ihre Entscheidung in den internen Notizen vermerkt und der Antrag geschlossen: als abgeschlossen, wenn alles gelöscht wird, mit partieller Löschung, wenn etwas aufbewahrt wird. Das Modul löscht oder anonymisiert nichts: Das tun Sie selbst in Odoo.

Das Blatt: Gruppen und Reiter

Request Details	Der Typ, der Kanal, das Eingangsdatum, die Antwortfrist, die verbleibenden Tage und die zugewiesene Person.
Data Subject	Name und E-Mail-Adresse der betroffenen Person, der Odoo-Kontakt für den Übertragbarkeitsexport und das Verfolgungs-Token.
Extension	**Deadline Extended**, **Extension Reason**, **Extended Deadline (3 months)** und **Extension Notification Due**, das dasselbe Datum wie die ursprüngliche Frist ist: einen Monat ab Eingang.
Identity Verification	Das Kontrollkästchen für verifizierte Identität, die Methode, das Datum und wer sie geprüft hat.
Response	Das Antwortschreiben und die Dateien des Portabilitätsexports.
Refusal	Die Rechtsgrundlage und die Begründung der Ablehnung.
Internal Notes	Notizen der Person, die den Fall bearbeitet.

Die Grundlage der Ablehnung kann **Manifestly Unfounded (Art. 12(5)(a))**, **Manifestly Excessive (Art. 12(5)(a))**, **Legal Exemption (Art. 23)** oder **Other** sein. Die internen Notizen und die Begründung werden nur dann verschlüsselt gespeichert, wenn der Server den Verschlüsselungsschlüssel hat. Ohne ihn werden sie unverschlüsselt gespeichert. Die Konfiguration zeigt dies unter **Encryption Key Configured** an.

Erinnerungen und Filter

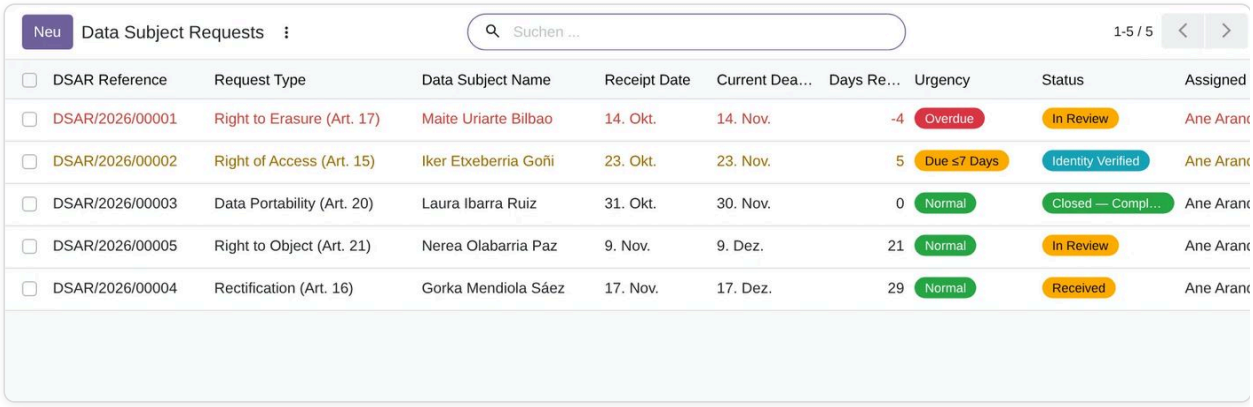
Die Filter der Liste sind **Open**, **Overdue**, der Filter für Fälle, die in sieben Tagen oder weniger ablaufen, **Erasure Requests** und **Access Requests**, mit den Gruppierungen **By Status** und **By Type**. Unter **GDPR Toolkit › Reports** finden Sie den **DSAR History Report**.

Die einzige E-Mail an die betroffene Person, die automatisch versendet wird, ist die Eingangsbestätigung eines über das Portal gestellten Antrags. Das Antwortschreiben wird vom Modul nicht versendet: Sie füllen es hier aus und versenden es über den von Ihnen gewählten Kanal.

Ein Beispiel von Anfang bis Ende

1 Der Antrag geht ein

Maite Uriarte Bilbao beantragt die Löschung ihrer Daten. Odoo setzt die **Response Deadline** einen Monat nach dem **Receipt Date**.



- **Echter Screenshot aus Odoo 20.** Die Liste mit dem Löschantrag, dem Auskunftsantrag, dem Portabilitätsantrag und zwei weiteren.

2 Die Frist wird überschritten

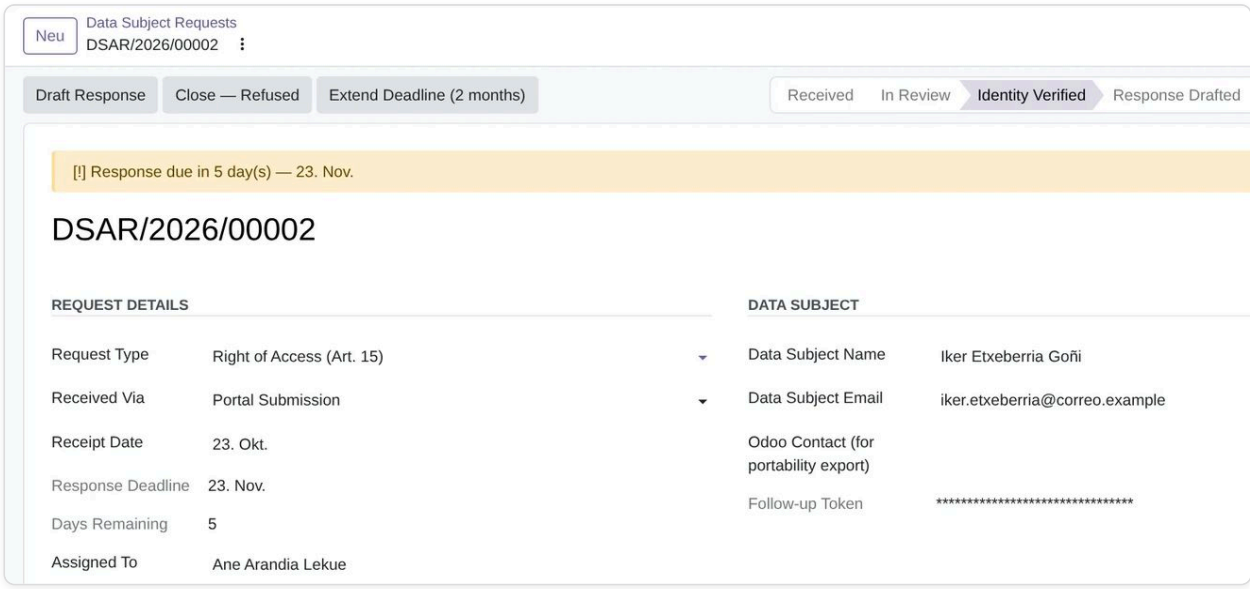
Niemand hat ihn geschlossen und die Frist ist bereits abgelaufen: **Days Remaining** zeigt -4, das Formular warnt, dass er überfällig ist, und der Antrag erscheint unter **Overdue**.



- **Echter Screenshot aus Odoo 20.** Die Liste der überfälligen Anträge, mit einem einzigen Antrag.

3 Ein weiterer Antrag läuft bald ab

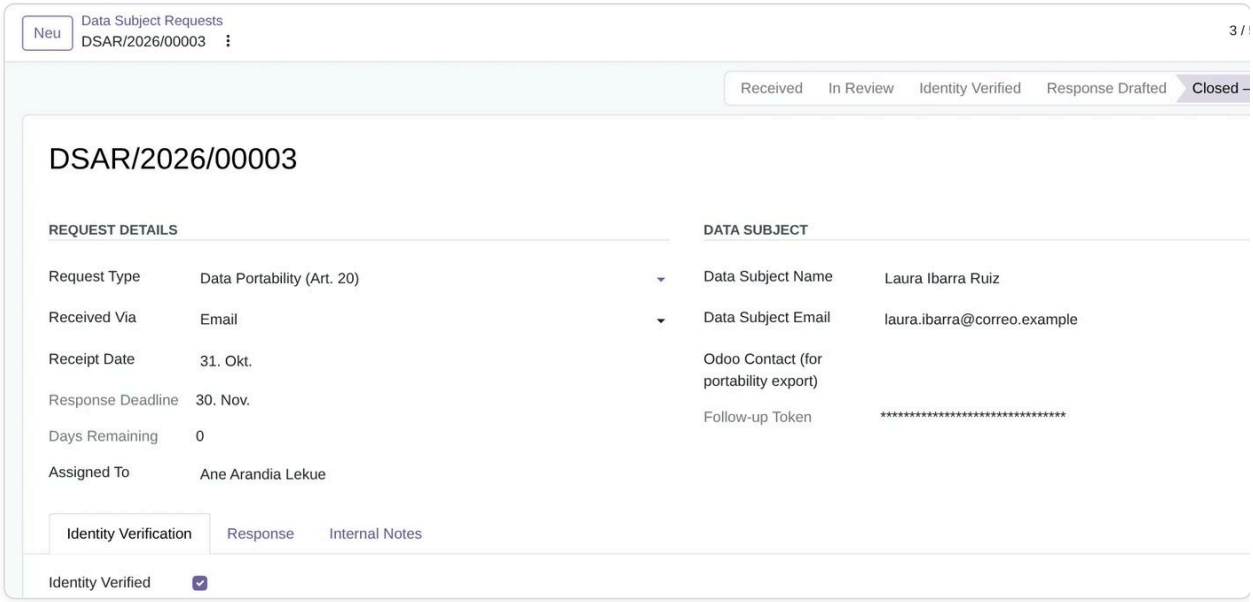
Iker Etxeberria Goñi hat Auskunft über seine Daten beantragt. Für seinen Antrag bleiben 5 Tage und seine Identität ist verifiziert: Er erscheint unter **Due This Week**.



- **Echter Screenshot aus Odoo 20.** Ein Antrag, der in 5 Tagen abläuft, mit verifizierter Identität.

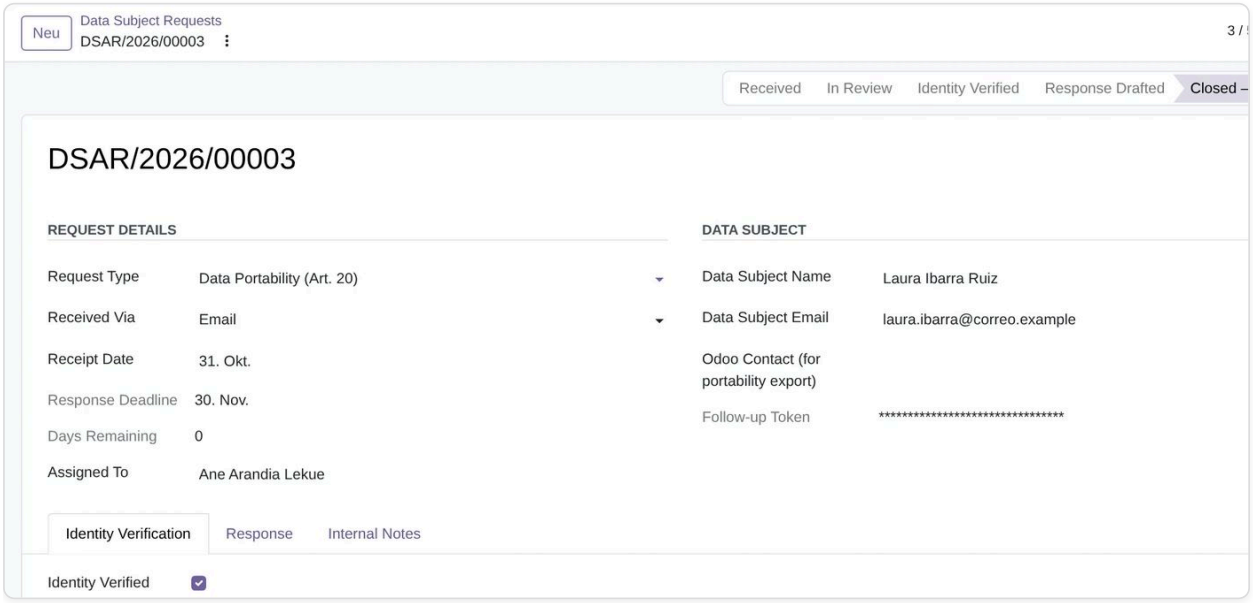
4 Er wird geschlossen

Der Portabilitätsantrag von Laura Ibarra Ruiz hat eine verifizierte Identität und ist als abgeschlossen geschlossen.



- **Echter Screenshot aus Odoo 20.** Ein als abgeschlossen geschlossener Portabilitätsantrag.

9 Portabilität, Löschung und das Datenschutzportal



- **Echter Screenshot aus Odoo 20.** Ein Portabilitätsantrag mit verifizierter Identität, bereits als abgeschlossen geschlossen.

Portabilitätsexport

Der Export wird manuell aus dem Antrag heraus über einen Assistenten erzeugt. Es gibt keine geplante Aufgabe, die ihn vorbereitet. Er verlangt zwei Dinge: eine verifizierte Identität und einen im Antrag verknüpften Odoo-Kontakt.

DSAR	Der Antrag, aus dem exportiert wird. Pflichtfeld.
Contact Data (res.partner)	Standardmäßig angekreuft. Enthält die Daten aus der Kontaktkarte.
Order History (sale.order)	Enthält die Bestellungen des Kontakts. Nur bei installierter App Verkauf.
HR Data (hr.employee)	Enthält die Mitarbeiterkarte. Nur bei installierter App Mitarbeiter.
I confirm explicit HR data inclusion	Bestätigungskästchen für die Personalstammdaten.
Export Format	Zwei Optionen: **JSON (machine-readable)** oder **CSV**.
Export File	Die erzeugte Datei, sobald der Export fertig ist.
Generate Export	Erstellt die Datei. Wird ausgeblendet, sobald der Export bereits erstellt wurde.
Close	Schließt den Assistenten.

Prüfung auf Konflikte bei der Löschung

Bei einem Löschantrag zählt **Retention Conflict Check** die vorhandenen Daten des Kontakts: gebuchte Rechnungen, Mitarbeiterkarten und Verkaufsaufträge, je nach installierten Apps. Der Assistent zeigt die Gruppen **Data Subject**, **Conflict Findings** und **Your Decision per Category**. Für jede Kategorie wählen Sie **Retain (legal obligation)** oder **Erase / Anonymise**. Die Kategorie Marketing und Einwilligung erscheint standardmäßig unter **Erase / Anonymise**.

Mit **Record Decision & Close DSAR** wird die Entscheidung in den internen Notizen festgehalten und der Antrag geschlossen: als abgeschlossen, wenn alles gelöscht wird, und als teilweise gelöscht, wenn etwas aufbewahrt wird. **Cancel** beendet den Vorgang, ohne etwas zu speichern.

Datenschutzportal

Das Portal befindet sich unter /my/privacy-rights in Ihrem Odoo und verlangt eine Anmeldung, daher braucht die betroffene Person ein Portalkonto. Das Modul fügt keinen Link unter Mein Konto hinzu: Die Adresse geben Sie ihr selbst weiter. Das Formular verlangt die Art des Rechts, einen Text von bis zu 2.000 Zeichen und bis zu 3 Dokumente mit je 50 MB. Nach dem Absenden kommt die Eingangsbestätigung per E-Mail und eine Statusseite mit einem eigenen Link, die Art und Status ohne personenbezogene Daten anzeigt.

> Das Modul löscht oder anonymisiert keine Daten: Die Löschprüfung zählt nur die vorhandenen Daten und hält Ihre Entscheidung fest. Das Löschen oder Anonymisieren nehmen Sie selbst in Odoo vor. Außerdem versendet das Modul kein Antwortschreiben.

Was beim Portabilitätsexport geschieht

Das Recht auf Datenübertragbarkeit ist das des Art. 20 Abs. 1 DSGVO: den Erhalt der personenbezogenen Daten, die die betroffene Person bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format. Deshalb bietet der Assistent JSON oder CSV an.

Der Assistent verweigert die Erzeugung des Exports in drei Fällen:

- Wenn die Identität nicht verifiziert ist: «Identity must be verified before generating a portability export.»
- Wenn die Anfrage keinen Odoo-Kontakt hat: «No Odoo contact linked to this DSAR. Please link a res.partner record first.» Verknüpfen Sie ihn im Feld **Odoo Contact (for portability export)** der Anfrage.
- Wenn die Kontaktdaten bereits anonymisiert wurden, warnt der Assistent, dass die Daten der betroffenen Person bereits anonymisiert wurden, dass eine manuelle Bearbeitung erforderlich ist und dass der DSB kontaktiert werden muss.

Die Kontaktdaten sind standardmäßig angekreuft. Bestellungen werden nur bei installierter App Verkauf aufgenommen: bis zu 500, aus der Gesellschaft des Antrags. Die Personalstammdaten werden nur bei installierter App Mitarbeiter und angekreuftem Bestätigungskästchen aufgenommen: die Mitarbeiterkarte dieser Person mit Stelle, Abteilung und privaten Kontaktdaten.

Wenn der Export abgeschlossen ist

Nach der Erzeugung meldet der Assistent, dass die Datei fertig und dem Antrag beigefügt ist, und zeigt die **Export File** an. Die Datei liegt außerdem im Reiter **Response** des Antrags.

Antragsstatus und Fristen

Die Frist für die Antwort beträgt einen Monat ab Eingang des Antrags und kann bei Bedarf um zwei weitere Monate verlängert werden; die Verlängerung und ihre Gründe sind der betroffenen Person innerhalb dieses ersten Monats mitzuteilen (Art. 12 Abs. 3). Das Modul versendet diese Mitteilung nicht: Sie versenden sie selbst, vor der **Extension Notification Due**.

Extend Deadline (2 months) verlangt eine Begründung und ändert den Status des Antrags nicht: Es ändert nur die **Current Deadline** auf die verlängerte Frist. Kein Schaltfläche führt zu einem geschlossenen Status mit verlängerter Frist.

Regeln der Löschprüfung

Der Assistent öffnet sich nur bei Löschanfragen und prüft den in der Anfrage verknüpften Odoo-Kontakt; ohne Kontakt findet er nichts zu zählen. Er zählt gebuchte Rechnungen, Mitarbeiterkarten und Verkaufsaufträge dieses Kontakts. Die beiden letzten Gruppen setzen voraus, dass die Apps Mitarbeiter und Verkauf installiert sind. Jede Gruppe hat ihr eigenes Hinweisfeld: **Pending / Recent Invoices Found**, **Active HR Records Found** und **Active Orders Found**. Die **Conflict Summary** fasst die Zählung als Text zusammen.

Die Entscheidungen werden je Gruppe getroffen: **Invoice Data Decision**, **HR Data Decision**, **Order Data Decision** und **Marketing / Consent Data Decision**. Bei den ersten drei wählen Sie zwischen **Retain (legal obligation)** und **Erase / Anonymise**; bei der Marketinggruppe zwischen **Retain** und **Erase / Anonymise**.

Beim Festhalten der Entscheidung wird der Antrag als abgeschlossen geschlossen, wenn alles gelöscht wird, und als teilweise gelöscht, wenn eine Gruppe aufbewahrt wird. Das Modul hält die Entscheidung nur in den internen Notizen fest. Die Zusammenfassung des Assistenten erscheint auf Englisch und nennt Aufbewahrungsfristen aus dem spanischen Recht: Prüfen Sie diese mit Ihrem DSB, denn sie gelten nicht für alle Länder.

Das Portal und seine Grenzen

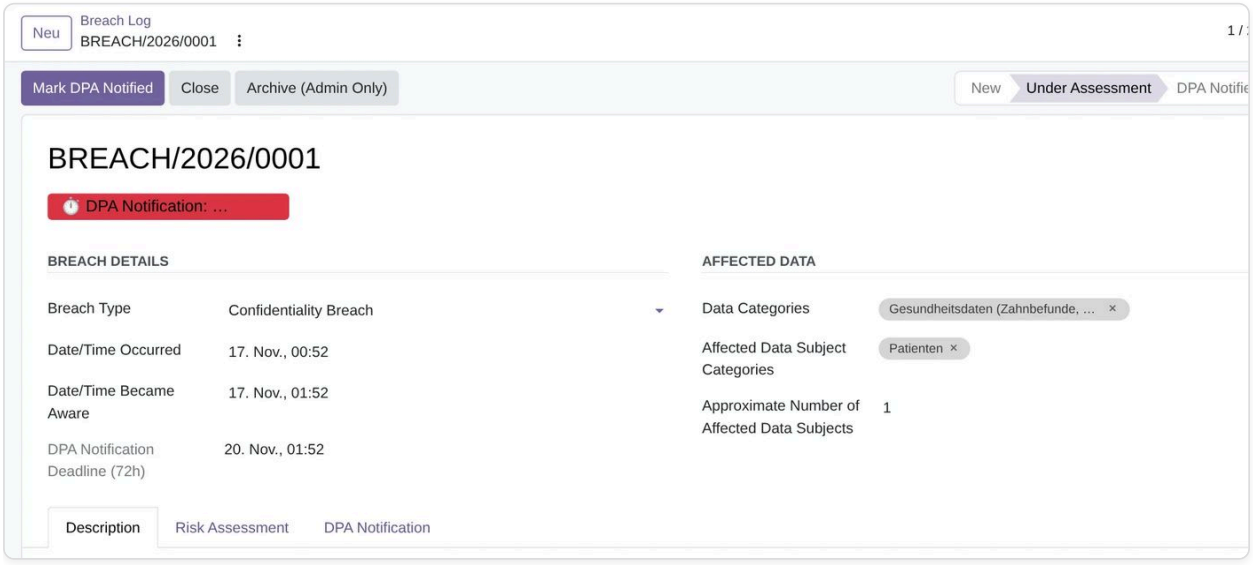
Das Portal setzt zwei Grenzen pro Person. Mit 3 Anträgen an einem Tag lässt es keine weiteren bis zum nächsten Tag zu. Mit 5 Anträgen in sieben Tagen nimmt es keine weiteren mehr an, setzt eine Prüfmarkierung in den Notizen des Kontakts und bittet die Person, sich mit Ihrem Unternehmen in Verbindung zu setzen. Ob ein Antrag offenkundig unbegründet oder exzessiv ist, entscheidet der Verantwortliche (Art. 12 Abs. 5).

Wer den Statuslink öffnet, sieht nur Art und Status des Antrags, ohne personenbezogene Daten. Die einzige E-Mail, die automatisch an die betroffene Person geht, ist die Eingangsbestätigung eines über das Portal gestellten Antrags; das Antwortschreiben verfassen und versenden Sie selbst.

Ein Beispiel von Anfang bis Ende

Laura Ibarra Ruiz hat die Übertragung ihrer Daten beantragt. Ihr Antrag hat eine verifizierte Identität und den verknüpften Odoo-Kontakt. Sie öffnen den Assistenten, lassen die Kontaktdaten angekreuzt, wählen JSON und klicken auf **Generate Export**: Die Datei erscheint unter **Export File** und ist dem Antrag beigefügt. Danach senden Sie ihr die Antwort über Ihren üblichen Kanal und schließen den Antrag als abgeschlossen.

10 Das Vorfallregister und die 72 Stunden



- **Echter Screenshot aus Odoo 20.** Eine Verletzung in Bewertung mit dem Fristcountdown und der Schaltfläche **Mark DPA Notified**.

Die Datenschutzverletzungen finden Sie unter **GDPR Toolkit › Breach Log › All Breaches**. Klicken Sie auf **Neu**, um eine anzulegen. Die **Breach Reference** vergibt Odoo beim Anlegen, sie lässt sich nicht ändern. Die Daten tragen Sie selbst im Formular ein. Es kommen keine Daten von außen.

Was auszufüllen ist

Breach Type	Pflichtfeld: **Confidentiality Breach**, **Integrity Breach**, **Availability Breach** oder **Multiple Types**.
Date/Time Occurred	Wann die Verletzung stattgefunden hat.
Date/Time Became Aware	Pflichtfeld. Ab diesem Zeitpunkt läuft die Meldefrist.
DPA Notification Deadline (72h)	Odoo berechnet sie aus dem Zeitpunkt der Kenntnisnahme.
Breach Description und **Likely Consequences**	Freitext im Reiter **Description**.
Impact Score und **Likelihood Score**	Im Reiter **Risk Assessment** wählen Sie jeden Wert von 1 bis 5.

Die Frist von 72 Stunden

Art. 33 Abs. 1 DSGVO verlangt, die Verletzung der Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden nach Kenntnisnahme zu melden. Das Modul setzt diese 72-Stunden-Frist ab dem **Date/Time Became Aware**. Beim Öffnen des Formulars sehen Sie, wie viel Zeit bleibt, in Stunden und Minuten; nach Ablauf steht dort „EXPIRED“. Die Berechnung erfolgt beim Öffnen und aktualisiert sich nicht automatisch auf dem Bildschirm. Die Aufgabe **GDPR: Breach Countdown Alert** läuft jede Stunde und warnt in den letzten 6 Stunden der Frist per E-Mail, solange die Verletzung nicht als gemeldet markiert ist: an die **Breach Alert Recipients** oder, falls keine hinterlegt sind, an die DSGVO-Verantwortlichen.

Risiko und Benachrichtigung der Betroffenen

Mit Auswirkung und Wahrscheinlichkeit berechnet Odoo den **Risk Score** und das **Risk Level**: niedrig bis 4, mittel bis 9, hoch bis 19 und kritisch ab 20. Diese Matrix stammt vom Modul, nicht aus der DSGVO. Bei hohem oder kritischem Risiko wird **Art. 34 Data Subject Notification Required** markiert. Die endgültige Entscheidung trifft der Verantwortliche oder sein DSB, und Sie können sie unter **DPO Final Art. 34 Determination** festhalten.

Status und Schaltflächen

Start Assessment	Setzt die Verletzung von **New** auf **Under Assessment**.
Mark DPA Notified	Erscheint nur in **Under Assessment**. Setzt den Status auf **DPA Notified** und speichert das Datum und die Uhrzeit. Das Modul meldet nichts: Das Meldeverfahren, die Referenznummer und die Nachweise tragen Sie selbst im Reiter **DPA Notification** ein.
Mark Data Subjects Notified	Erscheint nur in **DPA Notified** und wenn die Benachrichtigung nach Art. 34 verpflichtend ist. Setzt den Status auf **Data Subjects Notified** und speichert das Datum. Die Benachrichtigung erfolgt außerhalb von Odoo; den Nachweis legen Sie im Reiter **Art. 34 Notification** ab.
Close	Erscheint nicht bei **New** und **Closed**. Vor dem Schließen füllen Sie den Reiter **Post-Breach Review** aus: Ursache, Korrekturmaßnahmen, präventive Maßnahmen, wer genehmigt und das Datum.
Archive (Admin Only)	Nur für Odoo-Administratoren sichtbar. Öffnet einen Assistenten, der den **Archive Reason** abfragt.

Die Status sind **New**, **Under Assessment**, **DPA Notified**, **Data Subjects Notified** und **Closed**.

1. **Verletzung anlegen**
   Klicken Sie auf **Neu**, wählen Sie den **Breach Type** und tragen Sie ein, wann die Verletzung bekannt wurde.
2. **Bewerten**
   Klicken Sie auf **Start Assessment** und bewerten Sie Auswirkung und Wahrscheinlichkeit.
3. **Selbst melden und festhalten**
   Falls erforderlich, melden Sie die Verletzung selbst an die Aufsichtsbehörde und klicken Sie auf **Mark DPA Notified**.
4. **Mitteilen und schließen**
   Falls es Pflicht ist, benachrichtigen Sie die Betroffenen selbst und klicken Sie auf **Mark Data Subjects Notified**. Schließen Sie mit der Nachbereitung und **Close** ab.

> Eine Datenschutzverletzung lässt sich nicht löschen: Odoo antwortet «Breach records are append-only and cannot be deleted. Only an Odoo Administrator can archive a breach record with a written reason.» Nur ein Administrator kann sie archivieren, und ohne Begründung erscheint «Archive reason is required.»

Die Status im Einzelnen

New	Die Verletzung wurde gerade erfasst. Es kann nur die Bewertung begonnen werden.

Under Assessment	Auswirkung und Wahrscheinlichkeit werden bewertet. Von hier aus wird sie als der Aufsichtsbehörde gemeldet markiert.
DPA Notified	Jemand bestätigt, dass die Meldung außerhalb von Odoo erfolgt ist. Wenn die Risikostufe die Mitteilung nach Art. 34 vorsieht, kann sie als den Betroffenen mitgeteilt markiert werden.
Data Subjects Notified	Es wird vermerkt, dass die Betroffenen informiert wurden.
Closed	Die Verletzung ist abgeschlossen und kann nicht erneut geschlossen werden.

Regeln und Bedingungen

- **Start Assessment** ist nur im Status **New** sichtbar.
- **Mark DPA Notified** ist nur im Status **Under Assessment** sichtbar.
- **Mark Data Subjects Notified** ist nur im Status **DPA Notified** sichtbar und nur dann, wenn die Benachrichtigung nach Art. 34 verpflichtend ist.
- **Close** ist weder im Status **New** noch im Status **Closed** sichtbar.
- Die Workflow-Schaltflächen sind für die Gruppe der Modulmanager gedacht; **Archive (Admin Only)** ist nur für Odoo-Administratoren.
- Versucht ein Benutzer ohne diese Berechtigung zu archivieren, erscheint «Only Odoo Administrators can archive breach records.»
- Der Archivierungsassistent verlangt den **Archive Reason**; ohne ihn erscheint «Archive reason is required.»
- Art. 33 Abs. 1 verlangt die Meldung möglichst innerhalb von 72 Stunden. Erfolgt die Meldung nicht fristgerecht, sind die Gründe für die Verzögerung beizufügen.

Das Modul ändert nur den Status und vermerkt das Datum. Es meldet weder an die Aufsichtsbehörde noch informiert es Betroffene: Das tun Sie selbst, und hier halten Sie fest, was Sie getan haben.

Beschreibung und Folgen werden nur verschlüsselt gespeichert, wenn der Server den Verschlüsselungsschlüssel hat. Ohne ihn werden sie unverschlüsselt gespeichert, und die Konfiguration zeigt das unter **Encryption Key Configured** an.

Felder und Reiter des Datensatzes

Breach Details	Art, Zeitpunkt des Vorfalls, Zeitpunkt der Kenntnisnahme und die Meldefrist an die Aufsichtsbehörde.
Affected Data	**Categories of Data**, **Affected Data Subject Categories** und **Approximate Number of Affected Data Subjects**.
Description	Beschreibung, Folgen und **Measures Taken / Proposed**.
Risk Assessment	Auswirkung, Wahrscheinlichkeit, Punktzahl und Risikostufe.
DPA Notification	**DPA Notification Date/Time**, **Notification Method**, **DPA Reference Number** und Anhänge.
Art. 34 Notification	Falls gesendet: wann, und die Anhänge.
Post-Breach Review	Grundursache, Korrekturmaßnahmen, präventive Maßnahmen, wer genehmigt, und Datum.

In der Liste helfen die Filter **High/Critical Risk** und **DPA Notification Pending**, zu erkennen, was noch fehlt. Das Menü **Active Incidents** öffnet die Datenschutzverletzungen, die nicht geschlossen sind.

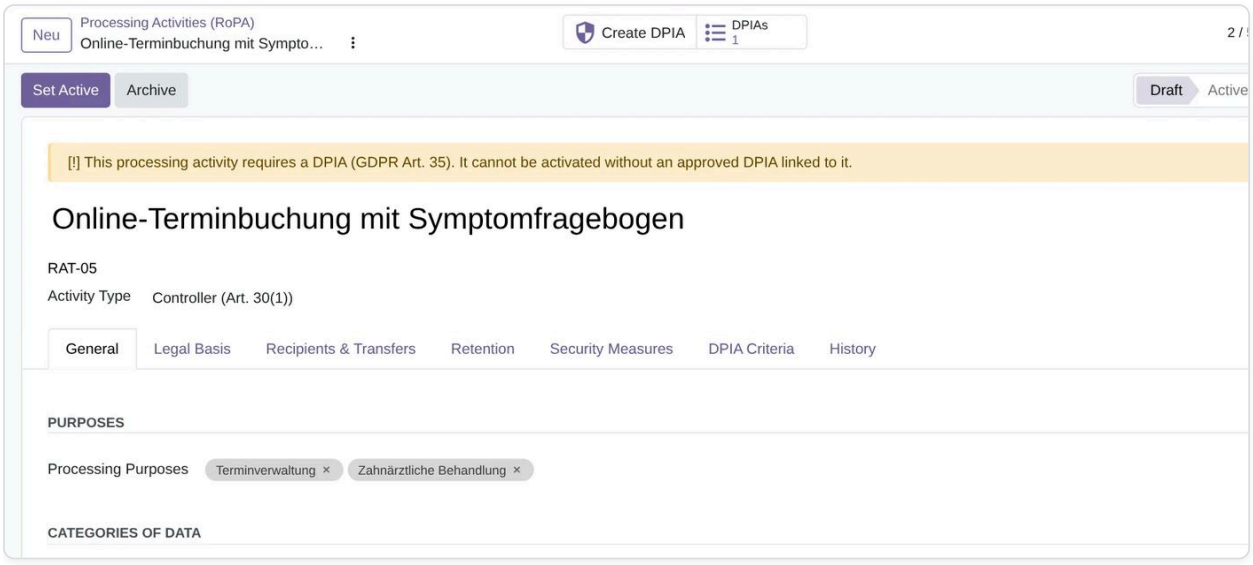
Ein Beispiel von Anfang bis Ende

Die erste Datenschutzverletzung auf den Screenshots ist eine **Confidentiality Breach**: Eine Röntgenaufnahme wurde per E-Mail an den falschen Patienten geschickt. Sie wurde eine Stunde nach dem Vorfall bekannt, Odoo setzte die Frist 72 Stunden später, und beim Öffnen blieben noch rund 42 Stunden. Betroffen sind Gesundheitsdaten von Patienten, die Risikostufe ist **Medium**, der Status **Under Assessment**, und es erscheint die Schaltfläche **Mark DPA Notified**. Die zweite, eine **Availability Breach** durch den Diebstahl des Laptops an der Rezeption bei verschlüsselter Festplatte, hat die Stufe **Low** und ist **Closed**: Bei einer geschlossenen Datenschutzverletzung bleibt nur die Schaltfläche **Archive (Admin Only)**.

MODUL-LEITFADEN · GDPR COMPLIANCE

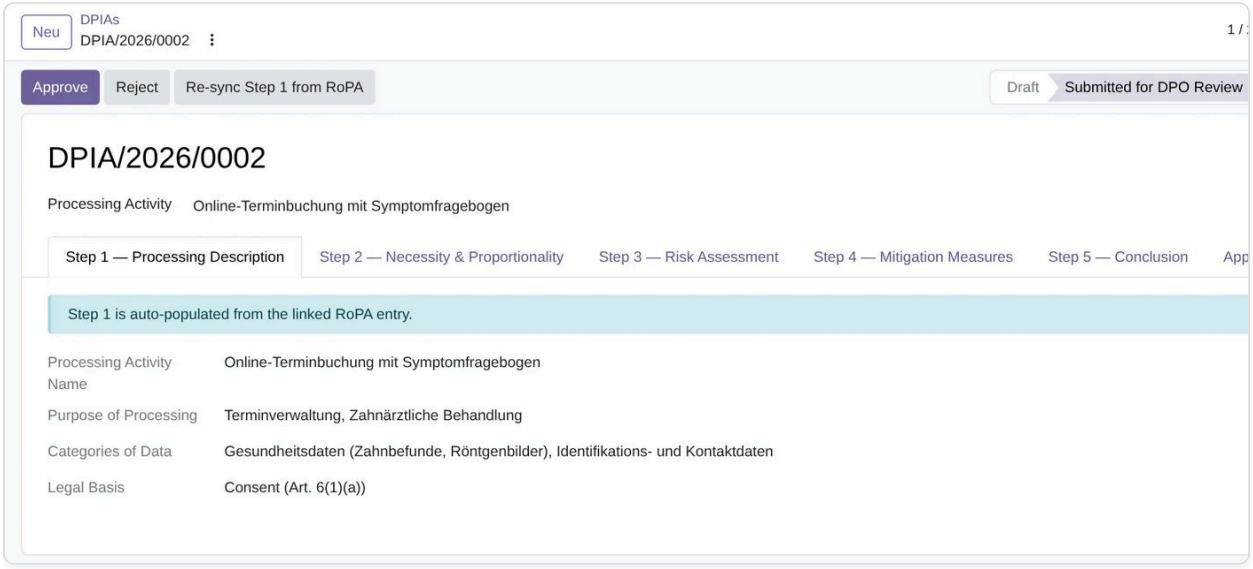
11 Die Datenschutz-Folgenabschätzungen (DSFA)

Auf dem Reiter **DPIA Criteria** jeder Aktivität gibt es neun Kontrollkästchen, eines pro Kriterium der WP248-rev.01-Leitlinien. Sind zwei oder mehr angekreuzt, oder ist die manuelle Markierung gesetzt, wird die Aktivität mit **DPIA Required** gekennzeichnet. Das ist eine allgemeine Regel dieser Leitlinien, keine gesetzliche Pflicht an sich. Die markierten Aktivitäten finden Sie unter **GDPR Toolkit › Processing Activities (RoPA) › DPIA Required**.



- **Echter Screenshot aus Odoo 20.** Eine Aktivität im Status **Draft** mit dem Hinweis, dass sie eine DPIA erfordert.

Die Bewertung öffnen Sie über die Karte der Aktivität oder über **GDPR Toolkit › DPIA › All DPIAs**. Die Referenz vergibt Odoo beim Anlegen des Datensatzes selbst.



- **Echter Screenshot aus Odoo 20.** Eine zur Prüfung eingereichte DPIA mit den Reitern der fünf Schritte und **Approval**.

Die fünf Schritte und der Genehmigungsreiter

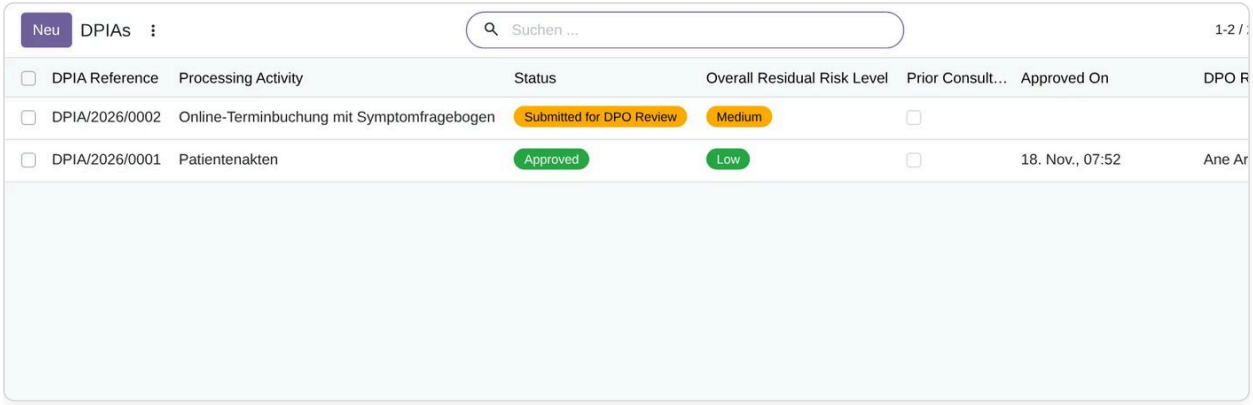
- Schritt 1, Beschreibung der Verarbeitung: Name, Zweck, Datenkategorien und Rechtsgrundlage nach Art. 6 werden automatisch aus der Tätigkeit im RAT übernommen.
- Schritt 2, Notwendigkeit und Verhältnismäßigkeit: Zweckbindung, Datenminimierung, Begründung der Speicherdauer und Maßnahmen für die Rechte der Betroffenen.
- Schritt 3, Risikobewertung: die Liste der identifizierten Risiken.
- Schritt 4, Risikominderungsmaßnahmen, als Freitext.
- Schritt 5, Schlussfolgerung und Restrisiko.
- Der Reiter **Approval**: wer eingereicht hat, wer geprüft hat, wann, und die Kommentare.

Jedes Risiko hat Auswirkung und Eintrittswahrscheinlichkeit vor den Maßnahmen und dieselben beiden Restwerte danach. Aus jedem Paar ergeben sich ein Punktwert und eine Stufe: bis 4 niedrig, bis 9 mittel, bis 19 hoch und ab 20 kritisch. Diese Matrix stammt vom Modul, nicht von der DSGVO und nicht von den Leitlinien des Europäischen Datenschutzausschusses. Bei hohem oder kritischem Restrisiko wird **Prior Consultation Required (Art. 36)** automatisch gesetzt. Wenn Sie die Konsultation einreichen, tragen Sie unter **Prior Consultation Submitted** und **Prior Consultation Notes** ein, was Sie selbst getan haben. Das Modul reicht sie nicht bei der Behörde ein.

Schaltflächen des Datensatzes

Submit for DPO Review	Setzt die DPIA von **Draft** auf **Submitted for DPO Review**. Nur im Status **Draft** sichtbar.
Approve	Genehmigt die DPIA. Nur im Status **Submitted for DPO Review** sichtbar.
Reject	Lehnt die DPIA ab. Nur im Status **Submitted for DPO Review** sichtbar und verlangt Kommentare des DSB.
Reset to Draft	Wenn sich eine DSFA im Status **Rejected** befindet, setzen Sie sie wieder auf **Draft** zurück.
Re-sync Step 1 from RoPA	Kopiert Schritt 1 erneut aus der Tätigkeit im RAT.

Die Status sind **Draft**, **Submitted for DPO Review**, **Approved** und **Rejected**. Die DPIAs, die auf Prüfung warten, finden Sie unter **GDPR Toolkit › DPIA › Awaiting DPO Review**.



- **Echter Screenshot aus Odoo 20.** Die Liste der DSFA mit Status und globalem Restrisiko.

> Einreichen, genehmigen und ablehnen dürfen nur die RGPD-Verwalter. Die endgültige Entscheidung liegt beim Verantwortlichen oder seinem DSB. Das Modul reicht die Konsultation nicht bei der Behörde ein und stellt keine Rechtsberatung dar.

> Eine Tätigkeit, die eine DSFA erfordert, wird ohne genehmigte verknüpfte DSFA nicht aktiviert: Die Tätigkeitsansicht weist darauf hin.

Status der DSFA

STATUS	BEDEUTUNG
Draft	Das ist der Ausgangsstatus: Die Schritte werden ausgefüllt, und **Submit for DPO Review** ist sichtbar.
Submitted for DPO Review	Die DPIA wartet auf die Entscheidung des DSB. In diesem Status sind **Approve** und **Reject** sichtbar.
Approved	Der DSB hat sie genehmigt, und das Datum steht unter **Approved On**.
Rejected	Der DSB hat sie mit Kommentaren abgelehnt. Die Schaltfläche **Reset to Draft** setzt sie zurück auf **Draft**.

Wann es nicht erlaubt ist

- Einreichen, Genehmigen und Ablehnen dürfen nur GDPR-Manager. Wer keiner ist, erhält je nach Schaltfläche die Meldung «Only GDPR Managers can submit a DPIA for review.», «Only GDPR Managers (acting as DPO) can approve a DPIA.» oder «Only GDPR Managers (acting as DPO) can reject a DPIA.»
- Ablehnen, ohne etwas in **DPO Comments** einzutragen, ergibt die Meldung «DPO comments are required when rejecting a DPIA.».
- **Reset to Draft** ist nur sichtbar, wenn sich die DPIA im Status **Rejected** befindet.

Felder und Reiter des Datensatzes

DPIA Reference	Odoo vergibt sie beim Anlegen des Datensatzes; sie ist nicht editierbar.
Processing Activity	Die Tätigkeit im RAT, zu der die DSFA gehört. Pflichtfeld.
Overall Residual Risk Level	Odoo berechnet es: Es ist das höchste der Restrisiken in der Liste.

Submitted By und **Submitted On**	Wer die DSFA zur Prüfung eingereicht hat und wann.
DPO Reviewer und **DPO Review Date**	Wer sie geprüft hat und wann.
DPO Comments	Text der Prüfung. Pflichtfeld bei Ablehnung.
Prior Consultation Submitted und **Prior Consultation Notes**	Was Sie vermerken, wenn Sie die Konsultation nach Art. 36 eingereicht haben. Das Modul reicht sie nicht ein.

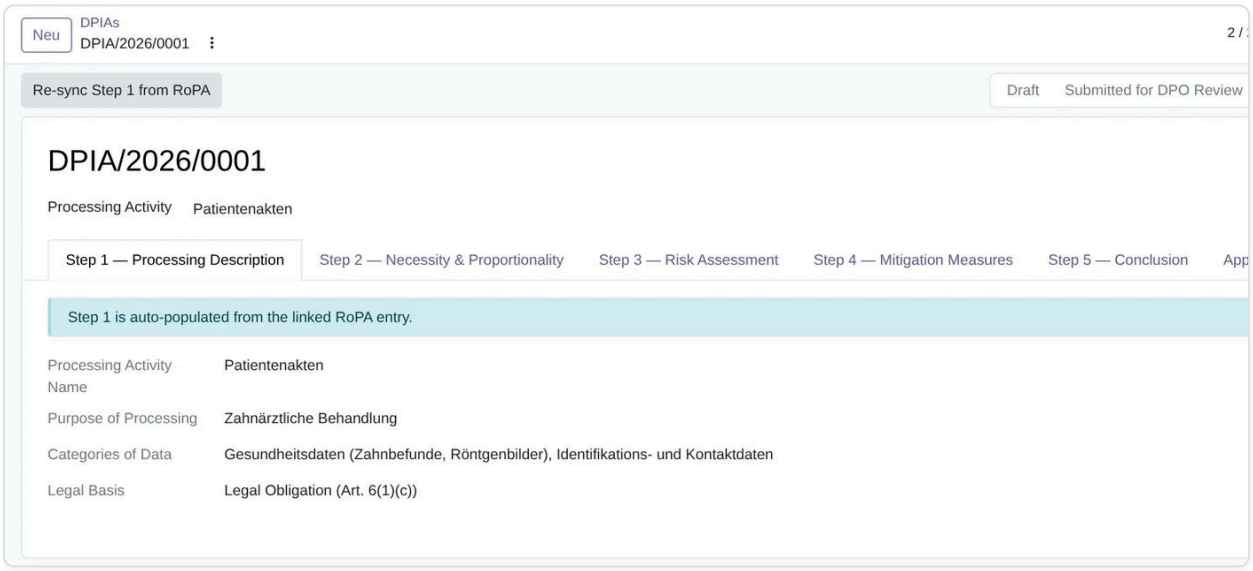
Die Ansicht hat sechs Reiter: die fünf Schritte und **Approval**. Jeder Schritt hat seine eigenen Texte, und mit **Re-sync Step 1 from RoPA** aktualisieren Sie Schritt 1, wenn Sie etwas an der Aktivität ändern. Die Filter sind **Awaiting DPO Review**, **Approved** und **High/Critical Residual Risk**, mit den Gruppierungen **By Status** und **By Risk Level**.

So wird das Risiko berechnet

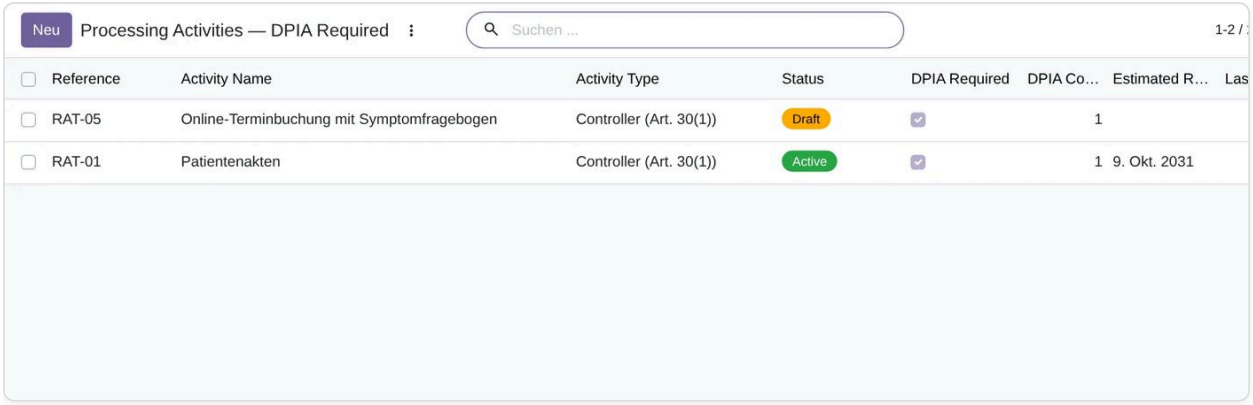
Jedes Risiko bewertet seine Auswirkung von unerheblich (1) bis katastrophal (5) und seine Eintrittswahrscheinlichkeit von sehr gering (1) bis sehr hoch (5). Beide werden multipliziert, und es ergibt sich ein Punktwert von 1 bis 25. Bis 4 ist **Low**, bis 9 ist **Medium**, bis 19 ist **High** und ab 20 ist **Critical**. Nach den Maßnahmen wird mit der Rest-Auswirkung und der Rest-Eintrittswahrscheinlichkeit wiederholt. Diese Schwellen stammen vom Modul. Bei hohem oder kritischem Restrisiko wird die Vorabkonsultation nach Art. 36 Abs. 1 markiert. Sie verlangt, die Behörde vor der Verarbeitung zu konsultieren, wenn die Bewertung ergibt, dass die Verarbeitung ohne risikomindernde Maßnahmen ein hohes Risiko zur Folge hätte.

Ein Beispiel von Anfang bis Ende

Im Beispiel der Screenshots ist die Aktivität RAT-05, die Online-Terminbuchung mit Symptomfragebogen, im Status **Draft** und trägt **DPIA Required**. Ihre Karte weist darauf hin, dass sie sich ohne genehmigte DPIA nicht aktivieren lässt. Von dort wird die DPIA angelegt, sie erhält die Nummer DPIA/2026/0002, und Schritt 1 enthält bereits Zweck, Datenkategorien und Rechtsgrundlage der Aktivität. Nach dem Ausfüllen der übrigen Schritte wird sie zur Prüfung eingereicht und steht in der Liste im Status **Submitted for DPO Review** mit dem Restrisiko **Medium**. Der DSB sieht sie unter **Awaiting DPO Review** und genehmigt oder lehnt sie mit seinen Kommentaren ab. Solange sie nicht genehmigt ist, bleibt die Aktivität im Status **Draft**.



- **Echter Screenshot aus Odoo 20.** Die DPIA der Patientenakte im Status **Approved**.

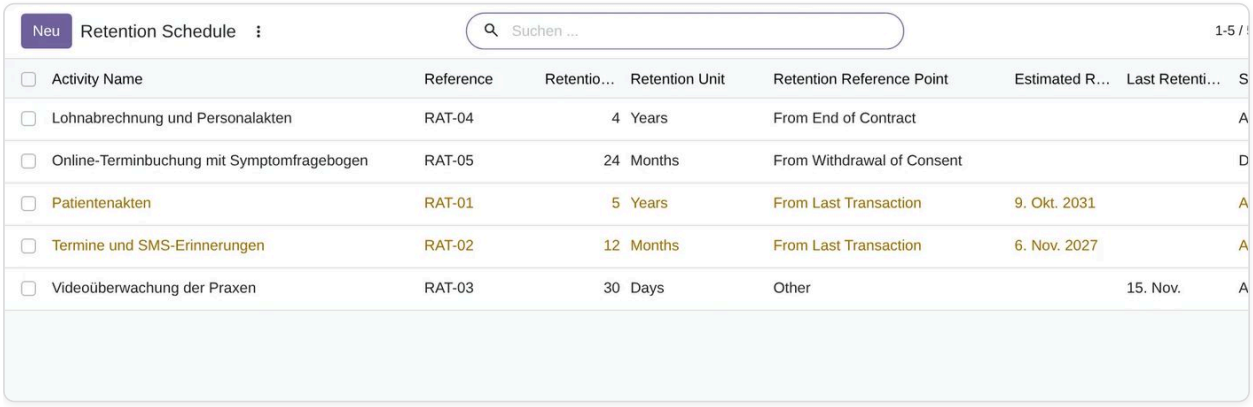


- **Echter Screenshot aus Odoo 20.** Die Aktivitäten mit **DPIA Required** und ihre DPIA-Nummer.

> Was dieses Modul nicht tut: Es reicht die vorherige Konsultation nicht bei der Behörde ein und entscheidet nicht für Sie, ob die Bewertung annehmbar ist. Die endgültige Entscheidung liegt beim Verantwortlichen oder seinem DSB, und dies ist keine Rechtsberatung.

MODUL-LEITFADEN · GDPR COMPLIANCE

12 Die Aufbewahrung und ihre Überprüfungen



- **Echter Screenshot aus Odoo 20.** Der **Retention Schedule** mit den fünf Verarbeitungstätigkeiten des Verzeichnisses.

Die Frist jeder Tätigkeit (Dauer, Einheit und Beginn der Berechnung) tragen Sie auf dem Reiter **Retention** der Tätigkeit ein, unter **GDPR Toolkit › Processing Activities (RoPA) › All Activities**. Odoo berechnet das **Estimated Retention End Date** nur, wenn der Beginn der Berechnung **Fixed Date** oder **From Last Transaction** ist und dieses Datum gesetzt ist. Bei **From End of Contract**, **From Withdrawal of Consent** oder **Other** bleibt es leer, und diese Tätigkeit erhält keine Erinnerung. Der **Retention Schedule** zeigt die Tätigkeiten mit gesetzter Frist, ihr geschätztes Datum und die **Last Retention Review**, die sich bei jedem Speichern einer Überprüfung automatisch aktualisiert.

Die Erinnerung kommt von der geplanten Aktion **GDPR: Retention Expiry Check**, die jeden Tag läuft. Für jede aktive Tätigkeit, deren geschätztes Datum innerhalb der Tage von **Retention Advance Warning (days)** liegt und die in den letzten 30 Tagen nicht überprüft wurde, legt sie eine Aktivität im Datensatz an und sendet eine E-Mail an die Empfänger der Benachrichtigungen aus den Einstellungen oder, falls keine hinterlegt sind, an die DSGVO-Verantwortlichen. Eine weitere Aktion, **GDPR: Annual RoPA Review Reminder**, erinnert einmal im Jahr daran, dass das Verzeichnis der Verarbeitungstätigkeiten durchzusehen ist.

Wo eine Überprüfung erfasst wird

Die Überprüfungen finden Sie unter **GDPR Toolkit › Retention Management › Review History**, dort öffnet sich die Liste **Retention Review History**. Eine Überprüfung legen Sie mit **Neu** an, und sie enthält diese Felder:

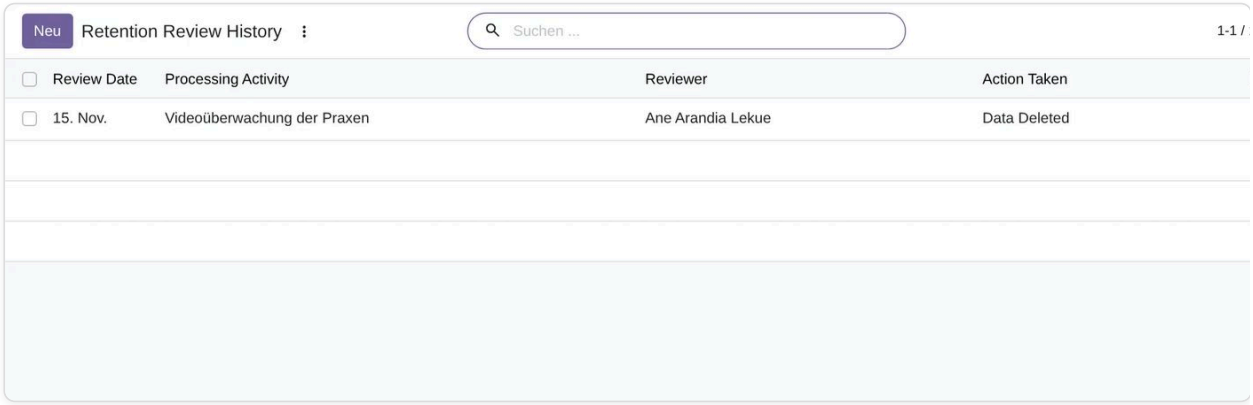
Processing Activity	Die Tätigkeit, die Sie überprüfen. Pflichtfeld.
Review Date	Wird mit dem heutigen Datum vorbelegt. Pflichtfeld.
Reviewer	Wird mit Ihrem Benutzer vorbelegt. Pflichtfeld.
Action Taken	Was Sie nach der Überprüfung getan haben. Pflichtfeld. Es gibt vier Optionen: **Data Deleted**, **Data Anonymised**, **Retention Extended** und die Option für überprüft ohne erforderliche Maßnahme.
Extension Justification	Der Grund für die Verlängerung der Aufbewahrung.
New Retention End Date	Das Datum, bis zu dem Sie die Aufbewahrung verlängern.
Notes	Freitext.

Der Datensatz der Überprüfung hat keine eigenen Schaltflächen oder Status. Die Optionen unter **Action Taken** sind das, was Sie festhalten, kein Status des Datensatzes.

So erfassen Sie eine Überprüfung

1. ### Den Verlauf öffnen

   Öffnen Sie **GDPR Toolkit › Retention Management › Review History** und klicken Sie auf **Neu**.



   - **Echter Screenshot aus Odoo 20.** Der **Retention Review History** mit einer bereits erfassten Überprüfung.

2. ### Die Tätigkeit wählen

   Füllen Sie **Processing Activity** aus. Das heutige Datum und Ihr Benutzer sind bereits eingetragen.

3. ### Die Maßnahme angeben

   Wählen Sie unter **Action Taken**, was Sie mit den Daten getan haben.

4. ### Wenn Sie die Aufbewahrung verlängern

   Bei **Retention Extended** füllen Sie **Extension Justification** und **New Retention End Date** aus.

5. ### Speichern

   Beim Speichern wird die **Last Retention Review** der Tätigkeit auf das Datum dieser Überprüfung gesetzt.

> Das Modul löscht oder anonymisiert keine Daten. Die Optionen **Data Deleted** und **Data Anonymised** halten nur fest, was Sie selbst außerhalb dieses Bildschirms getan haben. Bei **Retention Extended** lässt Odoo das Speichern nicht zu, wenn die Begründung («Extension justification is required when extending retention.») oder das neue Datum («New retention end date is required when extending retention.») fehlt. Das **New Retention End Date** bleibt in der Prüfung gespeichert, ändert aber nicht das geschätzte Datum der Aktivität: Um es zu verschieben, ändern Sie die Frist oder ihr Bezugsdatum auf dem Reiter **Retention**.

Was eine Überprüfung speichert

Jede Überprüfung verknüpft eine Verarbeitungstätigkeit mit dem Datum, an dem Sie sie überprüft haben, mit der Person, die es getan hat, und mit Ihrer Entscheidung. Die Firma wird automatisch von der Tätigkeit übernommen. Gespeichert wird nur, was Sie entschieden und getan haben: Das Modul löscht oder ändert keine Daten.

Die vier möglichen Maßnahmen

Data Deleted	Sie halten fest, dass die Daten nach der Überprüfung gelöscht wurden. Die Löschung nehmen Sie außerhalb des Moduls vor.
Data Anonymised	Sie halten fest, dass die Daten anonymisiert wurden. Die Anonymisierung nehmen Sie außerhalb des Moduls vor.
Retention Extended	Sie entscheiden, die Daten weiter aufzubewahren. Dafür sind eine Begründung und ein neues Aufbewahrungsende erforderlich, das in der Überprüfung gespeichert wird: Das geschätzte Datum der Tätigkeit ändert sich nicht.
Die Option für überprüft ohne erforderliche Maßnahme	Sie haben die Tätigkeit überprüft, und es ist nichts zu tun. Dies ist die vierte Option in der Liste **Action Taken**.

Regeln und Bedingungen

- Bei **Retention Extended** ohne **Extension Justification** speichert Odoo nicht und zeigt «Extension justification is required when extending retention.».
- Bei **Retention Extended** ohne **New Retention End Date** speichert Odoo nicht und zeigt «New retention end date is required when extending retention.».
- Bei den anderen drei Maßnahmen werden diese beiden Felder nicht verlangt.
- **Processing Activity**, **Review Date**, **Reviewer** und **Action Taken** sind Pflichtfelder.

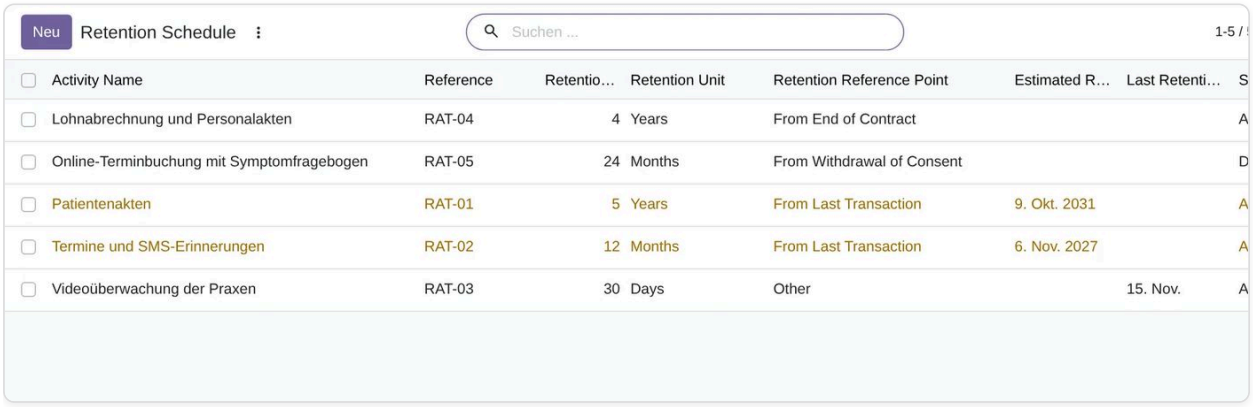
Jede gespeicherte Überprüfung aktualisiert auf der Tätigkeit die **Last Retention Review** mit dem **Review Date** dieser Überprüfung. Das sehen Sie in den Spalten des **Retention Schedule** und in der Liste der **Processing Activities (RoPA)**.

Die Erinnerungen

Die Aktion **GDPR: Retention Expiry Check** läuft jeden Tag. Sie warnt vor aktiven Tätigkeiten, deren geschätztes Enddatum innerhalb der Tage von **Retention Advance Warning (days)** liegt (standardmäßig 30) und die in den letzten 30 Tagen nicht überprüft wurden: Sie legt eine Aktivität im Datensatz an und sendet eine E-Mail. Eine Tätigkeit ohne geschätztes Datum erhält keine Erinnerung. Die Aktion **GDPR: Annual RoPA Review Reminder** erinnert einmal im Jahr daran, das Verzeichnis der Verarbeitungstätigkeiten zu überprüfen.

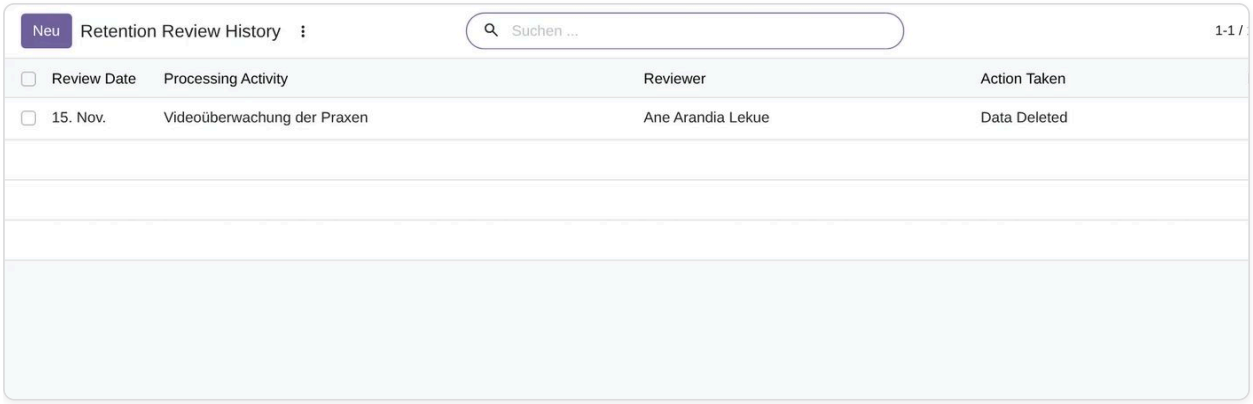
Ein Beispiel von Anfang bis Ende

Der **Retention Schedule** in den Bildschirmen enthält fünf Tätigkeiten. Die Krankenakte von Patienten wird 5 Jahre ab der letzten Transaktion aufbewahrt, und Termine sowie SMS-Erinnerungen 12 Monate: Beide haben ein geschätztes Enddatum. Die Videoüberwachung der Kliniken (30 Tage, mit Beginn der Berechnung **Other**), die Gehaltsabrechnungen (4 Jahre ab Vertragsende) und die Online-Terminbuchungs-App (24 Monate ab Widerruf der Einwilligung) haben keines, weil ihr Beginn der Berechnung ein Datum ist, das Odoo nicht kennt.



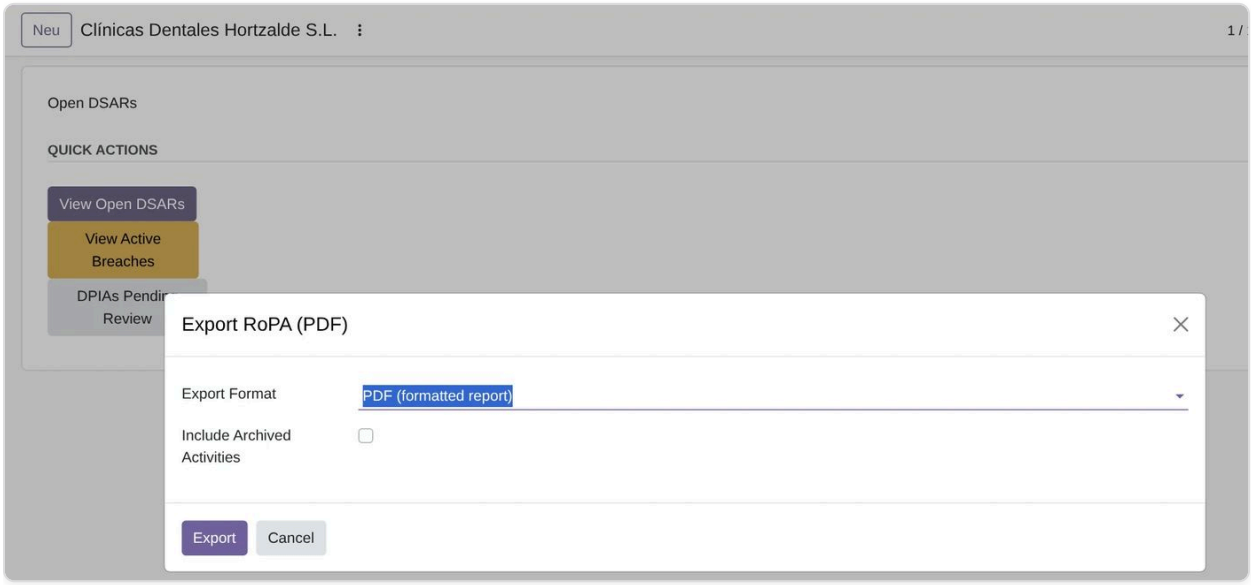
- **Echter Screenshot aus Odoo 20.** Der **Retention Schedule** mit den fünf Tätigkeiten und ihren geschätzten Daten.

In der **Retention Review History** gibt es eine Überprüfung der Videoüberwachung der Kliniken, durchgeführt von Ane Arandia Lekue, mit der Maßnahme **Data Deleted**. Sie enthält kein neues Aufbewahrungsende, weil diese Maßnahme es nicht verlangt. Im Kalender wird dieses Datum zur letzten Überprüfung der Tätigkeit.



- **Echter Screenshot aus Odoo 20.** Der **Retention Review History** mit der Überprüfung der Videoüberwachung.

13 Berichte, Exporte und Audit-Protokoll



- **Echter Screenshot aus Odoo 20.** Der Exportassistent des Verzeichnisses, mit dem Format und dem Kontrollkästchen für archivierte Tätigkeiten.

Das Verzeichnis exportieren

1. **Das Exportmenü öffnen**
   Öffnen Sie **GDPR Toolkit › Reports › Export RoPA (PDF)** oder **GDPR Toolkit › Reports › Export RoPA (Excel)**. Beide öffnen denselben Assistenten.

2. **Das Format wählen**
   Unter **Export Format** wählen Sie **PDF (formatted report)** oder **Excel (.xlsx)**. Vorbelegt ist das Format des Menüs, über das Sie gekommen sind.

3. **Über die archivierten Tätigkeiten entscheiden**
   Setzen Sie **Include Archived Activities**, wenn sie im Bericht erscheinen sollen. Ohne Häkchen fehlen archivierte Tätigkeiten.

4. **Auf Export klicken**
   Die Datei wird erzeugt. **Cancel** schließt den Assistenten, ohne etwas zu erzeugen.

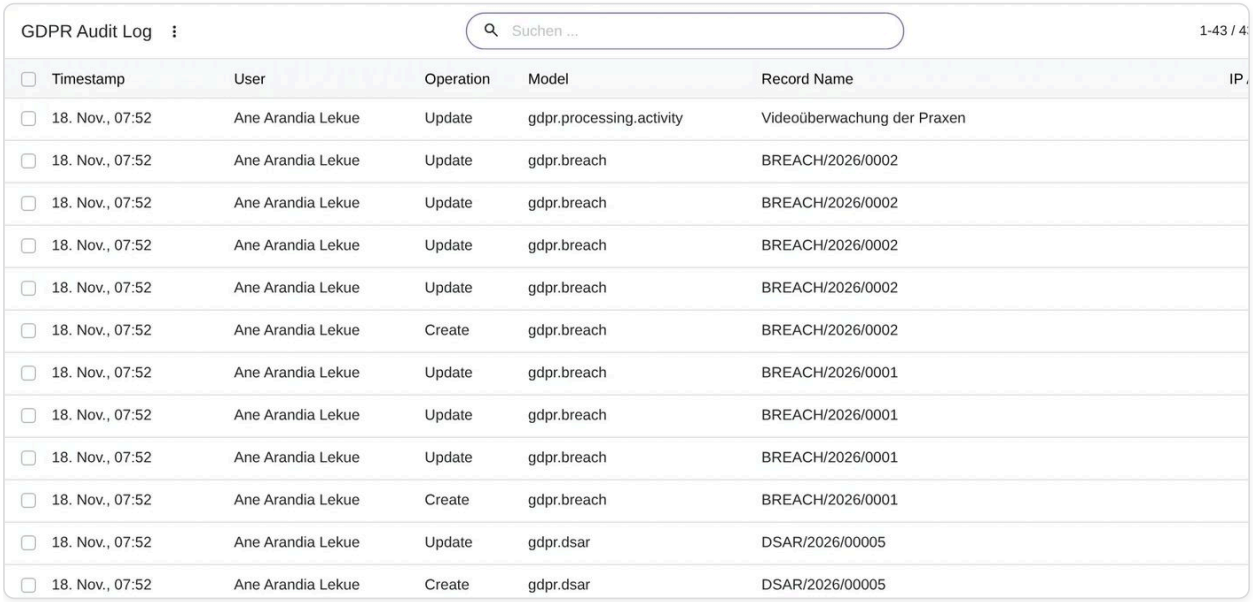
Die Excel-Datei enthält eine Zeile pro Tätigkeit. Die Spaltenüberschriften erscheinen in allen Sprachen auf Englisch.

- Wenn Ihr Unternehmen keine Verarbeitungstätigkeiten hat, meldet der Assistent «No processing activities found for this company.».
- Fehlt die Excel-Bibliothek auf dem Server, meldet er «openpyxl is not installed. Please install it via pip to use Excel export.». Sie muss auf dem Server installiert werden.

Weitere Berichte

Im selben Menü **Reports** öffnet **DSAR History Report** die Liste aller Anfragen, **Breach Log Report** die der Verletzungen und **DPIA Status Report** die der DSFA, um sie zu filtern, zu gruppieren oder zu exportieren. Jede Anfrage, Verletzung, DSFA und Tätigkeit können Sie im Datensatz als PDF drucken.

Audit-Protokoll



- **Echter Screenshot aus Odoo 20.** Das **GDPR Audit Log** mit Datum und Uhrzeit, Benutzer, Vorgang, Modell, Datensatzname und IP-Adresse.

Jeder Eintrag hält fest, wer die Änderung vorgenommen hat, wann, an welchem Datensatz und von welcher IP-Adresse aus. Die Änderungsübersicht schwärzt Felder mit personenbezogenen Daten. Erfasst werden die Vorgänge **Create**, **Update**, **Archive**, **Export** und **Portal Submission**.

Create Operations	Filter, der nur die Neuanlagen zeigt.
Updates	Filter, der nur die Änderungen zeigt.
Exports	Filter, der nur die Exporte zeigt.
By User	Gruppiert die Einträge nach Benutzer.
By Model	Gruppiert die Einträge nach Modell.
Change Summary	Auf der Maske jedes Eintrags: die geänderten Felder, mit durchgestrichenen personenbezogenen Daten.

> Niemand kann Einträge im Audit-Protokoll ändern oder löschen, auch kein Administrator. Odoo meldet «You do not have access rights to modify GDPR Audit Log records. Audit log entries are immutable compliance records.» oder «You do not have access rights to delete GDPR Audit Log records. They are permanent compliance records per Art. 5(2) GDPR accountability principle.».

Welche Optionen der Exportassistent hat

PDF (formatted report)	Formatierter Bericht, lesefertig oder zum Drucken. Er ist vorausgewählt, wenn Sie über **Export RoPA (PDF)** einsteigen.
Excel (.xlsx)	Tabelle mit einer Zeile pro Tätigkeit, zum eigenen Filtern und Sortieren.
Include Archived Activities	Am Anfang nicht gesetzt. Gesetzt, erscheinen archivierte Tätigkeiten im Bericht.

Beide Exportmenüs führen zum selben Assistenten.

Wann kein Export möglich ist

- Hat Ihr Unternehmen keine Verarbeitungstätigkeiten, meldet der Assistent «No processing activities found for this company.» und erzeugt nichts.
- Fehlt die Excel-Bibliothek auf dem Server, schlägt der Excel-Export mit «openpyxl is not installed. Please install it via pip to use Excel export.» fehl.

Die Vorgänge im Audit-Protokoll

VORGANG	WAS ERFASST WIRD
Create	Die Neuanlage eines Datensatzes.
Update	Eine Änderung an einem bestehenden Datensatz.
Archive	Die Archivierung eines Datensatzes.
Export	Der Export des RoPA nach Excel oder der Export der Datenübertragbarkeit.
Portal Submission	Eine Anfrage, die über das Datenschutzportal eingereicht wurde.

Felder des Eintrags

Timestamp	Wann es geschehen ist. Wird automatisch ausgefüllt.
User	Wer es gemacht hat.
Operation	Eine der oben genannten fünf.
Model und **Record Name**	Um welche Art von Datensatz es sich handelt und wie er heißt.
Record ID	Numerische Kennung des geänderten Datensatzes.
Die IP-Adresse	Von wo aus es gemacht wurde.
Change Summary	Namen der geänderten Felder und ihre Werte. Felder mit personenbezogenen Daten werden maskiert.
Company	Das Unternehmen, zu dem der Eintrag gehört.

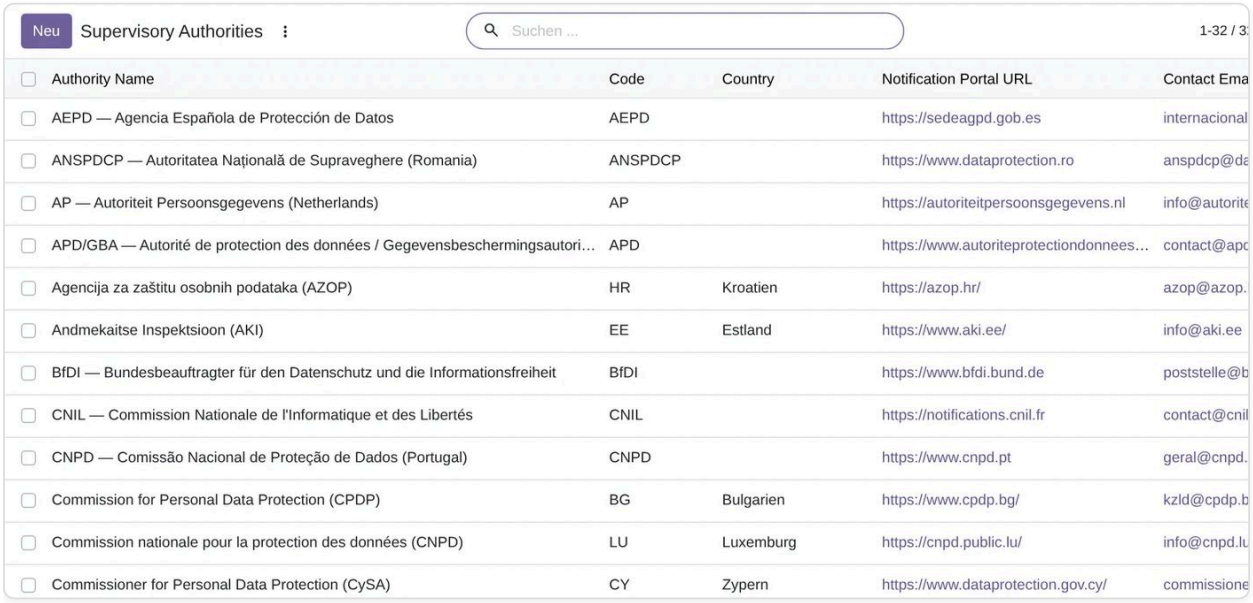
Was nicht möglich ist

Einträge können nur erstellt werden. Jeder Versuch, sie zu ändern oder zu löschen, unabhängig vom Benutzer, endet mit einer Fehlermeldung. Die Meldung verweist auf Art. 5 Abs. 2 DSGVO, den Grundsatz der Rechenschaftspflicht, als Grund für die Aufbewahrung.

Ein Beispiel von Anfang bis Ende

Sie öffnen **GDPR Toolkit › Reports › Export RoPA (Excel)**, lassen **Include Archived Activities** deaktiviert und klicken auf **Export**. Sie erhalten die Datei mit einer Zeile pro Aktivität. Danach öffnen Sie **GDPR Toolkit › Configuration › Audit Log** und filtern nach **Exports**: Dort sehen Sie den Export mit Ihrem Benutzer und Datum sowie Uhrzeit. In derselben Liste erscheinen die Anlagen und Änderungen Ihrer Aktivitäten und Verletzungen, mit dem Namen jedes Datensatzes.

14 Aufsichtsbehörden und Rechtsgrundlagen



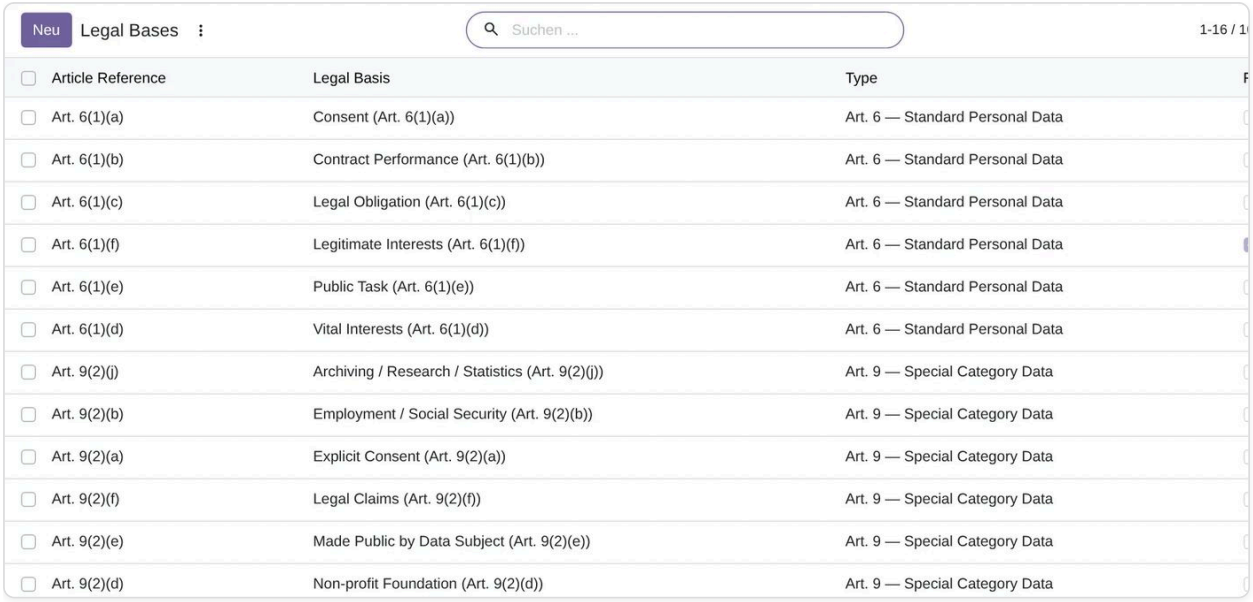
Authority Name	Code	Country	Notification Portal URL	Contact Ema
AEPD — Agencia Española de Protección de Datos	AEPD		https://sedeagpd.gob.es	internacional
ANSPDCP — Autoritatea Națională de Supraveghere (Romania)	ANSPDCP		https://www.dataprotection.ro	anspdcp@da
AP — Autoriteit Persoonsgegevens (Netherlands)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

- **Echter Screenshot aus Odoo 20.** Die Liste **Supervisory Authorities** mit ihren 32 Einträgen.

Das Modul enthält 32 Aufsichtsbehörden. Sie finden sie unter **GDPR Toolkit › Configuration › Supervisory Authorities**. Sie werden einmal bei der Installation geladen. Es gibt keine geplante Aufgabe und keine Schaltfläche zur Aktualisierung, und nur ein Administrator von Odoo kann sie ändern.

Authority Name	Vollständiger Name der Behörde. Pflichtfeld.
Country	Land, zu dem die Behörde gehört.
Code	Kürzel der Behörde, zum Beispiel AEPD, CNIL oder BfDI.
Notification Portal URL	Adresse des Portals, über das Meldungen eingereicht werden.
Contact Email	Kontakt-E-Mail der Behörde.
Breach Notification Form URL	Adresse des Formulars zur Meldung einer Verletzung.
Active	Kontrollkästchen, das angibt, ob die Behörde in Verwendung ist. Es ist standardmäßig aktiviert.

Die federführende Behörde wählen Sie unter **GDPR Toolkit › Configuration › DPO & Settings**.



- **Echter Screenshot aus Odoo 20.** Die Liste **Legal Bases** mit ihren 16 Einträgen.

Die Rechtsgrundlagen finden Sie unter **GDPR Toolkit › Configuration › Legal Bases**. Es sind 16, und sie werden bei der Installation geladen: die aus Artikel 6 und die aus Artikel 9.

Legal Basis	Bezeichnung der Grundlage. Pflichtfeld.
Article Reference	Artikelverweis, zum Beispiel Art. 6 Abs. 1 lit. a.
Type	Gibt an, ob es sich um eine Grundlage aus Artikel 6 für gewöhnliche personenbezogene Daten oder aus Artikel 9 für besondere Kategorien personenbezogener Daten handelt.
Requires Legitimate Interests Balancing Test	Kontrollkästchen, das die Grundlagen markiert, die diese Interessenabwägung verlangen.

> Diese Listen haben weder Status noch Workflow. Beide werden bei der Installation des Moduls geladen, und nur ein Administrator von Odoo kann sie ändern.

Was jede Liste enthält und wie sie identifiziert wird

Jede Behörde hat drei Angaben zur Identifikation: ihren **Authority Name**, ihr **Country** und ihren **Code**. Der Code ist Freitext, und der Hilfetext des Feldes nennt als Beispiele AEPD, CNIL und BfDI. Die drei übrigen Angaben (das Meldeportal, die Kontakt-E-Mail und das Verletzungsformular) sind Adressen bzw. eine E-Mail-Adresse, die Sie im Datensatz einsehen können.

Aktiv oder nicht aktiv

Jede Behörde hat das Kontrollkästchen **Active**, standardmäßig aktiviert. Es ist das einzige Merkmal des Datensatzes, das angibt, ob eine Behörde als in Verwendung gilt. Die Rechtsgrundlagen haben ebenfalls ein Aktiv-Feld, das aber auf keinem Bildschirm des Moduls erscheint, sodass Sie es in der Oberfläche weder sehen noch ändern können.

Die beiden Arten von Rechtsgrundlagen

TYP	WAS SIE ENTHÄLT
Grundlage aus Artikel 6	Die Grundlagen für die Verarbeitung gewöhnlicher personenbezogener Daten.
Grundlage aus Artikel 9	Die Grundlagen für die Verarbeitung besonderer Kategorien personenbezogener Daten.

Die Interessenabwägung

Das Kontrollkästchen **Requires Legitimate Interests Balancing Test** markiert die Grundlagen, die diese Abwägung verlangen. In der Liste erscheint zum Beispiel **Legitimate Interests (Art. 6(1)(f))**, mit dem Artikelverweis in der entsprechenden Spalte. Die Beschreibung jeder Grundlage existiert im Modell, wird aber auf keinem Bildschirm angezeigt.

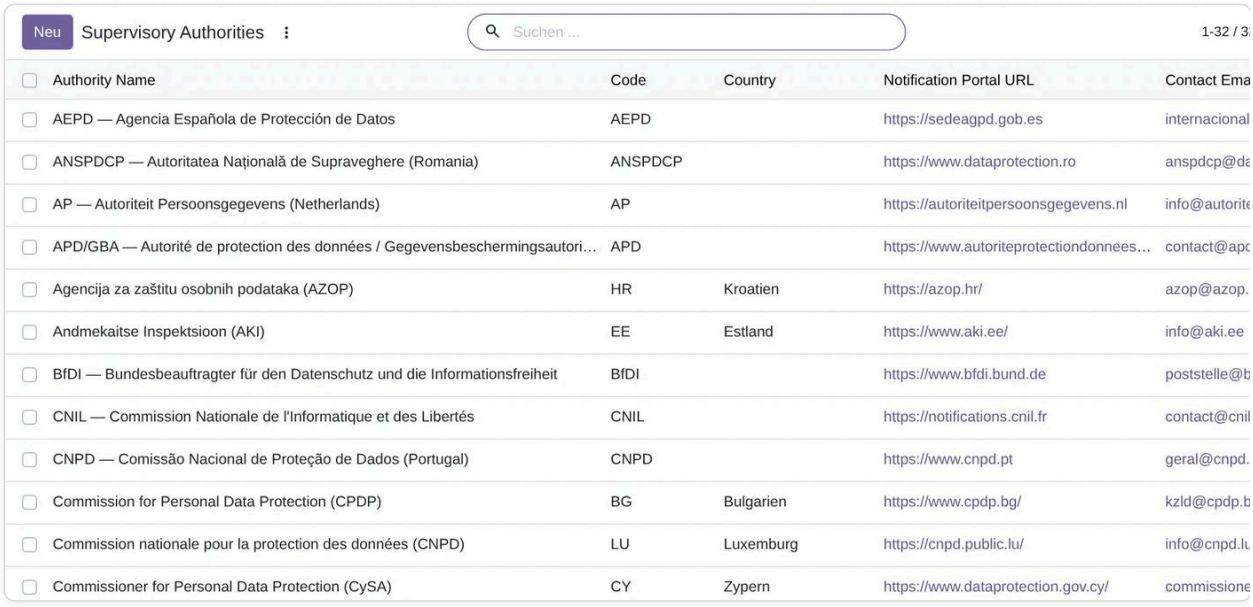
Regeln und Grenzen

- Der Name der Behörde und der Name der Rechtsgrundlage sind Pflichtfelder.
- Die Art der Grundlage ist ein Pflichtfeld und steht, wenn Sie nichts ändern, auf Grundlage aus Artikel 6.
- Die Listen werden bei der Installation geladen. Das Modul lädt sie nicht erneut und aktualisiert sie nicht von selbst.
- Das Modul meldet nichts an die Behörde. Das Portal und das Formular sind Adressen, über die Sie von außen melden und hier festhalten, was Sie getan haben.

Ein Beispiel von Anfang bis Ende

1 Die Behörden öffnen

Öffnen Sie **GDPR Toolkit › Configuration › Supervisory Authorities**. Die Liste zeigt 32 Einträge, darunter die AEPD: ihr Code ist AEPD.

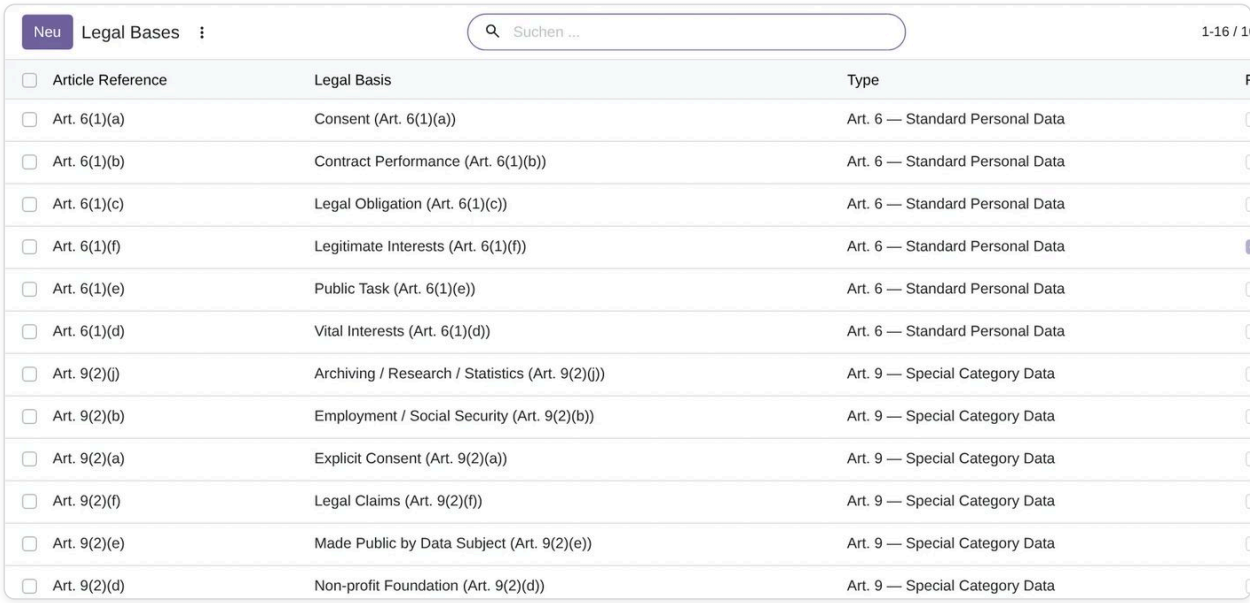


- **Echter Screenshot aus Odoo 20.** Die Liste zeigt Name, Code, Land, Portal und E-Mail jeder Behörde.

2 Die Rechtsgrundlagen öffnen

Öffnen Sie **GDPR Toolkit › Configuration › Legal Bases**. Die Liste zeigt 16 Einträge. Suchen Sie **Consent (Art. 6(1)(a))** und **Legitimate Interests (Art. 6(1)(f))**, bei der die Markierung für die Interessenabwägung

gesetzt ist.



- **Echter Screenshot aus Odoo 20.** Die Liste zeigt den Artikelverweis, die Rechtsgrundlage und ihren Typ.

MODUL-LEITFADEN · GDPR COMPLIANCE

15 Was an FlexigoTech Cloud geht und was zurückkommt

DATUM	RICHTUNG	WANN
Die Identifikation der Installation: ihre Kennung, ihre Adresse und ihr öffentlicher Code, die Odoo-Version und die Namen ihrer Module	Von Ihrem Odoo zu FlexigoTech Cloud	Beim Verbinden der Installation mit dem Dienst
Die Annahme der Bedingungen und des Auftragsverarbeitungsvertrags mit der E-Mail-Adresse der annehmenden Person	Von Ihrem Odoo zu FlexigoTech Cloud	Wenn Sie **Verbinden und Testphase starten** klicken, nachdem Sie bestätigt haben, dass Sie die Liste gelesen haben
Die Anfrage um Berechtigung des Dienstes für das Modul	Von Ihrem Odoo zu FlexigoTech Cloud	Die Module fragen automatisch; **Jetzt prüfen** fragt im Moment der Auslösung
Die Anfragen für die Hinweise der Überwachung	Von Ihrem Odoo zu FlexigoTech Cloud	Alle 6 Stunden, wenn die Installation neue Hinweise anfordert
Die Hinweise der Überwachung	Von FlexigoTech Cloud zu Ihrem Odoo	Bei der nächsten Anfrage, nachdem sich eine Quelle geändert hat

Was der Dienst überwacht

FlexigoTech Cloud prüft jeden Tag sechs offizielle Quellen und meldet, wenn sich eine davon ändert. Es handelt sich um die Rechtsakte der Europäischen Union, die die DSGVO ändern, veröffentlicht im Amt für Veröffentlichungen; das Verfahren 2025/0360(COD), als Digital-Omnibus bekannt, im Legislativen

Beobachtungsdienst des Europäischen Parlaments; das konsolidierte LOPDGDD im BOE; die Seite der Angemessenheitsbeschlüsse der Europäischen Kommission; und die Seiten mit Leitfäden und Werkzeugen der AEPD.

Die Hinweise erscheinen unter **Einstellungen › FlexigoTech Cloud** und kommen außerdem in einer täglichen E-Mail.

Was in Ihrem Odoo bleibt

Das Verzeichnis der Verarbeitungstätigkeiten, die Anträge der Betroffenen, die Verletzungen, die Datenschutz-Folgenabschätzungen und das Audit-Protokoll bleiben in Ihrer Datenbank. Das Modul sendet davon nichts an FlexigoTech oder an einen externen Dienst. Der Verbindungsbildschirm erinnert daran: Ihre Kunden, Bestellungen, Rechnungen und Produkte werden durch diese Verbindung nicht an FlexigoTech Cloud gesendet.

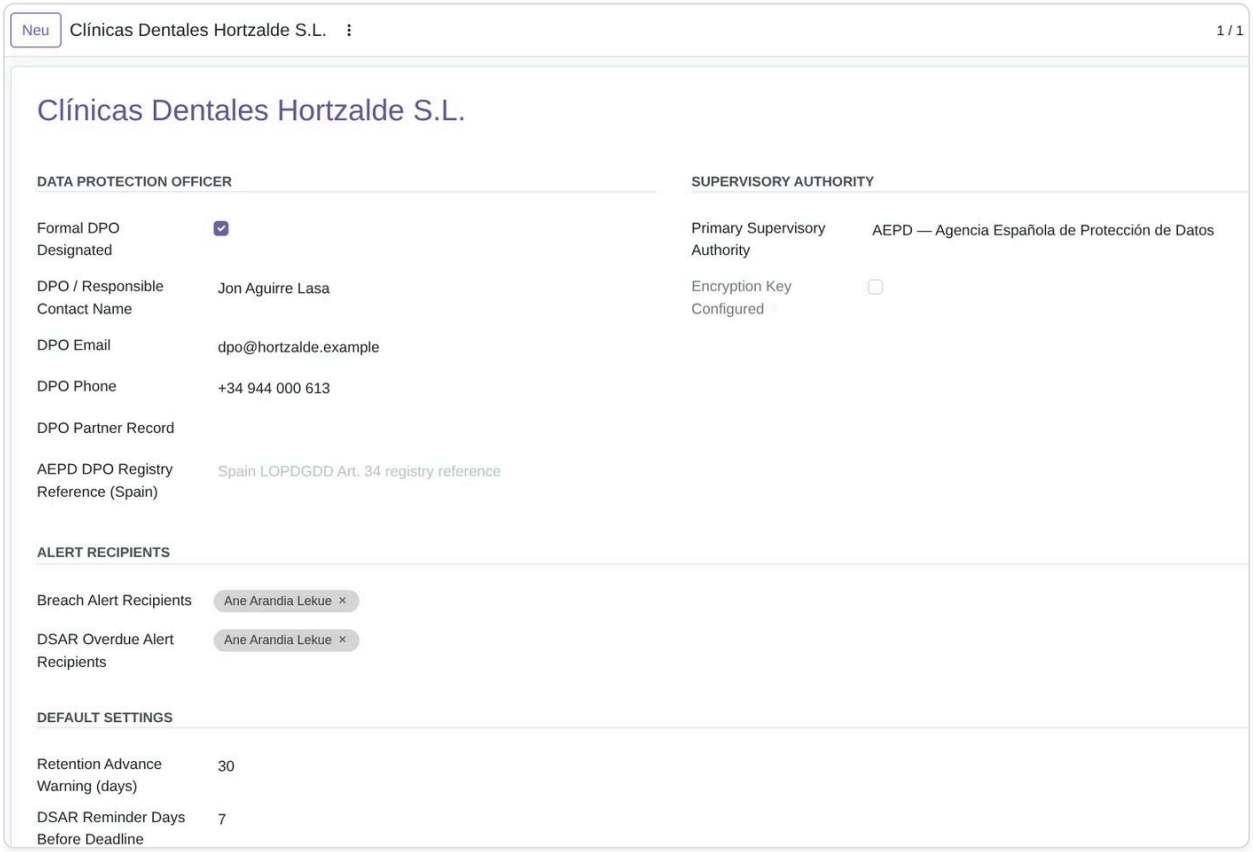
MODUL-LEITFADEN · GDPR COMPLIANCE

16 Was automatisch geschieht

AUFGABE	HÄUFIGKEIT	FUNKTION
GDPR: DSAR Deadline Reminder	Täglich	Sendet eine E-Mail, wenn bei einem offenen Antrag nur noch die Anzahl Tage übrig ist, die unter **DSAR Reminder Days Before Deadline** festgelegt ist: an die zugewiesene Person oder, falls diese keine E-Mail-Adresse hat, an die DSGVO-Verantwortlichen.
GDPR: Breach Countdown Alert	Stündlich	In den letzten 6 Stunden der Frist einer offenen Verletzung, die nicht als gemeldet markiert ist, sendet es eine E-Mail an die **Breach Alert Recipients** oder an die GDPR-Verwalter.
GDPR: Retention Expiry Check	Täglich	Hinterlässt eine Erinnerungsaktivität und sendet für jede aktive Aktivität eine E-Mail, deren Aufbewahrungsende naht und die in den letzten 30 Tagen nicht überprüft wurde.
GDPR: DSAR Overdue Escalation	Wöchentlich	Sendet die Zusammenfassung der überfälligen Anträge an die **DSAR Overdue Alert Recipients** oder an die GDPR-Verwalter.
GDPR: Annual RoPA Review Reminder	Alle 12 Monate	Erinnert per E-Mail daran, dass das Verzeichnis der Verarbeitungstätigkeiten überprüft werden muss.

Die Benachrichtigungen werden per E-Mail an Benutzer mit E-Mail-Adresse gesendet, in der jeweiligen Sprache. Die Häufigkeiten werden unter **Einstellungen › Technisch › Automatisierung › Geplante Aktionen** geändert, mit aktiviertem Entwicklermodus.

17 Die Moduloptionen und ihre Voreinstellungen



- **Echter Screenshot aus Odoo 20.** Die Optionen der GDPR-Konfiguration: der DSB, die Aufsichtsbehörde, die Empfänger der Benachrichtigungen und die Vorlaufzeiten in Tagen.

OPTION	VOREINSTELLUNG	FUNKTION
DPO Partner Record, **DPO / Responsible Contact Name**, **DPO Email** und **DPO Phone**	Leer	Angaben zu der Person, die als Datenschutzbeauftragte oder als Ansprechpartner fungiert.
Formal DPO Designated	Aktiviert	Gibt an, ob formell ein Datenschutzbeauftragter benannt wurde.
AEPD DPO Registry Reference (Spain)	Leer	Speichert die Referenz, unter der der DSB bei der AEPD geführt wird.
Primary Supervisory Authority	Leer	Wird aus den im Modul geladenen Aufsichtsbehörden ausgewählt.
Breach Alert Recipients	Leer	Benutzer, die die Verletzungsbenachrichtigungen erhalten. Wenn Sie keine auswählen, erhält sie die Gruppe **GDPR Toolkit / Manager** des Unternehmens.
DSAR Overdue Alert Recipients	Leer	Benutzer, die die Benachrichtigung über überfällige Anträge erhalten. Wenn Sie keine auswählen, erhält sie die Gruppe **GDPR Toolkit / Manager** des Unternehmens.
Retention Advance Warning (days)	30	Anzahl der Tage im Voraus, mit denen vor Ablauf der Aufbewahrungsfrist gewarnt wird.
DSAR Reminder Days Before Deadline	7	Tage vor der Frist eines Antrags, zu denen die Erinnerung versendet wird.

OPTION	VOREINSTELLUNG	FUNKTION
Art. 30(5) SME Exception Note Acknowledged	Deaktiviert	Sie bestätigen, dass Sie den Hinweis zur Ausnahme nach Art. 30 Abs. 5 für Unternehmen mit weniger als 250 Beschäftigten gelesen haben.
Encryption Key Configured	Je nach Server	Nur lesbar. Zeigt an, ob auf dem Server ein Verschlüsselungsschlüssel konfiguriert ist.

Es gibt nur eine Konfiguration pro Unternehmen. Wenn Sie eine zweite anlegen wollen, zeigt Odoo «Only one GDPR configuration record per company is allowed. A configuration already exists for company ....»

Die gesetzlichen Fristen (einen Monat für die Beantwortung eines Antrags und zwei weitere Monate Verlängerung, Art. 12 Abs. 3; 72 Stunden für die Meldung einer Verletzung, Art. 33 Abs. 1) sowie die Risikomatrix (Auswirkung mal Wahrscheinlichkeit) lassen sich nicht anpassen, da sie zum Modul gehören.

Was von Hand erledigt wird

ANSICHT	SCHALTFLÄCHEN
Verarbeitungstätigkeit aus dem RoPA	**Set Active** setzt die Aktivität von Entwurf auf aktiv; das ist nicht möglich, wenn sie eine DPIA braucht und keine genehmigte verknüpft ist. **Archive** archiviert sie. **Set to Draft** setzt sie zurück auf Entwurf. Die Schaltfläche zum Anlegen der DPIA öffnet eine Bewertung für diese Aktivität.
Betroffenenanfrage	**Verify Identity** hält die Verifizierung fest. **Draft Response** setzt die Anfrage auf „Antwort entworfen“. **Extend Deadline (2 months)** fügt zwei Monate Verlängerung hinzu (Art. 12 Abs. 3). **Close — Refused** und **Close — Partial Erasure** schließen die Anfrage mit Ihrer Entscheidung.
Verletzung	**Mark DPA Notified** vermerkt, dass Sie die Meldung vorgenommen haben. **Close** schließt die Verletzung. **Archive (Admin Only)** archiviert sie.
DSFA	**Approve** und **Reject** halten die Entscheidung der prüfenden Person fest. **Re-sync Step 1 from RoPA** füllt Schritt 1 erneut mit den Daten der verknüpften Tätigkeit.
Assistenten	**Export RoPA (PDF)** öffnet einen Assistenten mit **Export Format** und **Include Archived Activities**; **Export** erzeugt den Bericht und **Cancel** schließt ihn.

Die Schaltflächen für Anträge, Verletzungen und DSFAs sieht nur **GDPR Toolkit / Manager**. Die der Verarbeitungstätigkeit aus dem RoPA sehen alle, aber nur ein Verwalter kann sie nutzen, da **GDPR Toolkit / User** das Verzeichnis nur lesen darf. Eine Verletzung kann nur ein Odoo-Administrator archivieren.

18 Sicherheit und personenbezogene Daten

- Die Gruppe **GDPR Toolkit / User** sieht das RoPA nur lesend, kann Anträge erfassen und sieht diejenigen, die auf **Received** stehen oder ihr zugewiesen sind; sie zu ändern und deren Schaltflächen zu nutzen ist Sache von **GDPR Toolkit / Manager**.
- Die Gruppe **GDPR Toolkit / Manager** sieht alles und ist die Einzige mit den Arbeitsschaltflächen: Identität überprüfen, Antwort entwerfen, schließen, eine DSFA genehmigen, eine Verletzung als gemeldet markieren, unter anderem.
- **Archive (Admin Only)** bei Verletzungen sieht nur der Odoo-Administrator.
- Jedes Unternehmen sieht nur seine eigenen Datensätze.
- Anträge, Verletzungen und Tätigkeiten werden nicht gelöscht: Sie werden archiviert oder geschlossen.
- Die Historie des RoPA und das Auditprotokoll können nicht verändert werden.
- Die Auditzusammenfassung schwärzt personenbezogene Daten.
- Interne Notizen und die Begründung einer Ablehnung (Anträge) sowie die Beschreibung und die Folgen (Verletzungen) werden nur dann verschlüsselt gespeichert, wenn der Server die Umgebungsvariable GDPR_FERNET_KEY besitzt. Ohne sie werden sie unverschlüsselt gespeichert, das Serverprotokoll vermerkt dies, und die Konfiguration zeigt es unter **Encryption Key Configured** an.
- An FlexigoTech Cloud wird kein Antrag, keine Verletzung, keine DSFA und keine Verarbeitungstätigkeit übertragen. Die Daten Ihres Odoo bleiben in Ihrem Odoo. Der kostenpflichtige Dienst überwacht sechs amtliche Quellen und warnt, sobald sich eine davon ändert.

19 Mehrere Unternehmen

Jedes Odoo-Unternehmen hat seine eigene GDPR-Konfiguration. Wenn noch niemand das Konfigurationsmenü geöffnet hat, legt das Modul sie beim ersten Bedarf mit den Standardwerten an. Das Menü **Dashboard** öffnet die Konfiguration des aktiven Unternehmens und legt sie an, falls sie nicht existiert.

Jeder Datensatz (Tätigkeit, Antrag, Verletzung, DSFA) gehört zu einem Unternehmen, und jeder Benutzer sieht die Datensätze der Unternehmen, auf die er Zugriff hat. Die geplanten Aktionen durchlaufen jedes Unternehmen mit seiner Konfiguration. Die Benachrichtigungen gehen an die Empfänger, die diese Konfiguration angibt, und falls es keine gibt, an die GDPR-Verwalter dieses Unternehmens.

Das Datenschutzportal legt den Antrag im aktiven Unternehmen an, zum Zeitpunkt, an dem die betroffene Person ihn absendet.

Der Standard-Tarif kostet 29 € pro Monat oder 290 € pro Jahr, der Pro-Tarif 58 € pro Monat oder 580 € pro Jahr (Preise ohne MwSt.). Jedes Modul hat ein eigenes Abonnement für die Produktionsdatenbank; die Testkopien sind inbegriffen.

20 Wenn etwas schiefgeht

Eine Verarbeitungstätigkeit lässt sich nicht aktivieren, und es erscheint der Hinweis, dass eine genehmigte DSFA fehlt.	Schließen Sie eine mit der Aktivität verknüpfte DPIA ab und lassen Sie sie genehmigen. Sobald sie genehmigt ist, klicken Sie erneut auf **Set Active**.
Ein Betroffenenrecht-Antrag springt nicht in einen früheren Status zurück.	Der Status schreitet nur voran. Wenn Sie sich vertan haben, vermerken Sie es in den internen Notizen und arbeiten Sie vom aktuellen Status aus weiter.
Der Datenübertragbarkeits-Export wird nicht erzeugt.	Überprüfen Sie zuerst die Identität des Antrags und verknüpfen Sie einen Odoo-Kontakt im Feld **Odoo Contact (for portability export)**.
Sie können einen Antrag nicht als abgelehnt schließen.	Schreiben Sie zuerst die Begründung der Ablehnung. Sie ist Pflicht.
Sie können die Frist eines Antrags nicht verlängern.	Füllen Sie den Grund der Verlängerung aus. Ohne Grund lässt das Modul die Verlängerung nicht zu.
Sie können eine DSFA nicht ablehnen.	Schreiben Sie die Anmerkungen des DSB. Sie sind bei einer Ablehnung Pflicht.
Sie können eine Verletzung, einen Antrag oder eine Verarbeitungstätigkeit nicht löschen.	Sie gehören zur Prüfspur. Archivieren Sie sie. Bei Verletzungen kann nur ein Odoo-Administrator archivieren, und zwar mit schriftlicher Begründung.
Interne Notizen werden unverschlüsselt gespeichert.	Auf dem Server fehlt der Verschlüsselungsschlüssel. In der Konfiguration zeigt **Encryption Key Configured** an, ob er gesetzt ist.

Die Hinweise von Odoo sagen, was fehlt. Meist genügt es, die Angabe zu ergänzen und die Aktion zu wiederholen.

Weitere Hinweise, die Sie sehen können

«Only GDPR Managers can submit a DPIA for review.»	Bitten Sie einen GDPR-Verwalter, sie zur Prüfung einzureichen.
«Only GDPR Managers (acting as DPO) can approve a DPIA.»	Die Genehmigung nimmt ein GDPR-Verwalter vor, der als DSB auftritt. Bitten Sie die Person, die diese Berechtigung hat.
«Only GDPR Managers can perform this action.»	Die Aktion ist GDPR-Verwaltern oder Odoo-Administratoren vorbehalten. Bitten Sie einen von ihnen darum.
«Only Odoo Administrators can archive breach records.»	Bitten Sie einen Administrator, die Verletzung zu archivieren. Er muss eine Begründung angeben.
«Archive reason is required.»	Schreiben Sie den Archivierungsgrund und bestätigen Sie erneut.
«Extension justification is required when extending retention.»	Schreiben Sie bei der Aufbewahrungsprüfung die Begründung, bevor Sie die Verlängerung speichern.
«New retention end date is required when extending retention.»	Geben Sie das neue Aufbewahrungsende bei der Prüfung an, bevor Sie speichern.

«No Odoo contact linked to this DSAR. Please link a res.partner record first.»	Verknüpfen Sie den Kontakt in der Anfrage und wiederholen Sie den Export.
Der Hinweis, dass die Daten der betroffenen Person bereits anonymisiert wurden und eine manuelle Bearbeitung mit Ihrem DSB erforderlich ist.	Der Kontakt ist in Odoo bereits anonymisiert, es gibt keine Daten zu exportieren. Besprechen Sie mit Ihrem DSB, wie Sie antworten.
«No processing activities found for this company.»	Prüfen Sie beim Export des VVT, ob das aktive Unternehmen Tätigkeiten hat.

MODUL-LEITFADEN · GDPR COMPLIANCE

21 Andere Möglichkeiten

FORM	WAS DAS BEDEUTET
Von Hand	Tabellenkalkulationen für das Verzeichnis der Tätigkeiten, die Anfragen und die Verletzungen. Fristen werden manuell berechnet, und niemand warnt, wenn sie näher rücken.
Nur Odoo	Odoo 17, 18, 19 und 20 enthalten in der Community-Edition standardmäßig die Datenschutzsuche im technischen Menü der Einstellungen (mit Entwicklermodus). Sie suchen damit die Datensätze einer Person nach Name oder E-Mail, können sie archivieren oder löschen und ein Datenschutzprotokoll führen. Ein Verzeichnis der Tätigkeiten, Betroffenenanfragen, ein Verletzungsregister oder DSFA ist darin nicht enthalten.
Dieses Modul	Es ergänzt das Verzeichnis der Verarbeitungstätigkeiten, die Anfragen betroffener Personen mit ihrer Frist von einem Monat ab Eingang und der Verlängerung um zwei weitere Monate (Art. 12 Abs. 3), das Verletzungsregister mit dem 72-Stunden-Countdown ab Kenntnisnahme (Art. 33 Abs. 1) und die DSFA.

Zum Löschen oder Anonymisieren der Daten einer Person ist die Datenschutzsuche von Odoo zusammen mit diesem Modul nutzbar. Das Modul verwaltet die Anfrage und hält Ihre Entscheidung fest; das Löschen oder Anonymisieren nehmen Sie selbst in Odoo vor.

22 Tarife und Preis

9 €

Lizenz pro Odoo-Version.

+ FlexigoTech Cloud

STANDARD

29 €/Monat

oder 290 € im Jahr

Erste Antwort binnen 1 Arbeitstag

PRO

58 €/Monat

oder 580 € im Jahr

Erste Antwort binnen 4 Arbeitsstunden

Videocall bei Bedarf

14 Tage Testphase, ohne Karte

Preise zzgl. MwSt.

Die Lizenz des Moduls gilt pro Odoo-Version. FlexigoTech Cloud wird monatlich oder jährlich bezahlt, und die 14-tägige Testphase erfordert keine Kreditkarte.

23 Häufig gestellte Fragen

Funktioniert es ohne FlexigoTech Cloud?

Nein.

Was bietet das FlexigoTech-Cloud-Abonnement?

Die tägliche Überwachung von sechs amtlichen Quellen mit einer Benachrichtigung, wenn sich eine davon ändert. Die Hinweise erscheinen unter **Einstellungen › FlexigoTech Cloud** und in einer täglichen E-Mail.

Was kostet der FlexigoTech-Cloud-Dienst?

Der Standard-Tarif kostet 29 € pro Monat oder 290 € pro Jahr, der Pro-Tarif 58 € pro Monat oder 580 € pro Jahr, jeweils zzgl. USt. Dazu kommt die Lizenz des Moduls mit 9 € pro Odoo-Version.

Welche Quellen überwacht der Dienst?

Die Rechtsakte der Europäischen Union zur Änderung der DSGVO, das Verfahren des Digitalen Omnibus im Europäischen Parlament, das konsolidierte LOPDGDD-Gesetz aus dem BOE, die Angemessenheitsbeschlüsse der Europäischen Kommission sowie die Leitfäden und Werkzeuge der AEPD.

Was wird von meinem Odoo an FlexigoTech Cloud übermittelt?

Die Identifikation der Installation (Kennung, Adresse, öffentlicher Code, Odoo-Version und Modulnamen), die Annahme der Bedingungen mit der E-Mail-Adresse der annehmenden Person sowie die Anforderung der Dienstberechtigung. Das Verzeichnis der Tätigkeiten, die Anfragen, die Verletzungen, die DSFA und das Prüfprotokoll verbleiben in Ihrer Datenbank.

Funktioniert es mit Odoo Online?

Nein. Odoo Online erlaubt die Installation von Drittanbieter-Modulen nicht.

Wird Odoo Enterprise benötigt?

Nein. Es hängt nur von Modulen der Odoo Community ab (base, mail und portal) sowie von flexigotech_cloud. Es funktioniert in Community und Enterprise.

Für welche Odoo-Versionen gibt es das Modul?

Es gibt einen Zweig für jede der Versionen 17, 18, 19 und 20.

Welche Frist berechnet es für eine Anfrage einer betroffenen Person, und woher stammt sie?

Einen Monat ab Eingang der Anfrage gemäß Art. 12 Abs. 3 DSGVO. Die Spalte **Verbleibende Tage** zählt bis zur geltenden Frist.

Wie wird die Frist verlängert?

Mit **Extend Deadline (2 months)**, das zwei weitere Monate hinzufügt (Art. 12 Abs. 3) und eine Begründung verlangt. Es ändert nur die **Current Deadline**; der Status der Anfrage bleibt unverändert.

Was passiert, wenn die Frist einer Anfrage abläuft?

Die Anfrage erscheint in der Liste **Overdue**. Jede Woche sendet die Aufgabe **GDPR: DSAR Overdue Escalation** die Übersicht der überfälligen Anfragen an die Empfänger dieser Benachrichtigungen oder, falls es keine gibt, an die DSGVO-Manager.

Wie werden die 72 Stunden einer Verletzung gezählt, und wen warnt das Modul?

Die Frist läuft ab dem Datum und der Uhrzeit, die Sie als Zeitpunkt der Kenntnisnahme gemäß Art. 33 Abs. 1 erfassen. Jede Stunde warnt die Aufgabe **GDPR: Breach Countdown Alert** per E-Mail, wenn noch 6 Stunden oder weniger verbleiben, solange Sie die Verletzung nicht als gemeldet markiert haben.

Benachrichtigt es die Aufsichtsbehörde?

Nein. Die Meldung nehmen Sie selbst vor; hier halten Sie den Status, Datum und Uhrzeit, den Weg und das Aktenzeichen fest.

Informiert es die Betroffenen über eine Verletzung?

Nein. Wenn die Benachrichtigung nach Art. 34 erforderlich ist, nehmen Sie sie selbst vor und vermerken sie mit **Mark Data Subjects Notified**.

Löscht oder anonymisiert es die Daten bei einem Löschantrag?

Nein. **Retention Conflict Check** zählt, was vorhanden ist, und hält Ihre Entscheidung fest. Löschen oder Anonymisieren erledigen Sie selbst in Odoo.

Sendet es das Antwortschreiben an die betroffene Person?

Nein. Sie verfassen die Antwort im Reiter der Antwort auf Basis einer Vorlage und senden sie selbst. Die einzige E-Mail, die automatisch an die betroffene Person geht, ist die Eingangsbestätigung einer über das Portal gestellten Anfrage.

Was exportiert die Datenübertragbarkeit, und in welchen Formaten?

Die Kontaktdaten, die Bestellhistorie (mit der App Verkauf) und die Mitarbeiterakte (mit der App Mitarbeiter, mit ausdrücklicher Bestätigung). Die Formate sind JSON oder CSV.

Was braucht der Übertragbarkeitsexport, um erstellt zu werden?

Die verifizierte Identität und einen mit der Anfrage verknüpften Odoo-Kontakt. Ohne diese Angaben verweigert der Assistent den Export.

Wie stellt eine betroffene Person einen Antrag über das Portal, und was braucht sie dafür?

Sie ruft /my/privacy-rights in Ihrem Odoo auf, wofür eine Anmeldung nötig ist; sie benötigt also ein Portalkonto. Das Modul setzt keinen Link in „Mein Konto“: die Adresse geben Sie selbst weiter.

Wann markiert es eine DSFA als verpflichtend?

Wenn zwei oder mehr der neun Kriterien auf dem Reiter **DPIA Criteria** erfüllt sind oder wenn Sie sie manuell erzwingen. Diese Zwei-Kriterien-Regel ist eine allgemeine Richtlinie der WP248-Leitlinien, keine gesetzliche Pflicht.

Was ist die vorherige Konsultation?

Die Konsultation der Aufsichtsbehörde nach Art. 36. Bei hohem oder kritischem Restrisiko wird **Prior Consultation Required (Art. 36)** automatisch gesetzt. Wenn Sie die Konsultation einreichen, tragen Sie hier ein, was Sie getan haben; das Modul reicht sie nicht ein.

Kann ich eine Anfrage, eine Verletzung oder eine Tätigkeit löschen?

Nein. Tätigkeiten, Anfragen und Verletzungen werden archiviert oder abgeschlossen. Eine Verletzung darf nur der Odoo-Administrator archivieren, und dafür ist eine Begründung nötig.

Was speichert das Prüfprotokoll?

Datum und Uhrzeit, den Benutzer, die Operation, das Modell, den Datensatznamen und, sofern vorhanden, die IP-Adresse jeder Änderung. Niemand kann seine Einträge ändern oder löschen, auch kein Administrator.

Was wird verschlüsselt gespeichert?

Interne Notizen, die Begründung einer Ablehnung sowie die Beschreibung und Folgen von Verletzungen, allerdings nur, wenn der Server den Verschlüsselungsschlüssel besitzt. Ohne ihn werden sie unverschlüsselt gespeichert.

Funktioniert es mit mehreren Unternehmen?

Ja. Jedes Unternehmen hat seine eigene Konfiguration, und jeder Benutzer sieht nur die Datensätze der Unternehmen, auf die er Zugriff hat.

In welchen Sprachen werden die Bildschirme angezeigt?

Die Bildschirme des Moduls erscheinen auf Spanisch. In den übrigen Sprachen erscheinen sie auf Englisch; die Menüs und Schaltflächen von Odoo erscheinen in der Sprache jedes Benutzers.

Gilt es für ein Unternehmen mit weniger als 250 Beschäftigten?

Art. 30 Abs. 5 DSGVO befreit Unternehmen mit weniger als 250 Beschäftigten von den Pflichten der Absätze 1 und 2, sofern die Verarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, nicht nur gelegentlich erfolgt oder keine besonderen Datenkategorien bzw. Daten über strafrechtliche Verurteilungen und Straftaten umfasst. Das Modul beurteilt nicht, ob dies auf Sie zutrifft.

Wie viele Aufsichtsbehörden und Rechtsgrundlagen enthält es?

32 Aufsichtsbehörden und 16 Rechtsgrundlagen, die bei der Installation geladen werden. Die federführende Behörde wählen Sie unter **GDPR Toolkit › Configuration › DPO & Settings**.

Welche Berichte und Exporte gibt es?

Sie können das VVT als PDF oder Excel exportieren. Außerdem gibt es Berichte zum Verlauf der Betroffenenanfragen, zum Verletzungsregister und zum Stand der DSFA.

Welche Hinweise sendet es per E-Mail?

Fünf geplante Aufgaben: die tägliche Fristerinnerung für Anfragen, der stündliche Countdown für Verletzungen, die tägliche Prüfung der Aufbewahrung, die wöchentliche Eskalation überfälliger Anfragen und die Erinnerung an die jährliche Überprüfung des VVT.

Was zeigt das Menü Dashboard?

Drei Schaltflächen, die Listen öffnen: **View Open DSARs**, **View Active Breaches** und **DPIAs Pending Review**. Es zeigt keine Kennzahlen an.

Entscheidet es für mich, ob eine Verletzung gemeldet oder eine DSFA durchgeführt wird?

Nein. Die endgültige Entscheidung liegt beim Verantwortlichen oder seinem DSB. Die Risikomatrix (Auswirkung mal Wahrscheinlichkeit) stammt aus dem Modul, nicht aus dem Gesetz.

Ist das Rechtsberatung?

Nein.

MODUL-LEITFADEN · GDPR COMPLIANCE

24 Glossar

DSGVO	Die Datenschutz-Grundverordnung, Verordnung (EU) 2016/679. Aus ihr stammen die Fristen und Pflichten, die das Modul umsetzt.
LOPDGDD	Das spanische Gesetz zum Schutz personenbezogener Daten und zur Gewährleistung digitaler Rechte. FlexigoTech Cloud überwacht seinen konsolidierten Text im BOE.
AEPD	Die Spanische Datenschutzbehörde. Sie ist eine der 32 Aufsichtsbehörden, die das Modul enthält.
Aufsichtsbehörde	Die öffentliche Behörde, die in jedem Land den Datenschutz überwacht. Ihr werden Verletzungen gemeldet (Art. 33 Abs. 1). Unter **Primary Supervisory Authority** wählen Sie Ihre aus.
DSB	Der Datenschutzbeauftragte oder, falls keiner benannt ist, die für Datenschutz verantwortliche Person. Ihre Daten werden in der Konfiguration gespeichert.
Verantwortlicher	Wer über Zweck und Mittel der Verarbeitung entscheidet. Sein Verzeichnis der Verarbeitungstätigkeiten folgt Art. 30 Abs. 1.
Auftragsverarbeiter	Wer personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Sein Verzeichnis folgt Art. 30 Abs. 2.
Betroffene Person	Die Person, deren Daten verarbeitet werden und die ihre Rechte ausüben kann.
VVT	Das Verzeichnis der Verarbeitungstätigkeiten (Art. 30): ein Datensatz je Tätigkeit, mit deren Verlauf.
Betroffenenanfrage	Was eine betroffene Person verlangt: Auskunft (Art. 15), Berichtigung (Art. 16), Löschung (Art. 17), Einschränkung (Art. 18), Datenübertragbarkeit (Art. 20) oder Widerspruch (Art. 21).
Geltende Frist	Das Datum, bis zu dem eine Anfrage beantwortet werden muss: ein Monat ab Eingang und, bei Verlängerung, zwei weitere Monate (Art. 12 Abs. 3).
Datenübertragbarkeit	Das Recht, die vom Betroffenen bereitgestellten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten (Art. 20 Abs. 1). Das Modul exportiert sie als JSON oder CSV.
Löschung	Das Recht auf Löschung der Daten (Art. 17). Das Modul zählt die vorhandenen Daten und hält Ihre Entscheidung fest; das Löschen nehmen Sie selbst vor.

Datenschutzverletzung	Eine Verletzung des Schutzes personenbezogener Daten. Sie ist der Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden nach Kenntnisnahme zu melden, sofern die Verletzung voraussichtlich nicht zu einem Risiko führt (Art. 33 Abs. 1).
DSFA	Die Datenschutz-Folgenabschätzung (Art. 35) mit fünf Schritten.
Restrisiko	Das Risiko, das nach Anwendung der Schutzmaßnahmen verbleibt. Bei hohem oder kritischem Restrisiko wird die vorherige Konsultation markiert.
Vorherige Konsultation	Die Konsultation der Aufsichtsbehörde vor der Verarbeitung, wenn die DSFA ergibt, dass ohne Abhilfemaßnahmen ein hohes Risiko bestehen würde (Art. 36 Abs. 1). Die Konsultation reichen Sie selbst ein.
Rechtsgrundlage	Der Grund, der die Verarbeitung der Daten erlaubt. Das Modul enthält 16: 6 aus Art. 6 und 10 aus Art. 9.
Besondere Kategorien	Die Daten nach Art. 9, etwa Gesundheitsdaten. Für sie gelten eigene Rechtsgrundlagen.
Internationale Übermittlung	Die Übermittlung von Daten in ein Drittland. Die Tätigkeitskarte enthält das Land und die Garantie, auf die sie sich stützt.
Aufbewahrung	Die Dauer, für die die Daten jeder Tätigkeit gespeichert werden, mit geschätztem Fristende und Verlauf der Überprüfungen.
Audit-Protokoll	Die Liste, wer wann welche Änderung von welcher IP-Adresse aus vorgenommen hat. Es kann nicht geändert oder gelöscht werden.
Überwachung	Der Dienst von FlexigoTech Cloud, der jeden Tag sechs amtliche Quellen prüft und Sie benachrichtigt, wenn sich eine davon ändert.

25 Checkliste und Kontakt

- [ ] Sie haben Odoo 17, 18, 19 oder 20 auf Odoo.sh oder auf Ihrem eigenen Server. Odoo Online erlaubt die Installation von Drittmodulen nicht.
- [ ] Sie haben das Modul und seine Abhängigkeit flexigotech_cloud installiert.
- [ ] Sie haben die 14-tägige Testphase von FlexigoTech Cloud unter **Einstellungen › FlexigoTech Cloud** aktiviert und die Liste der übermittelten Daten gelesen.
- [ ] Sie haben **GDPR Toolkit › Configuration › DPO & Settings** geöffnet und die Daten des DSB sowie die **Primary Supervisory Authority** ausgefüllt.
- [ ] Sie haben die Empfänger für Meldungen über Datenschutzverletzungen und Betroffenenanfragen festgelegt.
- [ ] Sie haben jeder Person die Gruppe **GDPR Toolkit / Manager** oder **GDPR Toolkit / User** zugewiesen.
- [ ] Wenn Sie die internen Notizen und die Beschreibung der Verletzungen verschlüsseln möchten, haben Sie den Verschlüsselungsschlüssel auf dem Server hinterlegt und **Encryption Key Configured** bestätigt dies.
- [ ] Sie haben die Tätigkeiten des Verzeichnisses mit ihren DSFA-Kriterien und ihrer Aufbewahrungsfrist angelegt.
- [ ] Sie haben eine erste Anfrage erfasst und deren **Current Deadline** geprüft.
- [ ] Sie haben den Betroffenen die Adresse /my/privacy-rights Ihres Odoo mitgeteilt.
- [ ] Falls gewünscht, haben Sie das Verletzungsregister mit einer Testverletzung ausprobiert und den 72-Stunden-Countdown gesehen.

Wenn wir es gemeinsam mit Ihnen einrichten sollen, schreiben Sie uns. 2 Monate Support sind in allem enthalten, was Sie kaufen: Wir helfen Ihnen bei Installation und Konfiguration und sorgen dafür, dass alles läuft, per E-Mail und Videokonferenz.

E-Mail

Für Installation, Einrichtung und alle Fragen.
comercial@flexigotech.com

Im Web

Die Seite des Moduls mit Leitfaden und Preisen.
flexigotech.com/de/odoo-gdpr.html

In Odoo Apps

Die Seite des Moduls im Odoo-Store.
apps.odoo.com

GDPR Compliance ist ein Modul von FlexigoTech für Odoo. FlexigoTech ist eine Marke der Flexibles y Accesorios Gobe, S.L. (Barcelona, Spanien).