



HRemia

Annex to the client brochure

Legal & Technical Compliance Annex

What the law asks of an organisation that uses HRemia, how the platform supports each requirement, and how your legal and IT teams can verify every claim: article by article, table by table, test by test.

For Legal and the DPO

Part A. The EU and Greek framework, a Greek article-by-article matrix for N. 4990/2022 and KYA 47312/2023, the Directive for other countries, GDPR and the AI Act.

For IT and Security

Part B. Architecture and data flows, access control down to the database policies, encryption and keys, logging, retention, AI processing and the tests behind each guarantee.

For everyone reviewing

Part C. The questions legal departments ask, answered with a pointer to the section that proves each answer; the design boundaries and the organisation's own part.

Π-1 HR cannot read private chats

Π-2 anonymity is a database rule

Π-3 AES-256-GCM, keys per company

Π-4 row-level security

Π-5 EU storage

Π-6 legal deadlines

Π-7 append-only audit

Π-8 citation guard

Π-9 AI Act art. 50

Π-10 no training

Π-11 groups of 5+

Π-12 opt-in Memory

Π-13 officer's exclusive access

Π-14 encrypted push

Status: describes the platform release of the end of September 2026, written from the code that runs it. **Not legal advice and not a certification:** HRemia is designed to support compliance; your organisation remains the controller and makes its own assessment. **No prices.** Claim codes Π-1 to Π-21 link the brochure's claims to the sections that prove them.

0 Scope, how to read, claim codes

This annex accompanies the HRemia client brochure. It gives your legal department and your IT department the detail behind the brochure's claims: the legal framework, how each requirement is met, who is responsible for what, and how each guarantee can be checked in the product and in its automated tests.

START

0	Scope, how to read, claim codes	2
---	---------------------------------	---

PART A — LEGAL

A1	Legal framework	4
A2	Greece: N. 4990/2022 and KYA 47312/2023, article by article	6
A3	Directive (EU) 2019/1937, for companies outside Greece	12
A4	GDPR	15
A5	AI Act	19
A6	Who does what: platform and organisation	20

PART B — TECHNICAL

B1	Architecture and data flow	22
B2	Hosting, network and TLS	23
B3	Access control	24
B4	Encryption and key management	26
B5	Anonymity by design	28
B6	Audit and logging	29
B7	Backup, retention and deletion	30
B8	AI processing	31
B9	Controls mapped to ISO/IEC 27001:2022	33
B10	Evidence: the automated tests	34

PART C — QUESTIONS

C1	Questions legal departments ask	36
C2	Design boundaries and the organisation's part	39

What this annex is, and what it is not

- **A description of the service as released at the end of September 2026**, written from the code that runs it (the API, the database schema and the web application). It describes how the platform works for any organisation that uses it.
- **Not legal advice and not a certification.** HRemia is designed to support compliance. Your organisation remains the controller of its data and the party that must meet the obligations below. This annex supports your own assessment, for example your DPIA, and shows where the platform's part ends and the organisation's begins (A6).
- **No prices.** Commercial terms are in the proposal. This annex accompanies the client brochure (5th edition). The contract proposal also includes the proposed data processing agreement (DPA) under GDPR art. 28 with its annexes (among them the sub-processor list), the DPIA support pack and the AI Act transparency note.

Who should read what

Reader	Start with	Then
Legal department, Data Protection Officer	Part A: A1 to A6	Part C: questions 1 to 10 (C1)
IT, security, architecture	Part B: B1 to B10	A4 (GDPR measures), C2 (design boundaries)
Reports officer (in Greece: Υ.Π.Π.Α.), compliance	A2 (Greece) or A3 (other countries)	The checklist in A6
Management, procurement	C1 and C2	A6

Which law applies: the company's country

Each organisation records its country in the platform. For a company established in Greece (country GR), the reporting channel follows N. 4990/2022 and KYA 47312/2023, and the Greek terms appear: the Υ.Π.Π.Α. (Υπεύθυνος Παραλαβής και Παρακολούθησης Αναφορών, the reports officer), the special file and the National Transparency Authority (Ε.Α.Δ.) as external channel. For every other company, and for one that has not recorded its country, the channel follows Directive (EU) 2019/1937, and national specifics are documented per country with local counsel. A2 is therefore a Greece-specific chapter; A3 covers companies in other member states.

Evidence markers



Enforced by the PostgreSQL database itself: grants, row-level security, CHECK constraints. It holds even if the application code had a defect.

APP

Enforced by the application code.

TEST

Covered by an automated test named in [B10](#). Test names are given exactly as in the code (`apps/api/tests`), so your IT team can find them.

ORG

Your organisation's part. The platform supports it but cannot do it for you.

Claim codes

The brochure's guarantees carry claim codes. The table links each code to the brochure's wording and to the section of this annex that proves it. Codes Π-15 to Π-20 cover functions released in September 2026, and Π-21 exists only in this annex; the brochure (5th edition) uses Π-1 to Π-20.

Code	Guarantee	In the brochure (5th ed.)	Proof
Π-1	HR, managers and company administrators cannot read employees' private conversations, Memory or wellbeing profiles: a separate database schema on which the HR side of the application has zero grants, tested.	"HR and managers cannot read the chat"	B3 · B10
Π-2	An anonymous report cannot store the reporter's identity or be turned into a named one: a database CHECK constraint and trigger, an argon2-hashed access code, no IP address stored with the report, and no access log on our web server, whose error log records only critical faults; an IP address is kept only as a rate-limit counter, for at most 10 minutes. Cloudflare, through which traffic to hremia.eu and www.hremia.eu passes, processes IP addresses in transit for protection against attacks (A4 point 8).	"Anonymity is a database rule"; "no IP address is stored with the report"	B5 · B2 · B10
Π-3	AES-256-GCM encryption with keys per company; separate keys for conversations and for reports; each report field and each evidence file bound to its own record.	"Stored separately and encrypted"	B4
Π-4	Row-level security per company and, for personal records and conversations, per employee.	"Personal records, each with its source"	B3
Π-5	Data stored in the EU (Hetzner, Falkenstein, Germany); document search (embeddings) runs on the same server.	"Responsible AI"	B1 · B2 · A4
Π-6	Legal deadlines tracked on every case (acknowledgement within 7 days, in Greece 7 working days; feedback within 3 months of the acknowledgement); escalation with a recorded reason to the designated reports officer (or to a deputy when the officer already handles the case), or to the DPO when none is designated.	"Legal deadlines, built in"	A2 · A3 · B6
Π-7	The audit log is append-only for the application.	"Audit trail that cannot be edited"	B6
Π-8	Citation guard: an article number that is not in the organisation's documents never reaches the screen.	"Answers cite the article"	B8
Π-9	AI Act transparency (art. 50): every conversation starts with a notice that the user is talking to an AI assistant, and a permanent notice stays under the message field; the assistant says it is an AI whenever asked and reminds the user of it in sensitive contexts; AI-generated text carries a machine-readable mark; no emotion recognition; no employment decisions.	"An assistant that says what it is"	A5 · B8
Π-10	Established AI providers, named in the organisation's sub-processor list and used, under the DPA, on business terms without training on customer data; a primary model and one or more fallbacks, tried in order only when the one before is unavailable. By agreement, HRemia configures a provider of the organisation's own choice for it alone. Each call is recorded with the provider and model that served it (B8).	"Keeps working when a model fails"	A4 · B8 · B6
Π-11	Figures only for groups of at least 5; breaks recorded as company totals only.	"Small-group suppression", "Private breaks"	A4 · B5
Π-12	Memory is opt-in: off by default and switched on only by the employee; at most 25 short notes, each encrypted and bound to its owner; the employee reads, edits and deletes every note, or all of them, on the "What your assistant remembers" screen of their account or from the conversation.	"Memory the employee controls"	B8 · A4 · B10
Π-13	Only the reports officer (Υ.Π.Π.Α.) and deputies can read case files, enforced by the database, with a permanent record of every recusal (κώλυμα).	"The reports officer's exclusive access"	B3 · A2
Π-14	Notifications: web push encrypted end to end, so the push service cannot read it; sensitive notices show no content on a lock screen; quiet hours.	"Announcements and a notification centre", "Quiet hours"	B4 · B5

Code	Guarantee	In the brochure (5th ed.)	Proof
Π-15	A public reporting page per company, with no account, for everyone the law protects; named or anonymous, with a two-way mailbox; the reference and access code are shown once.	"A public page, no account needed"	A2 · B5
Π-16	The company's country decides the law followed: Greece, N. 4990/2022 and KYA 47312/2023; elsewhere, Directive 2019/1937.	"Reporting texts that follow each company's country"	A1 · A2 · A3
Π-17	One special file for every report, however it arrived, with its registration number and real time of receipt; provable acknowledgement and feedback; minutes the reporter confirms, corrects, signs or refuses.	"One special file, however the report arrived"	A2
Π-18	Closing with a message to the reporter and an outcome code, including the legal archive grounds; reopening; pseudonymised case-file export and referral log; a report about the officer: in Greece only registered and forwarded to the external channel, elsewhere handled by the other handlers.	"Outcome, referral, a report about the officer"	A2
Π-19	The officer's term and eligibility; the compliance centre: a live checklist against the company's law, dated company statements on the audit trail, a printable evidence pack.	"Reports officer pack", "Compliance centre and evidence pack"	A2 · A6
Π-20	Compliance figures are aggregate: 12-month metrics hide any category below the organisation's anonymity threshold (at least 5 cases), and the evidence pack holds no report content and nothing about reporters; an A4 poster with QR code and a website button are generated.	"Compliance centre and evidence pack"	A2 · A6
Π-21	Reports and case files, surveys and break data are never sent to an AI provider.	— (annex only)	B8

PART A

Legal

For the legal department and the Data Protection Officer: the texts that apply, how each requirement is met, and what remains the organisation's responsibility.

A1 Legal framework

A2 Greece, article by article

A3 Directive, other countries

A4 GDPR

A5 AI Act

A6 Who does what

A1 Legal framework

The platform touches four bodies of law: whistleblower protection, data protection, artificial intelligence and, for the service contract itself, the Data Act. The texts below are those in force at the end of September 2026.

European Union

Instrument	What it governs for this service	Status	Where
Directive (EU) 2019/1937 (whistleblowers)	Internal reporting channels for employers with 50 or more workers; acknowledgement within 7 days, feedback within 3 months; confidentiality; records; protection against retaliation. Minimum harmonisation: employers are bound through the national transposition (arts 25, 26).	Transposed in every member state	A3; Greece A2
Regulation (EU) 2016/679 (GDPR)	Every processing of personal data on the platform: roles (arts 4, 28), lawful bases (arts 6, 9, 10), principles (art. 5), data protection by design (art. 25), security (art. 32), DPIA (art. 35), transfers (Chapter V).	Applies	A4

Instrument	What it governs for this service	Status	Where
Regulation (EU) 2024/1689 (AI Act), as amended by Regulation (EU) 2026/1744	Provider and deployer roles; AI literacy (art. 4); prohibited practices, including emotion recognition at the workplace (art. 5(1)(f)); transparency (art. 50); high-risk use cases (Annex III).	In force since 1.8.2024, applying in stages	A5
Regulation (EU) 2023/2854 (Data Act), Chapter VI	Switching between data processing services, which include SaaS: notice, transition, export of the customer's data; switching charges phased out.	Applies since 12.9.2025; no switching charges from 12.1.2027	A4
Directive 2003/88/EC (working time)	Rest breaks. The in-app breaks are offered in addition to them and neither record nor replace them.	Applies through national law	A4

Greece

Text	What it governs	Where
N. 4990/2022 (ΦΕΚ Α' 210/11.11.2022), as in force	Transposes the Directive: who is protected (art. 6), conditions for protection (art. 7), the Υ.Π.Π.Α. in private-sector entities with 50 or more workers (art. 9), the internal procedure (art. 10), confidentiality (art. 14), personal data (art. 15), records (art. 16), protection measures: prohibition of retaliation, support, remedies, protection of persons concerned, no waiver of rights (arts 17–22), penalties (art. 23). Four later laws changed only the material scope (art. 4 and the Annex): v. 5095/2024, v. 5193/2025, v. 5232/2025 and v. 5321/2026.	A2
ΚΥΑ 47312/2023 (ΦΕΚ Β' 6944/11.12.2023)	The internal procedure in detail: channels and minutes (art. 2); receipt, acknowledgement and the special file (art. 3); handling, referral and archiving (art. 4); follow-up and feedback (art. 5).	A2
v. 4624/2019	Implements the GDPR: special categories of data (art. 22) and processing in the employment context, including the form of employee consent (art. 27).	A4
v. 5321/2026 (ΦΕΚ Α' 114/20.7.2026)	Implements the AI Act. The ΑΠΔΠΧ (Hellenic Data Protection Authority) is market-surveillance authority, among others for the transparency obligations of art. 50 (art. 3 §1). Breaches of the AI Act were added to the scope of N. 4990/2022 (art. 20). From 20.7.2026 it repealed Part A, Chapter B of v. 4961/2022 (arts 3–14), including the art. 9 duty to inform employees about AI systems (art. 26).	A5
v. 4808/2021	Violence and harassment at work. N. 4990/2022 leaves it unaffected (art. 9 §14), and harassment as such is outside the material scope of art. 4. The public form offers it as a separate subject and tells the reporter that the organisation's responsible person under v. 4808/2021 handles it. The report reaches the case handlers like any other; once a Υ.Π.Π.Α. is designated, the Υ.Π.Π.Α. forwards it to that person and, if nothing within art. 4 remains, archives it as out of scope (ΚΥΑ art. 4 §1 ββ).	A2
ΑΠΔΠΧ Decision 65/2018 (ΦΕΚ Β' 1622/10.5.2019)	The list of processing that requires a DPIA. It names whistleblowing systems in item 1.3, a first-category criterion that makes a DPIA mandatory on its own, and AI applications in item 3.1, a third-category criterion that does so together with a criterion of the first or second category.	A4

Other member states

The Directive sets minimum rules and each member state adds its own. Before the platform is offered in a new market, local counsel reviews the national layer and the result is recorded in a country annex: retention periods, the rules on anonymous reports, the competent external authority, duties towards worker representatives and the language of the legal documents. The table shows, as an indication, how three transpositions differ on the points the platform tracks.

Country and law	Acknowledgement	Feedback	Keeping the records
Germany, Hinweisgeberschutzgesetz	7 days (§ 17(1))	3 months after the acknowledgement (§ 17(2))	Deleted 3 years after the procedure ends (§ 11(5))
Italy, D.Lgs. 24/2023	7 days (art. 5)	3 months (art. 5)	At most 5 years after the final outcome (art. 14)
Spain, Ley 2/2023	7 calendar days (art. 9.2)	3 months from receipt; up to 3 more in complex cases (art. 9.2)	At most 10 years (art. 26)

Country and law	Acknowledgement	Feedback	Keeping the records
HRemia, every country	7 calendar days from receipt (Directive art. 9(1) (b)); in Greece 7 working days	3 calendar months from the acknowledgement or, without one, from the end of the 7 days (Directive art. 9(1)(f); in Greece, N. 4990/2022)	Set by the organisation (12 to 120 months from closing) or by the handlers for a single case; the content is then erased automatically, never while a case is open or kept until the proceedings are over (B7)

Indicative, as checked in September 2026. The country annex prepared with local counsel prevails. The platform computes the Directive's limits and, for a company in Greece, those of N. 4990/2022, and never sets a later date than these. Where a national law is stricter, as Spain's feedback period counted from receipt, the organisation observes the stricter limit, which the country annex records. **ORG**

Worker representatives. Many member states require the employer to inform or consult worker representatives, or to reach agreement with them, before introducing technical systems at work; in Germany, for example, co-determination under § 87(1) no. 6 BetrVG. The AI Act keeps national rules that are more favourable to workers (art. 2(11)). The platform's design helps: no individual monitoring, figures only for groups of at least five. The procedure itself is the organisation's **ORG**.

Employee data. The GDPR allows more specific national rules for employment (art. 88), provided they are more than a repetition of the GDPR (CJEU, C-34/21). This annex therefore relies on the GDPR's own articles and cites national provisions only where they add a condition, as art. 27 v. 4624/2019 does in Greece.

A2 Greece: N. 4990/2022 and KYA 47312/2023, article by article

For companies whose country is Greece. HRemia covers the technical requirements of N. 4990/2022 and KYA 47312/2023 for the Υ.Π.Π.Α.; the matrix below is the proof. For each requirement it names the feature, how your IT or legal team can verify it, and what remains the organisation's part.

How to read the matrix

- Verify** names an automated test (see B10) and the screen. Public page: *hremia.eu/{language}/speak-up/{company}*. Tracking page: *.../report/track*. Inbox: the case files, for handlers. Settings: company settings (reports officer, public page, poster). Compliance centre: *.../whistleblowing*.
- Protection of reporters is conditional: it applies when the conditions of art. 7 are met. The platform explains this and never promises protection.
- Deadlines: the law gives 7 *working* days to acknowledge and 3 months for feedback, counted from the acknowledgement or, without one, from the end of those 7 working days. The platform computes both for each case on the company's clock, counts months as calendar months, never sets a date later than the legal limit, and reminds the handlers 24 hours and 3 days before. Escalation shortens the time to act to 48 hours and 30 days; that is HRemia's policy, not the law.

Requirement	HRemia	Verify	Organisation
N. 4990/2022 — who is protected, and when			
Art. 6 — Protected are not only employees: former employees, applicants, the self-employed and consultants, shareholders and board members, volunteers and trainees, staff of contractors, subcontractors and suppliers; also facilitators and related persons.	A public reporting page per company, with no account: <i>hremia.eu/{language}/speak-up/{company}</i> . It asks how the reporter relates to the organisation (employee, former employee, applicant, contractor, supplier, trainee or volunteer, shareholder or board member, other, not stated). Employees can also report inside the app. APP	<code>test_the_page_names_the_company_and_hides_unknown_or_switched_off_ones</code> · Public page	Link the page prominently on the company website (KYA art. 2 §3) and tell non-employees it exists. ORG
Art. 7 — Protection depends on reasonable grounds to believe the information was true and in scope (§1); it covers internal and external reports and public disclosure (§2); anonymous reporters who are later identified are protected (§3).	Named or anonymous reporting on every platform route. The public page explains that protection applies when the law's conditions are met and never promises it; the assistant is instructed never to tell a person that they are protected. APP	Public page, section “Who is protected” · <code>companion/prompts.py</code>	Do not reject anonymous reports (KYA art. 2: a report may be named or anonymous); protect reporters in practice. ORG

Requirement	HRemia	Verify	Organisation
Art. 8 — Internal channels in the public sector.	A public-sector body uses the same functions; its designation rules follow art. 8.	—	Apply art. 8. ORG
N. 4990/2022 — the Υ.Π.Π.Α. (art. 9)			
Art. 9 §1–4 — Private entities with 50 or more workers designate a Υ.Π.Π.Α.; the duty lasts two more years after the threshold is reached; optional below 50; some sectors regardless of size.	The compliance centre shows whether a Υ.Π.Π.Α. is designated and can act. The platform does not know the legal headcount.	Compliance centre › “Reports officer designated”	Decide whether the duty applies; designate the Υ.Π.Π.Α. ORG
Art. 9 §5, §7 — A shared Υ.Π.Π.Α. for entities with 50–249 workers; the Υ.Π.Π.Α. may be an employee or a third party and reports directly to top management.	Any person with an account in the company (HR administrator or DPO role) can be designated, including an external or shared officer given such an account. The evidence pack has the fields “employee or third party” and “shared officer”.	Settings › Reports officer	Choose the officer; give them a direct reporting line to top management. For an external or shared officer, prefer the DPO role, which has no HR-administration screens (B3). ORG
Art. 9 §6 — A term of at least one calendar year; it may end earlier only for serious cause.	The term's start and end are kept with the designation. The compliance centre flags a term shorter than a year, ended or ending within 30 days; HR and the officer are notified 30 days before the end; an early end is recorded in the designation history. APP	<code>test_the_officers_term_is_at_least_a_year_in_greece_and_hr_is_warned_before_it_ends</code>	Set the term; document any serious cause. ORG
Art. 9 §8 (α)–(β) — Integrity, objectivity, impartiality; confidentiality. (γ) Withdrawal from a case with a conflict of interest (κώλυμα).	A handler records a κώλυμα on a case with its reason (encrypted). From that moment the database returns nothing of that case to them. Only another handler can lift it, and the withdrawal is never deleted: the lifting is recorded next to it. DB	<code>test_a_handler_who_withdraws_loses_that_case_only; test_a_withdrawal_is_kept_and_only_another_handler_can_lift_it</code>	Declare κώλυμα when it arises; keep deputies designated. ORG
Art. 9 §9; art. 10 §3 — Persons excluded from the role; other duties must not affect the officer's independence.	Each designee declares for themselves that no exclusion applies and no other duty conflicts, and can withdraw the declaration; it is dated and on the audit trail. APP	<code>test_each_designee_declares_their_own_eligibility</code>	Check eligibility; assign compatible duties. ORG
Art. 9 §10 (with art. 8 §6) — A reporter may go straight to the Ε.Α.Δ.	The public page shows the Ε.Α.Δ.'s external channel and never presents internal reporting as a precondition.	Public page, “External channel”	—
Art. 9 §11; art. 25 — The employer notifies the Labour Inspectorate of the Υ.Π.Π.Α.	The evidence pack includes a data sheet with the fields the Inspectorate's form asks for (legal name, ΑΦΜ, ΔΟΥ, registered office, ΚΑΔ, officer, term). The company records the notification as a dated statement with its reference. APP	Compliance centre › Evidence pack; statement “Labour Inspectorate notified”	File the notification through the Inspectorate's e-services. ORG
N. 4990/2022 — the procedure (art. 10)			
Art. 10 §1 — Reports in writing, orally, or through an electronic platform on the entity's website, accessible to persons with disabilities; a meeting with the Υ.Π.Π.Α. on request.	The platform channel: the public page and the in-app form. The reporter can attach up to 5 files to the report and to each later message (PDF, JPEG, PNG, DOCX, XLSX or TXT, up to 10 MB each); what could identify their author is removed before they are stored, encrypted (B5). The officer registers every other channel in the same special file: letter or delivery by hand, e-mail, telephone, voice message, meeting, other, with the real time of receipt, and can attach its enclosures; the clocks run from receipt. The form records a meeting request. APP	<code>test_the_officer_registers_a_letter_and_the_clocks_run_from_its_receipt; test_photos_and_pdfs Lose_gps_exif_xmp_and_authors_before_they_are_stored; test_the_officer_attaches_the_enclosures_of_a_report_they_registered</code>	Offer the oral route if chosen (telephone, voice messages); hold meetings on request. ORG

Requirement	HRemia	Verify	Organisation
Art. 10 §2 (α) — Information on how to report, posted in a visible place at the entity.	An A4 workplace poster with a QR code to the public page, generated per company (Greek and English for Greek companies), and an embed snippet for a website button: a plain link, with no script and no tracking. APP	Settings › Poster; Settings › Public page › Website button	Print and post the poster; place the button; record both in the compliance centre. ORG
Art. 10 §2 (β); KYA art. 3 §1 — The Υ.Π.Π.Α. receives reports on breaches within the scope of art. 4.	Every report, whatever its route, reaches the handlers' inbox and the special file. The public form asks what the report concerns, using the areas of art. 4 as amended (including national bribery offences, EU restrictive measures and, since v. 5321/2026, the AI Act), plus workplace conduct under v. 4808/2021 and "other". APP	Public page, subject of the report	Assess the scope; archive out-of-scope reports under ground ββ and forward what another organ must handle. ORG
Art. 10 §2 (γ) — Acknowledge receipt within 7 working days, in a way that can be proven.	The deadline is computed at receipt and is never later than the law's 7 working days; the handler is reminded 24 hours before. The acknowledgement is an explicit act with its time, its author and its method: a message on the platform, e-mail, post, telephone, in person, or minutes the reporter confirmed. The platform message reads, in Greek or English, "Your report was received and registered [in the special file] as HRM-... on ...". APP	<code>test_acknowledgement_and_feedback_are_provable_acts</code>	The Υ.Π.Π.Α. acknowledges. ORG
Art. 10 §2 (δ) — Forward the report for investigation, pseudonymised, or archive it with a decision.	A referral log: the company's competent organ, the prosecutor, Ε.Α.Δ., Competition Commission, Bank of Greece, ΑΠΔΠΧ, ΕΦΕΤ, Labour Inspectorate or another authority, with date, pseudonymisation, notice to the reporter and the body's answer. Closing requires an outcome code, including the archive grounds βα, ββ, βγ; archived cases can be reopened when new evidence arrives, keeping the earlier outcome. APP DB	<code>test_referrals_notices_and_a_pseudonymised_case_file; test_closing_needs_the_outcome_and_an_archived_case_can_be_reopened</code>	Decide; investigate through the competent organ. ORG
Art. 10 §2 (στ) — Follow up diligently and keep in contact with the reporter.	A two-way conversation on every case, also with anonymous reporters, who read and reply on the tracking page with the reference and access code. Internal notes never reach the reporter: for a named reporter who follows the case in the app, the database withholds them DB ; the tracking page reads only messages not marked internal APP .	Tracking page · policy <code>report_confidential_read_on_app.report_messages</code>	Reply within a reasonable time. ORG
Art. 10 §2 (ζ) — Feedback within 3 months of the acknowledgement.	The deadline is counted in calendar months, not 90 days, and is never later than the law's limit, with a reminder 3 days before. Feedback is dated the first time the handler marks a message as feedback or closes the case with a message to the reporter; a case cannot be closed without such a message. APP	<code>test_three_calendar_months_not_ninety_days</code>	Give substantive feedback. ORG
Art. 10 §2 (η) — Clear information on reporting externally to the Ε.Α.Δ.	The public page shows the Ε.Α.Δ.'s platform, e-mail, postal address and telephone; for a Greek company's report, the tracking page and the in-app form name the Ε.Α.Δ. with a link to its platform.	Public page, "External channel" · <code>test_tracking_names_the_reports_own_company_country</code>	Also post the information at the workplace. ORG
Art. 10 §2 (θ) — Training on ethics and integrity.	The training module can host integrity courses, with quizzes and certificates.	Training	The Υ.Π.Π.Α. plans the training. ORG

Requirement	HRemia	Verify	Organisation
N. 4990/2022 — external channel and public disclosure (arts 11–13)			
Arts 11–13 — The E.A.Δ. as external channel, its procedure, and the conditions for public disclosure.	Information only. The dated acknowledgement and feedback on every case document whether the organisation responded in time, which matters for art. 13(a).	Special file	—
N. 4990/2022 — confidentiality, personal data, records (arts 14–16)			
Art. 14 §1; art. 10 §2 (ε) — The reporter's identity and anything that points to it are disclosed only to the authorised staff who receive and follow up reports; technical measures such as pseudonymisation; the Y.Π.Π.A. keeps unauthorised persons out.	Once the Y.Π.Π.A. and deputies are designated, only they can read case content, and the database enforces it with RESTRICTIVE policies (B3); other HR administrators see only counts. Lock-screen and e-mail notifications say only that there is an update; escalation e-mails carry only the reference. Case text is encrypted with the company's report key; exports are pseudonymised by default. DB APP	<code>test_designating_handlers_closes_cases_to_other_hr_in_the_database_itself; test_referrals_and_minutes_are_hidden_from_hr_who_do_not_handle_reports</code>	Designate the Y.Π.Π.A. as a step of activation, before the public page is put to use (the page is technically on by default and can be switched off in Settings until the designation is recorded); until the designation, HR administrators and the DPO can read reports. ORG
Art. 14 §2–3 — Disclosure only where the law requires it, after informing the reporter in writing.	An export without pseudonymisation is an explicit choice and is recorded on the case's audit trail. A referral that sends the reporter's identity with the case, to anyone, the company's own organs included, requires its basis to be recorded: the reporter's consent, a written notice to them beforehand, or why telling them would jeopardise the investigation. The written notice can be given in the case conversation. APP	Case > Export	Decide whether the disclosure is lawful; inform the reporter. ORG
Art. 15 §1–3 — The GDPR applies; the entity is the controller.	HRemia acts as processor under a data processing agreement (A4).	—	Controller duties. ORG
Art. 15 §4 — Collect only what is necessary; delete data clearly unrelated or excessive without delay.	An anonymous report holds no user, name, contact details, department or IP address, enforced by the database. Every question of the public form beyond the report itself is optional, and what could identify their author is removed from evidence files before they are stored. DB A handler removes a passage that is clearly unrelated or excessive wherever it appears in the case (subject, report, questionnaire answers, messages, minutes and their earlier versions) and can erase an evidence file; a visible marker takes its place, and who removed it, when and why is recorded (the reason as an encrypted internal note, never the removed text). APP	<code>test_an_anonymous_report_keeps_nothing_that_points_at_a_person; test_excess_data_is_erased_and_a_case_is_kept_only_as_long_as_decided; test_a_handler_erases_an_excessive_file_and_retention_erases_them_all</code>	Decide what is unrelated or excessive, and have it removed without delay. ORG
Art. 15 §5–8 — Restrictions on informing the reported person and on data-subject rights; breach notice to the ΑΠΔΠΧ where informing the data subject would harm the purposes of the law.	The platform never informs reported persons or third parties by itself. HRemia informs the organisation of a personal-data breach without undue delay (GDPR art. 33(2)).	—	Decide and document the restrictions and notices. ORG

Requirement	HRemia	Verify	Organisation
Art. 16 §1; KYA art. 3 §6 — Keep a record of every report; in the private sector a special file kept by the Y.Π.Π.A. with a registration number.	The special file: one entry per report, whatever the channel, with its registration number (HRM-XXXX-XXXX), channel, receipt, acknowledgement, feedback, referrals and outcome; dates and codes only, as JSON or printable. A case file cannot be deleted from the application; when a closed case's content is erased at the end of its retention period, its entry in the special file stays, marked erased. APP DB	Inbox › Special file	Adopt the internal rules for the special file. ORG
Art. 16 §1 — Store reports for a reasonable and necessary period, and in any case until any investigation or proceedings end.	Case files are kept under their own encryption key, so erasing conversations never touches a file that must be retained. The organisation sets how long closed cases are kept (12 to 120 months from closing); at or after closing, the handlers can instead record a date for a single case, or keep it until the proceedings it started are over, and can place it on legal hold with a reason. When the period or the recorded date has passed, the platform erases the content of the closed case (text, questionnaire, messages, minutes, referrals, evidence files); its entry in the special file (registration number, dates, codes) stays, marked erased. An open case and a case kept until the proceedings are over are never erased. A legal hold keeps a case beyond the organisation's period; a date the handlers record for a single case is suspended while the hold lasts. The compliance centre flags closed cases without a retention decision. APP TEST	<code>test_closed_cases_ past_the_period_lose_ their_content_held_ and_open_ones_never; test_handlers_set_and_ lift_the_legal_hold_ with_a_reason_and_it_ stops_deletion; test_ excess_data_is_erased_ and_a_case_is_kept_ only_as_long_as_ decided</code>	Set the retention period for closed reports; decide each closed case's retention; place a case on legal hold while an investigation or proceedings are pending. ORG
Art. 16 §2-5 — Oral reports: recording only with lawful consent; otherwise complete and accurate minutes, which the reporter can check, correct and sign; a refusal to sign is noted.	Minutes of a telephone call, voice message or meeting: draft › shared with the reporter › confirmed on the platform or correction requested (the confirmation is recorded as the reporter's agreement, a simple electronic signature within art. 3(10) of Regulation (EU) 910/2014); or signed on paper, or refused, which is noted. Once shared they are never deleted; the reporter sees them on the tracking page or in their own case. A flag records whether a recording was made with consent; audio is not stored on the platform. APP DB	<code>test_minutes_are_ checked_corrected_and_ confirmed_by_the_ reporter</code>	Obtain consent before recording; keep any audio outside the platform under your own controls. Decide whether online confirmation suffices or a signature on paper is also wanted. ORG
N. 4990/2022 — protection and penalties (arts 17, 21-23)			
Art. 17 — Retaliation of any kind is prohibited.	Not a software function. Dated records and the audit trail help show what happened and when. The assistant never steers a person towards the one they describe as causing harm.	—	Prevent retaliation; brief managers. ORG
Art. 21 §2 — The identity of reported persons is protected throughout the investigation; the rules of arts 11, 13 and 14 apply to them too.	Case content, including what it says about the persons concerned, is readable only by the designated handlers and is encrypted; notifications carry no content. The pseudonymised export replaces the reporter's identity and, as "Third party A, B...", the other persons the officer selects: the people and organisations the reporter listed in the form as involved are proposed, and e-mail addresses and telephone numbers found in the case are listed. Nothing else is replaced automatically, so the officer reviews the text before it is sent (C2); e-mail addresses and telephone numbers left in it are flagged. APP DB	<code>test_designating_ handlers_closes_cases_ to_other_hr_in_the_ database_itself; test_ pseudonymised_export_ covers_inflections_ referral_details_and_ chosen_third_parties</code>	Review the text before forwarding and have the names of persons concerned replaced where the recipient does not need them. ORG

Requirement	HRemia	Verify	Organisation
Art. 22 — A clause or agreement that waives or limits the rights and remedies of the law, including an arbitration clause, is void to that extent.	The public page asks the reporter to accept nothing beyond acknowledging the privacy notice, and never presents internal reporting as a precondition for going to the E.A.Δ.	Public page	Keep such clauses out of contracts, policies and settlements. ORG
Art. 23 — Breaching confidentiality is a criminal offence (§1 γ); legal persons can be fined EUR 10,000 to 500,000 for offences committed for their benefit (§5).	Database-enforced access and an audit trail of every case listing, export and change of designation reduce the room for unauthorised access. DB	<code>test_every_inbox_listing_is_audited_with_its_count_only</code>	Organisational measures and training. ORG
KYA 47312/2023			
Art. 2 §1 — Written reports by post or by hand in a marked envelope, or by e-mail to the Υ.Π.Π.Α.'s address.	The officer's dedicated address is published on the public page. Letters and e-mails are registered in the special file with the time they arrived. APP	<code>test_the_page_shows_the_reports_officer_once_hr_sets_them</code>	Keep the mailbox; receive envelopes. ORG
Art. 2 §2 (α)–(β) — Telephone and voice messages: recorded only with consent; otherwise minutes checked, corrected and signed. (γ) Meeting on request, with minutes.	Minutes workflow as under art. 16; the form records a meeting request. APP	<code>test_minutes_are_checked_corrected_and_confirmed_by_the_reporter</code>	Offer the line if chosen; hold the meeting. ORG
Art. 2 §3 — The platform: in a prominent place on the website, clear instructions, accessible to persons with disabilities, in Greek and English.	Five short steps with guidance on each; Greek and English, and eight more languages. Accessibility built in: labelled fields, errors tied to their field, each step announced to screen readers. APP	Public page	Place the link prominently; include the page in your accessibility review. ORG
Art. 2 §4 — The Υ.Π.Π.Α. helps the reporter with information on rights and the procedure.	The public page explains who is protected, what happens next, the limits of anonymity and the external channel, and shows the officer's contact.	Public page	Assist on request. ORG
Art. 3 §2 — Provable acknowledgement within 7 working days; with no contact details, the reporter follows up with the registration number.	Anonymous reporters read the acknowledgement on the tracking page; the page tells them the date to come back. APP	<code>test_the_tracking_page_tells_the_reporter_when_to_expect_an_answer</code>	—
Art. 3 §3 — For an oral report, the signed minutes are the acknowledgement; a refusal is noted.	Minutes the reporter signed on paper, or confirmed on the platform (see art. 16 above), count as the acknowledgement; a refusal is recorded. APP	<code>test_minutes_are_checked_corrected_and_confirmed_by_the_reporter</code>	Decide whether online confirmation counts as signing (see art. 16). ORG
Art. 3 §4, §6 — Confidentiality measures; the special file.	See art. 14 and art. 16 above.	—	—
Art. 3 §7 — Someone not competent who receives a report passes it to the Υ.Π.Π.Α. without changing it or revealing the reporter.	An HR administrator who is not a handler, or a manager, can register a report they received: it goes to the handlers unchanged and they cannot read it back. DB	<code>test_someone_not_competent_forwards_a_report_they_then_cannot_read</code>	Instruct staff to forward reports. ORG

Requirement	HRemia	Verify	Organisation
Art. 4 §1 (α) Forwarding, pseudonymised. (β) Archiving on grounds βα, ββ, βγ, with notice to the reporter; reopening on new evidence.	Referral log and pseudonymised case-file export: the reporter's name, contact details and account are replaced by "Reporter A", also inside the free text; the officer can also have the other persons the reporter named, and the contact details the platform finds in the case, replaced ("Third party A"...). The export lists evidence files by name and SHA-256 hash, never their content. Outcome codes carry the ground; archiving as out of scope records whether other breaches were forwarded. (APP)	<code>test_pseudonymisation_finds_the_name_with_or_without_accents_and_leaves_amounts_alone; test_pseudonymised_export_covers_inflections_referral_details_and_chosen_third_parties; test_the_exported_case_file_lists_names_and_hashes_never_content</code>	Read the free text before sending: a detail can still identify. (ORG)
Art. 4 §2 — A crime prosecuted ex officio: a copy to the prosecutor without delay, and the reporter is told.	A referral marked as such can only go to the prosecutor (database CHECK); the notice to the reporter is prepared in their conversation. (DB)	<code>test_referrals_notices_and_a_pseudonymised_case_file</code>	Send the copy. (ORG)
Art. 4 §3 — A report making allegations against the Υ.Π.Π.Α., or against the organ that investigates reports within the entity, is only registered in the special file and forwarded to the Ε.Α.Δ., and the reporter is told.	The reporter, or a handler, marks the case as concerning the Υ.Π.Π.Α. or a deputy. Where another handler can act, the mark withdraws the Υ.Π.Π.Α. from the case automatically, and the withdrawal is recorded; where no one else can, the Υ.Π.Π.Α. registers and forwards the case without being shown who reported. The case then allows only the steps of registering and forwarding it (acknowledgement, minutes, access code, pseudonymised export, removal of excessive data, forwarding to the Ε.Α.Δ. with the notice to the reporter, closing as forwarded); every other action is refused, for every handler. Only a deputy who is not concerned can remove a mark made by mistake, with a recorded reason, and the reporter is told; the Υ.Π.Π.Α. never can. (APP)	<code>test_a_report_about_the_officer_is_only_registered_and_forwarded_to_the_ead; test_a_deputy_removes_a_mistaken_mark_with_a_reason_and_the_reporter_is_told</code>	Forward to the Ε.Α.Δ.; mark a report about the internal investigating organ in the same way. (ORG)
Art. 4 §4 — Retention.	See art. 16 above.	—	—
Art. 5 §1–3 — Follow-up and contact; the competent organ informs the Υ.Π.Π.Α. promptly; feedback within 3 months; the external body's answer is kept.	Case conversation; referral log with the date and content of the answer received; feedback deadline as under art. 10 §2 (Ζ). (APP)	<code>test_referrals_notices_and_a_pseudonymised_case_file</code>	Make sure the competent organ reports back. (ORG)

A3 Directive (EU) 2019/1937, for companies outside Greece

For companies established in other member states, the channel follows the Directive; the national transposition may add requirements **(A1)**. The compliance centre checks such a company against the Directive, and the platform never sets a deadline later than the Directive's.

Article	Requirement	HRemia	Organisation
Art. 4	Who is protected: workers, the self-employed, shareholders and management, volunteers and trainees, contractors' and suppliers' staff, former workers and applicants; facilitators and related persons.	Public page per company with no account; the reporter's relationship is asked. (APP)	Link the page on the website. (ORG)
Art. 6(1)	Protection requires reasonable grounds to believe the information was true and in scope.	Explained on the public page, never promised. (APP)	—

Article	Requirement	HRemia	Organisation
Art. 6(2)–(3)	Whether anonymous reports must be accepted is left to national law; anonymous reporters later identified are protected.	Anonymous reporting on every route, with a two-way mailbox. DB	Check the national rule (see A1). ORG
Art. 7	Internal reporting is encouraged where the breach can be addressed effectively internally.	The public page describes the external route as well and never makes internal reporting a precondition.	—
Art. 8(1), (3)	Employers with 50 or more workers establish internal channels.	The platform is the channel; the compliance centre shows what is still missing.	Decide whether the duty applies. ORG
Art. 8(5)–(6)	Channels may be operated by a third party; employers with 50–249 workers may share resources.	HRemia operates the channel as processor; handlers are designated by the organisation.	Designate the handlers. ORG
Art. 9(1)(a)	Secure channels that keep the reporter's identity confidential and keep unauthorised staff out.	Database-enforced exclusive access for designated handlers; encrypted case text (B3, B4). DB	Designate before launch. ORG
Art. 9(1)(b)	Acknowledge within 7 days.	7 days from receipt; reminder 24 hours before; provable acknowledgement. APP	Acknowledge. ORG
Art. 9(1)(c)	An impartial person or department to follow up.	Designated reports officer and deputies; recusal per case, kept on record; eligibility declaration. DB	Choose impartial handlers. ORG
Art. 9(1)(d)–(e)	Diligent follow-up, including of anonymous reports where national law provides for it.	Assignment, internal notes, escalation with a recorded reason, conversation with anonymous reporters. APP	Follow up. ORG
Art. 9(1)(f)	Feedback within 3 months of the acknowledgement (or of the end of the 7 days).	3 calendar months, never later than the Directive's limit; reminder 3 days before; feedback dated. APP	Give feedback. ORG
Art. 9(1)(g)	Clear information on reporting externally to competent authorities.	The public page, the tracking page and the in-app form have an external-channel section; for companies outside Greece it refers to the competent authorities of their country, and the tracking page takes the country from the report's own company.	Name the national authority in your information. ORG
Art. 9(2)	Reporting in writing or orally, and a meeting on request.	Platform, officer's register for letters, e-mails, calls, voice messages and meetings; minutes. APP	Offer the oral route if national law requires it. ORG
Art. 16	Confidentiality of the reporter's identity.	As art. 9(1)(a); pseudonymised exports; notices without content. DB APP	—
Art. 17	Processing under the GDPR; personal data manifestly not relevant is not collected or, if collected by accident, is deleted without undue delay.	Anonymous reports hold no identifying fields; every question of the public form beyond the report itself is optional; what could identify their author is removed from evidence files before they are stored; a handler removes a passage or a file that is not relevant wherever it appears in the case, and the removal is recorded with its reason. DB APP	Decide what is not relevant. ORG
Art. 22(2)	The identity of persons concerned is protected while investigations are ongoing.	Case content is readable only by the designated handlers; the pseudonymised export replaces the reporter's identity and the other persons the officer selects, and the officer reviews the text before it is sent (C2). DB APP	Review the text before forwarding; have names of persons concerned replaced where not needed. ORG

Article	Requirement	HRemia	Organisation
Art. 18(1)	Records of every report, kept no longer than necessary.	Register of reports with dates and codes. A closed case is kept for the period the organisation sets (12 to 120 months from closing) or until the date its handlers record; its content is then erased automatically and its register entry stays. An open case is never erased; a legal hold keeps a case beyond the organisation's period, and suspends any date the handlers record for the case (B7). APP	Set retention per national law. ORG
Art. 18(2)-(4)	Oral reports and meetings: recording with consent, or accurate minutes the reporter can check, correct and sign.	Minutes workflow: shared, confirmed or corrected online, signed on paper, or refused and noted. APP	Obtain consent before recording. ORG
Art. 19	Prohibition of retaliation.	Not a software function; dated records and the audit trail support evidence.	Prevent retaliation. ORG

Verification: `test_a_company_outside_greece_is_checked_against_the_directive`, `test_tracking_names_the_reports_own_company_country` and `test_under_the_directive_a_report_about_the_officer_is_handled_by_the_others`. The same public page, tracking page, special file, minutes, evidence files and referral log described in A2 serve every country; only the legal texts, the external authority and the labels change. The Greek rule that a report about the officer is only registered and forwarded (KYA art. 4 §3) is not applied: such a report is handled by the other handlers, and the reports officer is withdrawn from it where another handler can act.

A4 GDPR

Your organisation is the controller; HRemia is the processor. This section sets out the roles, the lawful basis per feature, how minimisation and storage limitation are applied, the data-subject rights, the DPIA, the sub-processors and the contract.

1. Roles and the contract

Party	Role	Basis
Your organisation	Controller for all data processed on its behalf: employees, reporters and persons named in reports, and also employees' private conversations with the assistant. Being controller does not require having access to the data.	GDPR art. 4(7); for reports, N. 4990/2022 art. 15 §3 in Greece; CJEU C-210/16, para. 38, and C-25/17, para. 69
HRemia	Processor. It processes only on your documented instructions and may not use your data for its own purposes, such as training or evaluating AI models.	GDPR arts 28, 29, 28(10)
HRemia	Independent controller only for its own customer-relationship data (contacts, invoicing), its website contact form and the security records of its infrastructure.	—
Sub-processors	Hosting (Hetzner), DNS, protection against denial-of-service attacks and routing for hremia.eu and www.hremia.eu (Cloudflare), AI providers, browser push services (point 8).	GDPR art. 28(2) and (4)

The data processing agreement (DPA) is part of the service agreement and is based on the standard contractual clauses of Implementing Decision (EU) 2021/915. It covers every point of art. 28(3): processing only on documented instructions, including transfers (a); confidentiality of staff (b); the art. 32 security measures (c); the conditions for sub-processors (d); assistance with data-subject requests and with arts 32–36 (e, f); deletion or return at the end (g); information and audits, and an alert if an instruction appears to infringe the GDPR (h). Its annexes describe the processing (with the art. 9 and art. 10 data), the technical and organisational measures (Part B of this annex), the sub-processors, the reporting channel, the AI functions, the retention and deletion programme and, where relevant, a country annex (for a company in Greece, the Greek country annex). Sub-processor changes are notified in advance, with a right to object; if an objection cannot be met with an alternative provider in a dedicated configuration, the organisation may terminate. The DPA lists exhaustively the cases in which HRemia's staff may access the infrastructure technically: support on the organisation's written request, a security incident and a legal obligation; each access is documented and notified to the organisation where the law allows. Where the website's general texts and the signed DPA differ, the DPA prevails.

2. Lawful basis per feature

The controller chooses and documents the lawful basis (arts 5(2), 24). For special categories, a basis under art. 6 and a condition under art. 9(2) are both needed (CJEU C-667/21), and data that reveals a special category indirectly counts too (C-184/20; C-252/21). Our assessment, for your decision:

Feature	Personal data	Art. 6	Art. 9 / art. 10	Note
Reporting channel	The reporter (if named), the persons concerned and the facts; possibly health, sex life, trade-union membership, alleged offences	6(1)(c) with the national law (Greece: N. 4990/2022 arts 9, 15 §2); 6(1)(f) where the organisation is not obliged	9(2)(g), substantial public interest as set by the Directive and the national law (our assessment: N. 4990/2022 does not regulate special categories expressly); 9(2)(f), legal claims; for harassment also 9(2)(b) with v. 4808/2021. Art. 10 data: under the Directive and the national law	Record the art. 10 reasoning in the DPIA
Leave	Kind of leave (sick, maternity, parental...), dates, certificate received yes/no and its date	6(1)(b), (c)	9(2)(b): the employer's labour and social-security obligations; in Greece art. 27 §3 with art. 22 §3 v. 4624/2019	No diagnosis field; no free-text note on health-related periods
Employment record, HR directory	Contract type, grade, dates; office contacts	6(1)(b), (c)	—	What HR recorded; no national ID, no bank data

Feature	Personal data	Art. 6	Art. 9 / art. 10	Note
Assistant: private conversations, attachments, wellbeing profile, Memory	Whatever the employee chooses to write: possibly health, family, trade-union or religious matters. The assistant also receives the employee's own leave data, including health-related periods	Decided by the organisation	Decided by the organisation. 9(2) (b) and (h) are hard to apply to an optional support tool; explicit consent (9(2)(a)) fits most clearly, with the limits in point 3	The chosen condition must also cover the health-related leave data the assistant receives
Surveys	Multiple-choice answers	6(1)(f)	Only if the organisation asks about a special category	Results only for groups of 5+
Training	Assignments, completion, quiz score, attestation	6(1)(b), (c) or (f), depending on whether the training is legally required	—	Scoring is arithmetic, not AI
Announcements, notifications	Read and acknowledgement records where HR asks for them; push subscriptions	6(1)(b) or (f)	—	The reader is told when their confirmation is recorded
Breaks	Minutes used today (cache only); daily company totals	6(1)(f), or (b) where part of the employment terms	—	Purpose limited to the allowance and totals
Audit log	Who did what and when (metadata)	6(1)(c), (f): accountability and security	—	Never message or report content

3. Consent at work, and how the platform supports the organisation's choice

Consent is valid only when freely given, which is rarely the case between employer and employee (recital 43; EDPB Guidelines 05/2020, paras 21–22). In Greece, employee consent must also be in writing or in electronic form, clearly separate from the employment contract, refer expressly to special categories where they are involved, and state the purpose and the right to withdraw (art. 27 §2–3 v. 4624/2019). The platform supports whichever basis the organisation chooses:

- Using the assistant is optional.
- HR, managers and company administrators cannot read the conversations **DB** and see only aggregate usage, not who uses the assistant or how often. Not using it is invisible, and refusing consent must carry no detriment; the consent template says so.
- The application has no consent step of its own. If the organisation chooses explicit consent, HRemia provides a consent and information template (arts 7, 13 GDPR; art. 27 v. 4624/2019); the organisation collects it before giving access. Memory has its own switch, which only the employee can turn on. On withdrawal, on the organisation's instruction, HRemia deletes the employee's conversations, and the employee can delete their Memory notes at any time. Access to the assistant comes with the employee account; the platform has no separate switch per employee.

4. Data minimisation, fact by fact (arts 5(1)(c), 25)

Fact	How it is enforced
The assistant reaches only the asking employee's own records	RESTRICTIVE policies <code>companion_own_leave</code> and <code>companion_own_training</code> on the assistant's database role: even a query that forgot its filter cannot return a colleague's leave, employment record or training result (B3). DB TEST
HR and the employer cannot read conversations	The HR side of the application runs as a database role with no grant at all on the schema that holds conversations, Memory and wellbeing profiles. DB TEST
An anonymous report holds nothing that points at a person	No user account, name, contact details or department, enforced by CHECK constraints (B5); no IP address and no browser identifier (user agent) stored. DB TEST
Case content, within the organisation, only for the Y.Π.Π.A./reports officer and deputies	From their designation, enforced by the database (B3). DB TEST

Fact	How it is enforced
Figures only for groups of at least 5	Surveys, culture and wellbeing insights, breaks and the compliance centre's breakdowns; smaller groups are withheld. Assistant usage is shown only as totals. APP TEST
Breaks: no per-person record	Minutes per person live only in the cache for two days; the database holds daily totals per company and game, in a table with no user column. DB
Surveys: answers without identity	Multiple choice only; answers stored without a user identifier and without a timestamp; a separate table records who has answered, not what. DB
Health-related leave: no reason	No diagnosis field; the employee's request note and HR's note on the recorded period are dropped for sick, maternity and parental leave; a certificate is recorded as yes/no and a date. HR's short decision note on a request is kept; it should contain no health data. APP TEST
Notifications say little	Anything about a report or a health-related absence shows only "new update" on a lock screen or in an e-mail; escalation e-mails carry only the case reference. APP
Document search stays on our server	Embeddings are computed locally; only the relevant excerpts go to the AI provider with a question. APP
The employee's name and e-mail are not sent to the AI provider	The assistant receives the records listed in B8, not the identity fields. APP
Evidence files carry no hidden identity	Before a report's file is stored, photos lose GPS position, camera and date data (EXIF, XMP, IPTC); PDFs lose author, creator, dates and earlier revisions; Word and Excel files lose author, company, last-modified-by and the names on comments and tracked changes. The uploader is recorded only as reporter or handler. APP TEST
Memory keeps only what the employee stated about their work	At most 25 notes of up to 200 characters; no judgements about the employee's emotions, health or personality; special-category facts are held back unless the employee explicitly asks for that one fact to be kept; no plans to resign, sue or report the employer, and no names of other people (B8). APP TEST

5. Storage limitation (art. 5(1)(e))

- The organisation sets its retention periods in Settings > Retention and automatic deletion: a general period (default 24 months) and, where it chooses, separate periods for conversations and Memory, for closed reports (at least 12 months from closing) and for the audit trail, each from 6 to 120 months. A preview shows, as counts only, what the next run would delete.
- A daily run, from 03:00 in the company's time zone, deletes what has passed its period: conversations with their messages and attachments, counted from their last activity; Memory notes not created or changed within the conversations period; the content of closed reports, whose entry in the special file stays, marked erased; and audit entries, except those about a case whose content is kept. For reports the specific rules apply (Greece: N. 4990/2022 arts 15 §4, 16): an open case is never deleted; the handlers can set a date for a single case, keep it until the proceedings it started are over, or place it on legal hold with a reason, which keeps it beyond the organisation's period (and suspends any date recorded for the case, B7). Each run leaves one audit entry, with counts only. [APP](#) [TEST](#)
- Deleted data remains in the encrypted backups until their cycle ends, up to about six months (B7).
- Short-lived data expires automatically: break minutes per person after 2 days, rate-limit counters after at most 10 minutes, sign-in links after 20 minutes, sessions after 7 days.

6. Data-subject rights

- Access and portability (arts 15, 20):** every user can download a machine-readable export of the data the organisation holds about them (profile, reports they filed, training records, a summary of their assistant usage, and their Memory notes with their own Memory activity): Account > Export. Employees read their own conversations in the app; a machine-readable export of their conversations and the deletion of a single conversation are carried out by HRemia on the organisation's instruction, without disclosing the content to HR, and conversations are deleted automatically at the end of the retention period (B7).
- Rectification and erasure:** HR corrects records; employees edit or delete each Memory note, delete all of them, or switch Memory off, at any time, on the "What your assistant remembers" screen of their account or from the conversation; a person whose role changes keeps these rights over their notes. Deleting an employee's account deletes their conversations, attachments, wellbeing profile and Memory.

- **Reported persons and third parties:** the national whistleblowing law may restrict information and rights while needed to protect the report and the reporter (Greece: N. 4990/2022 art. 15 §5–7); the controller decides. **ORG**
- **Anonymous reporters** have no account and nothing stored that identifies them; they follow their case with the reference and access code.
- **No solely automated decisions** with legal or similarly significant effect (art. 22): the platform takes no decisions about employees.

7. The DPIA

A DPIA is mandatory for this processing (art. 35(1), (4)). In Greece the ΑΠΔΠΧ list (Decision 65/2018) names whistleblowing systems in item 1.3, which on its own makes a DPIA mandatory, and AI applications in item 3.1, which does so together with a criterion of the first or second category. HRemia assists under art. 28(3)(f): the contract proposal includes a DPIA support pack (data flows, a table of lawful bases, an assessment of risks and measures, an employee-information template covering the AI assistant and Memory, and an explicit-consent template if consent is chosen); this annex provides the data flows (B1), the lawful bases (point 2), and the risks and measures (B3 to B8). The platform keeps a printable DPIA record (Compliance) and the compliance centre records when the DPIA was done. Where appropriate, the views of workers' representatives are sought (art. 35(9)). **ORG**

8. Sub-processors and transfers

Sub-processor	Service	Location	Data	Safeguards
Hetzner Online GmbH, Germany	Hosting of the platform, database and files	Falkenstein, Germany	All platform data	EU; art. 28 agreement
Hetzner Online GmbH	Encrypted off-site backups	EU	Database backups	EU; art. 28 agreement
AI model providers, primary and fallbacks (established providers such as OpenAI, Anthropic and Google; those used for each organisation are named in its sub-processor list)	Answers of the assistant and the AI coach, Memory updates, quiz drafting, translation; the fallbacks, in order, only when the one before is unavailable	Per provider, stated in the list	As listed in B8	Business terms: no training on your data, limited retention (period stated per provider), data processing agreement; outside the EEA: an adequacy decision or the standard contractual clauses of Implementing Decision (EU) 2021/914
Browser push services (Google, Mozilla, Apple, Microsoft, depending on the device)	Delivering push notifications, only if the employee allows them	Per provider	Content encrypted end to end, plus delivery metadata	The provider cannot read the content
Cloudflare, Inc. (USA)	DNS, protection against denial-of-service (DDoS) attacks and routing of traffic to our server, for hremia.eu and www.hremia.eu	Cloudflare's network, as a rule the location nearest the visitor	The visitor's IP address and the traffic in transit; stores no platform content (caches only static application files, such as images and code)	Cloudflare's data processing agreement with standard contractual clauses; certification under the EU-US Data Privacy Framework

Where a provider processes outside the EEA, the transfer relies on an adequacy decision, for example Implementing Decision (EU) 2023/1795 (EU-US Data Privacy Framework) for certified entities, or on the standard contractual clauses of Implementing Decision (EU) 2021/914 with a transfer impact assessment. For Cloudflare, Inc. the safeguards are its certification under the EU-US Data Privacy Framework and the standard contractual clauses of its data processing agreement. Document search runs on HRemia's own server, with no third party. Platform e-mails (sign-in links, notices) are sent by the mail service of our own server in Germany (mail.hremia.eu), which does not pass through Cloudflare, and carry no case or chat content; escalation e-mails carry only the case reference. YouTube videos an organisation embeds in a course are its own content choice: the employee's browser connects to Google when playing them.

9. Switching provider (Data Act)

HRemia is a provider of data processing services within the meaning of the Data Act, so its Chapter VI switching rules apply to the service agreement: a notice period of at most two months, a transitional period of 30 days to complete the switch, export of the organisation's data in a structured, commonly used and machine-readable format, and no switching charges from 12 January 2027. At the end of the contract data is returned or deleted as the DPA provides (GDPR art. 28(3)(g)). The export of the organisation's data as a whole is carried out by HRemia on request; self-service exports exist for single persons, for the special file and for each case file.

A5 AI Act

Regulation (EU) 2024/1689 has been in force since 1 August 2024 and applies in stages; Regulation (EU) 2026/1744 moved some dates. HRemia provides AI systems built on general-purpose models of established providers; your organisation deploys them.

Date	What applies	For HRemia
2.2.2025	Prohibited practices (art. 5); AI literacy (art. 4)	Applies; see below
2.8.2025	Obligations of providers of general-purpose AI models (arts 53, 55)	Borne by the model providers
2.8.2026	Transparency obligations (art. 50) and most remaining provisions	Applies; see below
2.12.2026	Machine-readable marking of AI-generated content (art. 50(2)) for generative systems placed on the market before 2.8.2026 (art. 111(4), inserted by Regulation (EU) 2026/1744); a system first placed on the market later must comply from that date	Applies: every AI-generated text carries a machine-readable mark (see Transparency below)
2.12.2027	High-risk systems of Annex III, as postponed by Regulation (EU) 2026/1744	Not high-risk by intended purpose (below)
2.8.2028	High-risk systems under Annex I (products)	Not applicable

Roles

HRemia is the **provider** (art. 3(3)) of the AI systems it offers under its name: the assistant with its Memory, the AI coach, quiz drafting and translation of content. They are built on general-purpose AI models of third-party providers, which bear the obligations of arts 53 and, where applicable, 55. HRemia does not train or fine-tune models. Your organisation is the **deployer** (art. 3(4)). A deployer that changes the intended purpose so that a system becomes high-risk takes on the provider's obligations (art. 25(1)(c)).

Intended purpose and classification

The systems inform and support. They are **not** intended for decisions about workers (recruitment, evaluation, promotion, termination, allocation of tasks, monitoring of performance or behaviour) and not for evaluating learning outcomes: quiz scores are computed arithmetically, not by AI. With this purpose they are not high-risk under Annex III, points 3 (education and vocational training) and 4 (employment). The intended purpose and the prohibited uses are set out in the AI annex of the contract. The platform takes no decision with legal or similarly significant effect on employees (GDPR art. 22).

Prohibited practices (art. 5)

- Emotion recognition at the workplace (art. 5(1)(f)).** The prohibition concerns AI systems that infer the emotions of people at work from biometric data (art. 3(39)). The platform captures no biometric data: no voice, no camera, no keystroke patterns. It does not detect or score anyone's emotions, mood or burnout, and the Memory function is forbidden to hold judgements about emotions or health **TEST**. An employee may choose to attach a picture to a conversation; the assistant and the AI Coach are instructed never to identify, infer, rate or describe anyone's emotions, mood, stress, attitude, personality or intentions from a face, a body posture, a photo or a voice, the employee's own included, and the rule is repeated next to every image a model receives **TEST**. For wellbeing, the organisation receives only totals from categories employees choose themselves, for groups of at least five. See the Commission's guidelines on prohibited practices, C(2025) 5052, paras 244–251 and 257.
- Manipulation and exploitation of vulnerabilities (art. 5(1)(a), (b)).** The assistant is instructed not to diagnose, to point to professional help and crisis lines when someone is at risk, never to take or suggest employment decisions, never to promise an outcome, and never to steer a person towards the one they describe as causing harm.

Transparency (art. 50)

- Art. 50(1), interaction with an AI system.** Every conversation, new or reopened, and every AI Coach session opens with the notice "You're talking to an AI assistant, not a person.", shown before anything the model writes. A permanent notice under the message field reads: "Hremia is an AI assistant, not a doctor or therapist. A human can always help." The training assistant is labelled "AI Coach". The assistant is designed to say that it is an AI whenever asked, in any words and as often as asked, and never to claim to be human (Commission guidelines C(2026) 5054, para. 40); both notices are part of the page and do not depend on the model's answers. It also says plainly when it cannot see an earlier conversation, beyond what Memory keeps if the employee has switched it on, instead of pretending to remember.
- Art. 50(2), marking of AI-generated text.** Every text a model writes or translates on the platform is marked in machine-readable form: an **ai_generated** flag with a provenance object (generator, model class, time of creation) in the data; an **X-AI-Generated** header on every API response that carries such text; the same marking on the frames of a streamed

reply that carry model text; a column in the database derived from who wrote the row; schema.org markup in the page; and, in exports, pointers (RFC 6901) to every AI-generated segment. It covers the replies of the assistant and the AI coach, Memory notes written by the automatic update, quiz questions drafted or translated by a model, and translated announcements with their push notifications, e-mails and calendar files. Text a person wrote carries no mark, and a Memory note the employee corrected becomes theirs. The scheme is published in machine-readable form at [/v1/ai/provenance](#), and a visible “AI” label accompanies AI-written Memory notes, quiz questions and translations. The marking is metadata: the text itself is not altered and carries no watermark. The Commission's guidelines also call for a means of detection available to those exposed to the content, and for robustness as far as technically feasible (C(2026) 5054, paras 69–72, 75–76 and 80–86); HRemia reviews the adequacy of its scheme against the code of practice under art. 50(7). [APP](#) [TEST](#)

- The Commission's guidelines recommend a first-turn disclosure together with a persistent label (para. 37) and consider periodic, context-aware reminders likely to be necessary in riskier contexts, among them conversations in which users may express emotional distress or seek legal or health advice (para. 40). The platform shows both notices described above, and the assistant is instructed to say, in one short clause, that it is an AI in long or emotionally heavy conversations, when the employee asks for legal or health guidance, and whenever it points them to a person who can help.

AI literacy (art. 4) and the employer’s obligations

Providers and employers take measures to support the AI literacy of their staff (art. 4, as amended by Regulation (EU) 2026/1744). HRemia supplies an AI transparency note with instructions for administrators and employees; the organisation runs its own literacy measures, for which the training module can be used [ORG](#). The employer obligations of art. 26, including informing worker representatives (art. 26(7)), apply only to high-risk systems and so not here. Informing employees under GDPR arts 13–14 still applies, and the notice should cover the assistant explicitly; HRemia provides a template.

Greece

The ΑΠΔΠΧ is the market-surveillance authority for the art. 50 obligations (v. 5321/2026 art. 3 §1), so the same authority oversees GDPR and AI Act transparency for this service. Breaches of the AI Act can now be reported through the N. 4990/2022 channel (v. 5321/2026 art. 20); the public form lists the AI Act among the areas a report may concern. The specific duty to inform employees about AI systems in art. 9 v. 4961/2022 was repealed from 20.7.2026 (v. 5321/2026 art. 26).

A6 Who does what: platform and organisation

HRemia provides the channel, the safeguards and the records; the organisation designates the people, takes the decisions and meets the duties the law places on the employer.

Area	HRemia provides	Your organisation does
Reporting channel	Public page and in-app form, with evidence files stripped of identifying metadata; officer's register for letters, e-mails, calls, voice messages and meetings; two-way mailbox for anonymous reporters	Links the page on its website; decides on oral routes; holds meetings on request
Designation	Υ.Π.Π.Α./reports officer and deputies with database-enforced exclusive access; term; eligibility declarations; history	Designates eligible, independent people; notifies the Labour Inspectorate (Greece)
Deadlines	Computed at receipt; reminders; provable acknowledgement and feedback; metrics	Acknowledges, follows up and gives feedback in time
Handling	Referral log, outcome codes with archive grounds, reopening, pseudonymised export, report-about-the-officer route	Investigates through its competent organs; decides; informs the reporter
Publicity	A4 poster with QR code, website button, evidence pack	Posts the information at the workplace; places the link prominently
Data protection	Processor measures (B2 to B7), DPA, sub-processor list, DPIA support	Controller: lawful bases, employee information, DPIA, retention decisions, data-subject requests
AI	Intended purpose, safeguards, AI notices and machine-readable marking, no training on your data	Deploys within the intended purpose; AI literacy; informs employees
Employees and representatives	Aggregates only (5+), no individual monitoring, templates	Informs and, where national law requires, consults worker representatives

Checklist before going live

- ☐ Set the company's country and legal details (name, tax number, registered office).
- ☐ Designate the Y.Π.Π.A./reports officer and at least one deputy, and record the term, as a step of activation and before the public page is put to use (the page is technically on by default: switch it off in Settings until the designation is recorded).
- ☐ Each designee declares their eligibility in the platform.
- ☐ Greece: notify the Labour Inspectorate and record the notification.
- ☐ Adopt the internal reporting procedure (in Greece, the rules of the special file) and record it.
- ☐ Carry out the DPIA and record it.
- ☐ Place the website button prominently and record the page address.
- ☐ Print and post the workplace poster, and record it.
- ☐ Decide on oral reporting (telephone, voice messages) and on meetings.
- ☐ Choose the lawful bases (A4 point 2); if consent is chosen for the assistant, collect it with the template.
- ☐ Inform employees (GDPR arts 13–14), covering the assistant and the AI functions.
- ☐ Inform or consult worker representatives where national law requires it.
- ☐ Upload the organisation's own policies and regulations for the assistant, and keep them current.
- ☐ Set the retention periods (general, conversations and Memory, closed reports, audit trail) and review the preview of what the daily run would delete.
- ☐ Sign the service agreement and the DPA; review the sub-processor list.
- ☐ Plan AI-literacy measures for administrators and employees.

The compliance centre (.../whistleblowing) tracks the items the platform can see and records, with date and proof, the ones it cannot: the website link, the workplace notice, the Labour Inspectorate notification, the procedure and the DPIA. Its evidence pack can be printed for an auditor or for the Labour Inspectorate; it contains no report content and no information about reporters.

PART B

Technical

For IT, security and architecture: how the platform is built and hosted, who can reach what down to the database policies, how data is encrypted, logged, backed up and deleted, what the AI receives, and which tests prove it.

- B1 Architecture and data flow
- B3 Access control
- B5 Anonymity by design
- B7 Backup, retention, deletion
- B9 ISO/IEC 27001 mapping

- B2 Hosting, network, TLS
- B4 Encryption and keys
- B6 Audit and logging
- B8 AI processing
- B10 Evidence: tests

B1 Architecture and data flow

HRemia is a web application used in the browser or installed as a web app on a phone; nothing is installed on the organisation's network. Everything it stores lives on its server in Germany and in encrypted backups in the EU. Its addresses hremia.eu and www.hremia.eu are served through Cloudflare's network, for protection against denial-of-service attacks (route 1).

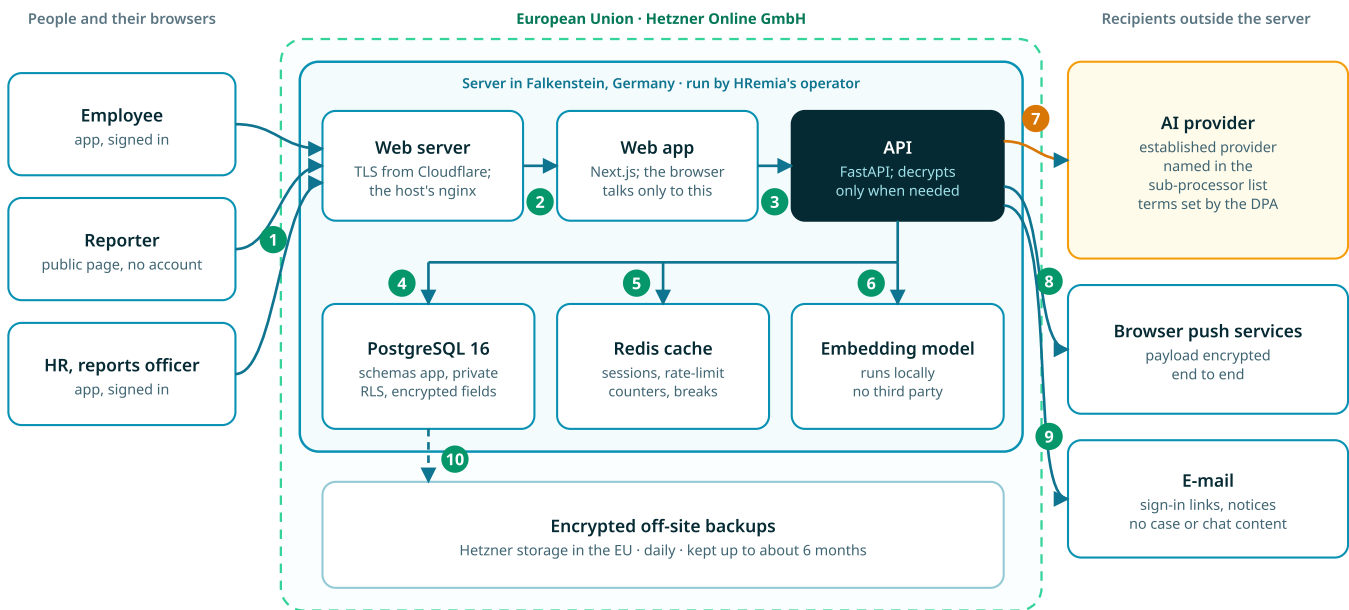


Figure 1. Numbers refer to the table below. Route 1 runs through Cloudflare's network (DNS, protection against denial-of-service attacks) for hremia.eu and www.hremia.eu, with TLS on both legs; e-mail (route 9) does not. Reports, surveys and break data never take route 7.

#	Hop	What crosses it	Protection
1	Browser → Cloudflare → web server	Pages, messages, reports and their evidence files, the session cookie	TLS from the browser to Cloudflare and TLS from Cloudflare to our server (SSL mode "Full (strict)", which validates our server's certificate); Cloudflare (DDoS protection, A4 point 8) stores no platform content and caches only static application files; cookie HttpOnly, Secure, SameSite=Lax; the public reporting page needs no account
2	Web server → web app	The same, inside the server	Local connection

#	Hop	What crosses it	Protection
3	Web app → API	The browser never calls the API directly; the web app forwards its requests	Internal container network
4	API → PostgreSQL	All stored data	Internal network; three database roles, row-level security, encrypted fields (B3, B4)
5	API → Redis	Session look-ups (the token's hash with the user's id, company, role, e-mail, display name and language, until the session ends), rate-limit counters (IP at most 10 minutes), per-person break minutes (2 days)	Internal network, password required; snapshots on the server's disk, not part of the backups
6	API → embedding model	Document text and questions, turned into vectors for search	Same server; no third party
7	API → AI provider	Only what B8 lists per function	Named in the sub-processor list; business terms without training, under the DPA (B8); an endpoint configured for the organisation alone must use https
8	API → push services	An encrypted notification; sensitive ones say only that there is an update	RFC 8291 encryption, RFC 8292 sender identity
9	API → e-mail	Sign-in links and notices; an urgent announcement with its title and opening lines; escalation e-mails carry only the case reference	Sent through the mail service on the same server (mail.hremia.eu, STARTTLS), which does not pass through Cloudflare; no case or chat content
10	Database → backups	Encrypted database dumps	Encrypted repository in the EU; kept up to about 6 months

B2 Hosting, network and TLS

- **Server.** A dedicated (bare-metal) server rented from Hetzner Online GmbH in Falkenstein, Germany, administered by HRemia's operator. It is not shared with other Hetzner customers, but it also runs the operator's other websites and e-mail service: HRemia runs in its own containers, with its own database and internal network, and only the web server is reachable from the internet. Physical security is provided by the data-centre operator.
- **Components.** Containers for the web app (Next.js), the API (Python, FastAPI), the database (PostgreSQL 16 with pgvector) and the cache (Redis 7). The database and the cache listen only on the internal container network and cannot be reached from the internet.
- **TLS and Cloudflare.** hremia.eu and www.hremia.eu are served through Cloudflare's network on purpose, for protection against denial-of-service (DDoS) attacks; Cloudflare, Inc. is a listed sub-processor (A4 point 8). Both legs of the route are encrypted: the visitor's browser connects to Cloudflare over TLS, and Cloudflare connects to our server over TLS (SSL mode "Full (strict)", which validates our server's certificate). Cloudflare therefore processes the visitor's IP address and the traffic in transit; it stores no platform content and caches only static application files, such as images and code. On our server, the web server (nginx) terminates the TLS connection from Cloudflare and forwards to the web app. E-mail (mail.hremia.eu) does not pass through Cloudflare. An AI endpoint configured for an organisation alone must have an https address; the platform refuses plain http (B8).
- **Visitor IP addresses.** Our web server keeps no access log for hremia.eu and www.hremia.eu, and its error log for the site records only critical faults. It accepts the visitor's address from Cloudflare's **CF-Connecting-IP** header only on connections from Cloudflare's published address ranges, and passes it to the application as **X-Real-IP**, overwriting any value a browser sent. No IP address is stored in the database (B5); Cloudflare's own processing of IP addresses is described in A4 point 8.
- **Logs.** Container logs are size-limited (three files of 10 MB per container) and record events, identifiers, counts and error types, not message or report content. Some error lines name a person or a file: a failed e-mail is logged with its recipient's address, a failed attachment extraction with the file name.
- **Secrets.** Database passwords and the master key are held in the server's environment configuration, not in the code repository. Outside development the API refuses to start with empty or default secrets. **APP**
- **Rate limits per client IP address** **APP** **TEST**, keyed on the address our web server sets (**X-Real-IP**), never on a header the client can choose (**apps/api/app/core/ratelimit.py**): sign-in (10 per minute; sign-in links 5 per 5 minutes), in-app reports (30 per 5 minutes), public page (60 per minute), public report submission (5 per 10 minutes), tracking (15

- per minute), evidence files (10 uploads per 10 minutes with the reference and access code; 30 per 10 minutes for a named reporter; 60 per 5 minutes for handlers), assistant (30 messages per minute). A hidden field on the public form lets bots “succeed” while nothing is stored. If the cache is unavailable, rate limiting is skipped rather than blocking the service (fail-open).
- **Document search** uses a multilingual embedding model (384 dimensions) that runs inside the API on the same server, with vectors in PostgreSQL (pgvector, HNSW index).

B3 Access control

Access is decided twice: by the application, and again by the database, which is the one that holds even if the application code had a defect.

Roles in the application

Role	Can see	Cannot see
Employee	Their own conversations, Memory and wellbeing profile; their own leave, requests, employment record and training; their own named reports and the files on them, except files on handlers' internal notes; company documents through the assistant; announcements	Anyone else's records or conversations
Manager	Aggregate insights and survey results (groups of 5+); the staff list and training results; can register a report received in person, which goes to the handlers unchanged and cannot be read back	Conversations; report content; anyone's break use
HR administrator	Company administration (people, leave, documents, courses, announcements, settings, including retention periods); aggregate insights; the AI processing log; report content only while no reports officer is designated	Conversations, Memory, wellbeing profiles (no database grant); report content once officers are designated
DPO	Compliance pages, DPIA record, audit counts, compliance centre, retention periods, the AI processing log; report content as for HR administrators	As for HR administrators
Υ.Π.Π.Α./reports officer, deputies	A designation on an HR administrator or DPO account: full case files, including evidence files, except cases they withdrew from; the legal hold on a case	Conversations
HRemia platform staff	Aggregate numbers per organisation in the application; an organisation's AI-provider configuration (endpoints and models, never the stored keys) and its AI processing log	Any content through the application; technical access to infrastructure only in the cases of A4 point 1

Sign-in and sessions

Accounts created for an organisation, at its activation or by its HR, have no password: they sign in with a one-time link sent to the user's e-mail address, valid for 20 minutes and usable once, and no second authentication factor is used, so an account is as secure as its user's mailbox. Password sign-in (argon2id) exists only for accounts HRemia itself creates with a password, such as its platform administrator's. The session lasts 7 days and ends at sign-out; the server stores only a SHA-256 hash of the session token and of each sign-in link. The session cookie is HttpOnly, Secure and SameSite=Lax. APP

Three database roles

Role	Used for	Rights
<code>hremia_app</code>	Everything the HR side and the employee's non-chat screens do	Schema <code>app</code> under row-level security; no grant at all on schema <code>private</code> ; <code>app.audit_log</code> : INSERT and SELECT, no UPDATE or DELETE; no SELECT on HR's internal closing note and the officer's outcome note; no access to the platform keys or to an organisation's AI-provider configuration and credentials (<code>app.tenant_ai_config</code>); read-only on the AI processing log and the retention runs; <code>app.report_attachments</code> : SELECT and INSERT under the case rules, UPDATE only of the erasure columns, no DELETE
<code>hremia_companion</code>	The assistant: conversations, attachments, wellbeing profile, Memory	Schema <code>private</code> (read, write); read-only on the <code>app</code> tables it needs: the company and its wrapped chat key, its users and departments, documents, the directory, courses and course assignments, and the employee's own leave, requests, employment record and training results, these last four narrowed to the asking employee by RESTRICTIVE policies; insert-only on usage and audit records
<code>owner</code>	Schema creation and one-off upgrades at start-up, sign-in, platform administration (including an organisation's AI-provider configuration, whose sealed keys no other role can read), global checks such as e-mail uniqueness, creating a company's report key, background jobs (deadline reminders, notification delivery, the daily retention run, counting AI calls in the processing log) and the look-ups without a signed-in user: the public page by company, and anonymous tracking, with its evidence files, by reference and access code	The PostgreSQL superuser that owns the schemas; bypasses row-level security and every grant above. It never returns case or conversation content to a signed-in employee's or HR user's screen; on those screens it is used only for narrow server-side steps that the role rules cannot express, for example the e-mail uniqueness check, the reporting-channel details, showing HR and the DPO which AI endpoints serve their company (never the keys), the read-only preview of the next retention run (counts only) and rewriting an earlier version of the minutes when a handler removes a passage from a case

Row-level security

Every table in `app` that holds company data has a `tenant_isolation` policy (the exceptions are the sessions and sign-in links, which hold only token hashes); every table in `private` has an `owner_isolation` policy. The API sets the company and the user for each transaction (`set_config(..., true)`, local to the transaction).

```
CREATE POLICY tenant_isolation ON app.<table>
  USING (tenant_id = current_setting('app.current_tenant', true)::uuid)
  WITH CHECK (tenant_id = current_setting('app.current_tenant', true)::uuid);

CREATE POLICY owner_isolation ON private.<table>      -- conversations, messages, attachments,
  USING (tenant_id = current_setting('app.current_tenant', true)::uuid      -- wellbeing_profiles,
        AND user_id = current_setting('app.current_user', true)::uuid)      -- memory_prefs, memory_items, memory_events
  WITH CHECK (... the same ...);

REVOKE ALL ON SCHEMA private FROM hremia_app;
REVOKE ALL ON ALL TABLES IN SCHEMA private FROM hremia_app;

From apps/api/app/core/ddl.py: the idempotent schema, checked at every start and applied whenever it changes.
```

RESTRICTIVE policies

A RESTRICTIVE policy is ANDed with the others: it can only narrow what a query returns, never widen it.

Policy	Table	Rule
<code>companion_own_leave</code>	<code>leave_entitlements</code> , <code>leave_records</code> , <code>employment_records</code> , <code>leave_requests</code>	For the assistant's role: only rows of the asking employee

Policy	Table	Rule
companion_own_training	course_completions	For the assistant's role: only the asking employee's results
report_confidential_read, _update, _delete	reports	Read: the named reporter's own case, or full access (below). Change and delete: full access only
report_confidential_read, _insert, _update, _delete	report_messages	Full access; the reporter reads non-internal messages of their own case and may add only plain messages
report_confidential_*	report_minutes	Full access; the named reporter sees minutes once shared and may only confirm them or ask for a correction; only drafts can be deleted
report_confidential_read, _insert, _update, _delete	report_attachments	Handlers with full access see every file; the named in-app reporter sees their own case's files except those on internal notes; a reporter adds files only to their side of the thread. No DELETE grant; a trigger lets a stored file only be erased (content, name and hash removed), never rewritten or moved
report_confidential_read, _insert, _update	report_referrals, report_outcomes, report_minutes_versions	Handlers with full access only. The application role has no DELETE grant: a referral, a decision or an earlier text of the minutes goes only when the daily retention run erases the closed case's content (B7)
report_confidential_read	audit_log	Entries about a case follow the case
recusal_own_insert, recusal_lifted_by_another	report_recusals	Only one's own withdrawal can be recorded; only another handler with full access can lift it; no DELETE grant
report_handlers_managed_*	report_handlers	Only the officer in post (or, with none, a deputy) changes the handler set; before any designation, an HR administrator
report_handler_not_deleted	users	A designated handler's account cannot be deleted from under the set
sensitive_recipient_only	notifications	A sensitive notification is readable only by its recipient

The reports-officer rule

"Full access" to a case is decided in the database by `app.report_scope()` and `app.report_access()`: SECURITY DEFINER functions with a pinned `search_path`. A user has full access if they are an HR administrator or DPO of the company, have not withdrawn from the case, and either are an active designated handler or the company has designated nobody. For signed-in users the designation fails closed: once any designation exists, it stays in force whatever happens to a designee's role. HR's internal closing note and the officer's outcome note are not even selectable by the application role; handlers read them through functions that require full access. INSERT is deliberately not restricted, so that an anonymous reporter and the public channel can file a case. Transactions that must not carry a user (an anonymous report; filing from the public page; messages, evidence files and the confirmation of minutes from the tracking page; a report handed on by someone not competent to receive it) run without a signed-in user, and for them the two functions return full scope. There it is the API, not the database, that keeps the channel from reading cases back: it never uses INSERT ... RETURNING on these tables, and the tracking page reads only the case its reference and access code identify. APP

```
CREATE POLICY report_confidential_read ON app.reports AS RESTRICTIVE FOR SELECT TO hremia_app
USING (reporter_user_id = (SELECT nullif(current_setting('app.current_user', true), '')::uuid)
OR ((SELECT app.report_scope()) = 'all'
AND NOT EXISTS (SELECT 1 FROM app.report_recusals x
WHERE x.report_id = reports.id
AND x.user_id = (SELECT nullif(current_setting('app.current_user', true), '')::uuid)
AND x.revoked_at IS NULL)));
```

The case is visible to its named reporter, or to a handler with full access who has not withdrawn from it (κώλυμα).

B4 Encryption and key management

Layer	Mechanism
In transit	TLS from browsers to Cloudflare and from Cloudflare to the server, for hremia.eu and www.hremia.eu (B2); https required for AI endpoints configured for an organisation alone (B8); STARTTLS for e-mail.

Layer	Mechanism
Push notifications	End to end: aes128gcm content coding (RFC 8188) with keys derived from an ECDH exchange with the browser's subscription key (RFC 8291); sender identity by a VAPID token signed with ES256 (RFC 8292). A fresh key and salt for every message. TEST
At rest, in the application	AES-256-GCM with a random 96-bit nonce per value and a 128-bit authentication tag. APP
Keys	Envelope encryption: a 256-bit master key (KEK) wraps a data key per company. Each company has two: a chat key (<code>app.tenant_keys</code>) and a report key (<code>app.report_keys</code>), each wrapped with its own associated data, so neither unwraps as the other. Erasing conversations by destroying the chat key (crypto-shredding) never touches case files that must be kept, and replacing or destroying one key leaves the other untouched. Keys are not rotated automatically.
Binding to the record	Each encrypted report field is bound to its column and row (associated data <code>hremia-field:2 reports.body <id></code>); a case message also to its case and to whether it is an internal note; a Memory item to its owner. A value copied into another row or column, or left in place while the row around it changes, does not decrypt. TEST Conversation messages, attachments and the wellbeing profile use the chat key without this row binding; the database's <code>owner_isolation</code> policy keeps them with their owner.
Evidence files on reports	Sealed with the company's report key and bound to the file's id, its case, its message, whether that message is an internal note, and the SHA-256 of the cleaned file; the file name is sealed too. A file copied to another row or case, made visible to the reporter or given another hash does not decrypt. TEST
API keys of an organisation's own AI provider	Sealed with AES-256-GCM under a separate platform key, itself wrapped by the master key with its own associated data, and bound to the organisation and the endpoint; never returned by the API or written to the audit log, and sent only to the address they were entered for. TEST
Authenticity	Once a company's report text is fully encrypted, anything that is not current ciphertext is not returned as text: plaintext written straight into the database cannot pass itself off as a reporter's words.
Passwords, access codes	argon2id with a random salt; the access code cannot be recovered, only verified.
Session tokens, sign-in links	Only SHA-256 hashes are stored.

What is encrypted

Conversations: message content, attachments (file and extracted text), the wellbeing profile, Memory items. **Reports:** subject, text, the reporter's name and contact details where given, the questionnaire, messages, minutes, referral notes, recusal reasons, the reason for a legal hold, the closing message, the internal closing note, the outcome note, and evidence files with their file names. **Not encrypted at application level,** protected by the database permissions and row-level security of **B3**: the HR records (leave, including health-related leave kinds and certificate dates, employment records and HR's notes, requests and decisions), the directory, the organisation's documents and their search index, courses and quiz results, survey answers, announcements and notifications, the accounts (names, e-mail addresses, roles), conversation titles (the first 60 characters of the employee's first message), the file names of conversation attachments, the type and size of evidence files, and case metadata such as dates, categories, codes and deadlines, which the deadline tracking and the aggregates need.

Key custody, stated plainly

- The keys are HRemia's: the master key is held in the server's environment configuration, outside the database, and is included, in the same encrypted repository as the database dumps, in the off-site disaster-recovery backup so that the service can be rebuilt; that backup's protection therefore rests on the repository's passphrase. The keys are not customer-managed and are not held in a hardware security module (HSM).
- HRemia can therefore technically decrypt data. Through the application its staff see only aggregate numbers and the organisation's AI configuration, never content or keys; technical access is limited to the cases listed in the DPA (**A4** point 1), documented and notified where the law allows.
- The API process holds the master key and the passwords of all three database roles. The separate roles protect against a defect in the HR-side code; they do not protect against a compromise of the server itself.
- Encryption protects data at rest. To show a case to an authorised handler, or to answer an employee, the API decrypts in memory; for the assistant, the conversation is sent to the AI provider as described in **B8**.
- Encrypted is not anonymised: conversations and reports remain personal data and are treated as such.

B5 Anonymity by design

An anonymous report cannot hold the reporter's identity: not by policy, but because the database refuses the row.

```
ALTER TABLE app.reports ADD CONSTRAINT anonymity_invariant CHECK (
  (kind = 'anonymous' AND reporter_user_id IS NULL
   AND (reporter_access_hash IS NOT NULL OR source = 'officer')
   AND reporter_name IS NULL AND reporter_contact IS NULL)
 OR (kind = 'named' AND source = 'app' AND reporter_access_hash IS NULL
   AND (reporter_user_id IS NOT NULL OR reporter_detached_at IS NOT NULL))
 OR (kind = 'named' AND source = 'public' AND reporter_user_id IS NULL
   AND reporter_access_hash IS NOT NULL AND reporter_name IS NOT NULL AND reporter_contact IS NOT NULL)
 OR (kind = 'named' AND source = 'officer' AND reporter_user_id IS NULL AND reporter_name IS NOT NULL)
);
ALTER TABLE app.reports ADD CONSTRAINT reports_anonymous_no_department
  CHECK (kind <> 'anonymous' OR department_id IS NULL);
CREATE TRIGGER reports_keep_anonymous BEFORE UPDATE OF kind ON app.reports
  FOR EACH ROW EXECUTE FUNCTION app.keep_anonymous_reports_anonymous();
-- raises 'an anonymous report stays anonymous' when an anonymous report's kind would change
```

From `apps/api/app/core/ddl.py`. Source 'officer' is a report the Y.Π.Π.A./reports officer registers from a letter, e-mail, call or meeting: an anonymous one has an access code only if the officer handed one over; a named one carries the name given, never a user account. A named in-app report keeps its link to the reporter's account until that account is deleted; the link is then dropped and the time recorded (`reporter_detached_at`).

Control	Detail
Access code	12 characters from a 32-character alphabet without look-alikes (0/O, 1/I), about 60 bits, from a cryptographically secure generator. Shown once, with copy, save as .txt and print; stored only as an argon2id hash, so it cannot be recovered or re-sent. APP DB
Reference	HRM-XXXX-XXXX (8 characters, about 40 bits); typing is forgiving (case and dashes ignored); look-ups are rate-limited. TEST
No IP, no browser identifier	The database has no column for an IP address or user agent on reports. Our web server keeps no access log for hremia.eu and www.hremia.eu, and its error log records only critical faults; the traffic reaches it through Cloudflare, which processes the visitor's IP address in transit for protection against attacks and for routing (A4 point 8). The rate limiter keeps the visitor's IP address only as the key of a counter that expires after at most 10 minutes; it is not linked to a report or an account, and the cache is not backed up. APP
Audit without identity	An anonymous report is logged with actor type “anonymous” and no user; a public-page report as “system”; metadata only. APP
No account on the public page	Nothing to sign in to. An unsent draft stays only in the browser tab's session storage and disappears when the report is sent or the tab is closed; the privacy notice must be acknowledged before sending. APP TEST
Evidence files	A reporter can attach up to 5 files to each message, 10 MB each (PDF, JPEG, PNG, DOCX, XLSX, TXT). Before anything is stored, what can identify their author is removed: photos are re-encoded from their pixels, so GPS position, camera and date data (EXIF, XMP, IPTC) do not survive; PDFs are rebuilt without document information, XMP, earlier revisions, scripts or embedded files; Word and Excel files lose author, company, last-modified-by and the names on comments and tracked changes. Executables, macro-enabled and password-protected files are refused. Content and file name are encrypted with the company's report key (B4). The uploader is recorded only as “reporter” or “handler”: the table has no column for the user who uploaded, and an anonymous upload keeps no identity, even from a signed-in browser. APP DB TEST
No department	Department labels can identify people in small teams, so an anonymous report cannot carry one (CHECK above). DB TEST
Anonymous stays anonymous	No function of the application changes a report's kind or adds a reporter to an existing case APP , and the database refuses it: the trigger <code>reports_keep_anonymous</code> rejects any update that would change an anonymous report's kind, whichever database role issues it, the owner included, as long as the trigger is in place: the superuser could disable it, as it can bypass grants and row-level security (B3). DB TEST

Control	Detail
Content can still identify	Details such as dates, places or who was present, or the language a report was written in (which is stored with it), can let someone work out who wrote it. The form and the assistant say so, so the reporter decides what to include.
Notifications	Lock screens and e-mails say only that there is an update; escalation e-mails carry only the reference. APP
Small groups	Insights, surveys, breaks and the compliance centre's breakdowns hide groups below the company's threshold (at least 5). APP TEST
Surveys	No user identifier and no timestamp on answers; a separate table records who answered, not what. DB Answers are thus separated from identity; they are not anonymised against someone with direct access to the platform's database.
Breaks	Per-person minutes only in the cache, for 2 days; the database holds daily totals per company and game; days with fewer than five people are left out. DB TEST

B6 Audit and logging

- **Append-only for the application.** `app.audit_log` can be written but not changed or deleted by the application: its role has INSERT and SELECT, and UPDATE and DELETE are revoked. The assistant's role can only INSERT. The PostgreSQL superuser (owner) is not bound by these grants; it is used by the server's start-up and background tasks, by sign-in and platform administration, for the narrow server-side steps listed in B3, and by HRemia's operator. One of those background tasks is the daily retention run: it deletes entries older than the audit-trail period the organisation sets (6 to 120 months; by default the general retention period), keeps every entry about a case whose content is still kept, and records each run as one `retention.run` entry with counts only. **DB** **TEST**
- **Metadata only.** Entries record who did what, when, on which object, with flags such as "reason given" or "pseudonymised", never message or report content. The reason for an escalation is stored as an encrypted internal note on the case, not in the log. **APP**
- **Scoped.** The log is isolated per company; entries about a case are visible only to handlers with full access to it. The compliance page shows counts per action through a function that returns numbers, not rows. **DB**
- **AI usage.** Each assistant reply records the employee, the conversation, the model, the tokens and the latency in `app.ai_usage`, for governance and cost, with no content. The application role can read these rows; the application shows HR and the DPO totals only **APP**. A background Memory update is recorded with the day only, without the employee or the conversation, so that the figures do not show who has Memory switched on. In addition, `app.ai_processing_log` counts every AI call made for an organisation, per day, against the endpoint (name, region, host) and the model that served it, with failures counted separately; it holds no content, no person and no time of day, only the server writes it, and the organisation's HR administrators and DPO read their own rows on the Compliance page. **APP** **TEST**
- **Memory activity.** Switching Memory on or off, edits, deletions and automatic updates are recorded, as counts and flags without content, in the employee's own Memory log in the private schema (the latest 100 entries), not in the audit log that HR can reach; the employee receives it in their data export. **DB**

Examples of recorded events

<code>report.created</code>	Actor "anonymous", "system" (public page) or the named user; channel, category
<code>report.assigned</code> , <code>report.escalated</code>	Who, to whom; whether a reason was given; how many were notified
<code>report.exported</code>	Whether pseudonymised, whether internal notes were included, format
Inbox listings	That a user listed cases, with the count only
<code>report_handlers.updated</code> ; eligibility declared or withdrawn	The designation history used by the evidence pack
<code>compliance.whistleblowing_attested</code> , <code>compliance.evidence_generated</code>	Statements and evidence packs, with date and author
<code>companion.message</code> , <code>companion.attachment</code>	Metadata only: language and token count; the kind of file. The employee's Memory settings, edits and deletions are recorded in their own private log, not here

Examples of recorded events

<code>company.retention_updated</code> , <code>retention.run</code>	The retention periods and who changed them; each daily run with its counts and the periods applied, without identifiers or text
<code>report.attachments_added</code> , <code>report.attachment_downloaded</code> , <code>report.attachment_erased</code>	Who (or “anonymous”) and how many files; never file names
<code>report.redacted</code> , <code>report.erased</code>	How many passages were removed, never the removed text; a case's content erased at the end of its retention period
<code>report.retention_set</code> , <code>report.legal_hold_set</code> , <code>report.legal_hold_lifted</code>	A case's retention decision; a legal hold placed or lifted (its reason is kept as an encrypted internal note on the case)
<code>report.concerns_handler_flagged</code> , <code>report.concerns_handler_removed</code> , <code>report.recused</code>	A report marked as concerning the officer, the officer's automatic withdrawal, a mark removed by a deputy with a reason
<code>admin.tenant_ai_updated</code> , <code>admin.tenant_ai_viewed</code> , <code>admin.tenant_ai_tested</code>	Changes to, views and tests of an organisation's AI-provider configuration by the platform administrator; never the keys

Deadline monitoring: a background job warns the assigned handler, or the designated handlers, 24 hours before an acknowledgement falls due and 3 days before feedback falls due; HR and the officer are warned 30 days before the officer's term ends. Escalation shortens the time to act to 48 hours and 30 days and moves the case to an independent handler: the officer or the next deputy, or the DPO where no one is designated. [APP](#) [TEST](#)

B7 Backup, retention and deletion

Data	Kept	How it goes
Conversations and their attachments	The organisation's period for conversations (6 to 120 months; by default the general period, 24 months), counted from each conversation's last message or attachment	Deleted automatically by the daily run, with their messages and attachments; an attachment never sent in a conversation goes after the same period; all are deleted with the employee's account. Company-wide, on instruction: crypto-shredding by HRemia, destroying the chat key (the key stays in the backups until their cycle ends)
Wellbeing profile	While the account exists	The employee changes it at any time; deleted with the account
Memory	Until the employee deletes it; a note not created or changed within the conversations period is deleted automatically, and so is the employee's older Memory activity	The employee edits, deletes or clears the notes at any time; switching Memory off keeps them until the employee deletes them or they reach the end of the period; deleted with the account
Case files, minutes, referrals, evidence files	Open cases: always. Closed cases: the organisation's period for closed reports (12 to 120 months from closing; by default the general period), or the date the handlers set for the case, or until the proceedings it started are over (Greece: for a reasonable and necessary period, in any case until any investigation or proceedings end)	At the end of the organisation's period the daily run erases the content and keeps the entry in the special file, marked erased; a case on legal hold is kept. A date the handlers record for a case is applied the day after it, except while the case is on legal hold. A case kept until the proceedings are over is not erased. A handler erases a passage or file that is unrelated or excessive at any time. A case file cannot be deleted from the application; own key, so erasing conversations never affects it
Leave, employment record, training	Until HR deletes them or the person's account is deleted	HR corrects and deletes records; deleting an account deletes the person's records. Not part of the daily run
Break minutes per person	2 days, in the cache	Expire automatically
Rate-limit counters (client IP)	At most 10 minutes, in the cache	Expire automatically
Sign-in links; sessions	20 minutes, single use; 7 days	Expire automatically

Data	Kept	How it goes
Audit log	The organisation's period for the audit trail (6 to 120 months; by default the general period); entries about a case whose content is kept stay with the case	Deleted automatically by the daily run, which records itself with counts only
Backups	Daily; kept up to about 6 months	Expire with the backup cycle

Each night the database is dumped on the server and copied, with the deployment files and the master key needed to rebuild the service, into an encrypted repository (BorgBackup) off the server, on Hetzner storage in the EU. Restores from the off-site copy were tested in July and August 2026. The cache is not backed up. Data deleted from the live system remains in backups until their cycle ends. The daily run starts from 03:00 in each company's time zone, once a day, one company at a time. HR administrators and the DPO set the periods in Settings › Retention and automatic deletion and can preview, as counts only, what the next run would delete; the organisation's periods cannot be set below the minimums in the table; a date the handlers record for a single case is applied as recorded, except under a legal hold. [APP](#) [TEST](#)

B8 AI processing

What each AI function sends to the provider, what it never sends, and the checks around it.

Function	Sent to the AI provider	Never sent	Checks
Assistant	System instructions (with the date and how the platform works); the relevant excerpts of the organisation's documents; the employee's own leave record, including health-related leave kinds and whether a certificate was received (never a reason; HR's notes only on other kinds of leave), their leave requests and decisions (including HR's decision note), their employment record as HR filed it (date of appointment, post, contract type and end date, category, grade and pay scale, probation and tenure dates, recognised prior service, HR's note), the HR directory and their course list; the Memory notes if switched on; up to the last 24 messages of the conversation, the current one included; attachments (the document's text, pictures, and up to five pages of a PDF rendered as images)	The employee's name and e-mail (not added by the platform; the employee may still write them); the wellbeing profile; other employees' data, apart from the HR directory's contacts; reports; surveys; breaks	Citation guard; legal-assurance filter; script check; no diagnosis; no employment decisions; no inference of emotions from a face or photo (the rule is repeated next to every image); an AI notice at the start of every conversation; states it is an AI and reminds the employee of it in sensitive contexts; machine-readable marking of the reply; says when it cannot see an earlier conversation
Memory update (opt-in)	After each completed reply (never in the AI Coach): the employee's latest message (up to 4,000 characters), the assistant's previous reply as context (up to 1,500 characters) and the current notes, to update the short list of facts the employee stated	The same exclusions	The model returns only additions, changes and removals; any other reply changes nothing. Forbidden to hold judgements about emotions, health, personality or reliability, plans to resign, sue or report the employer, or names of other people; a check in the code drops notes naming a special category (health, sick or maternity leave, religion, union membership, sexual orientation, convictions...), unless the employee explicitly instructs that one fact to be kept, and notes describing feelings or such plans TEST ; at most 25 notes of 200 characters; runs on the organisation's AI chain
AI Coach	Excerpts of the course material and the conversation	Personal records; Memory	Stays within the course material; article numbers still checked
Quiz drafting (HR)	Passages of the chosen policy	Personal data	Each correct answer must be backed by a verbatim quotation; a second check sees only the source passage; only questions HR publishes reach employees

Function	Sent to the AI provider	Never sent	Checks
Translation	The text of an announcement or quiz question	Personal data	A second pass compares meaning, names, dates and numbers; a failed translation is not stored and the original is shown

Never sent to an AI provider Π-21

Reports and case files, their evidence files, minutes, referrals, surveys, break data and the wellbeing profile. The code paths for reports, surveys and breaks make no AI call; for case files and the evidence pack an automated test fails if their code uses an AI module TEST.

Providers and terms Π-10

Answers come from general-purpose models of established providers such as OpenAI, Anthropic and Google, or from a provider or model the organisation chooses by agreement (below). Under the DPA, the providers used for an organisation are named in its sub-processor list with their data processing agreement and retention period, and are used on paid business terms under which they do not use the data to train their models and keep it only for a limited period. An organisation's data goes only to the chain that applies to it: HRemia's chain or, where one is configured, the organisation's own (below). A chain is a primary model and one or more fallbacks; a fallback is tried, in order, only when the one before fails before answering (a usage limit, an error, no response or an empty answer); a lighter model of the primary provider handles short tasks such as Memory updates. Every AI call made for an organisation is counted, per day, against the endpoint and model that served it (B6). HRemia does not train or fine-tune models, and does not use customer data to evaluate them; models are chosen after comparative evaluation on Greek legal texts. APP TEST

The organisation's own provider or model

By agreement, and after a comparative evaluation on scenarios the organisation defines, an organisation can use a provider or model of its own choice, for example under its own contract and in a region it chooses. HRemia's platform administrator configures it for that organisation alone, with up to five endpoints in order (name, https address, model, lighter model, region, reference of the data processing agreement); the organisation's HR cannot change it. From then on every AI call made for the organisation (the assistant, the AI coach, Memory updates, quiz drafting and translation, including background tasks) goes to that chain, in order; HRemia's own providers follow it only where the organisation asks for them as a fallback, which is off by default. The API keys are stored encrypted (B4), are never shown again and are sent only to the address they were entered for. The organisation's HR administrators and DPO see on the Compliance page which chain serves the organisation and, per day, which endpoint received its data and how many calls failed. APP TEST

Checks on the output Π-8

- **Citation guard.** Documents are indexed article by article. The model may not state an article or section number that does not appear in the excerpts it was given, or that it cited earlier in the same conversation after the same check. The check runs on the stream, so an unverifiable number never reaches the screen. Cross-references inside a quoted article are allowed, because they are in the source. Article words are recognised in all ten languages. APP TEST
- **Legal assurances** such as "there is no obligation" or "nobody can force you" are removed unless the sources support them (Greek and English). TEST
- **Script check.** A reply that mixes writing systems inside a word is detected and logged. TEST
- **Personal records** are stated as recorded; the model is told not to calculate entitlements, and to refer to HR what is not on file. TEST
- **Sources shown.** The employee sees which document and article an answer used.

Memory Π-12

Off until the employee switches it on, on the "What your assistant remembers" screen, reached from their account and from the conversation; only an employee can switch it on. The list holds at most 25 short notes of facts the employee stated (their role or shift, an ongoing situation, how they like to be addressed, what they decided to do), each encrypted and bound to its owner, in the private schema with the same protections as conversations. After each completed reply a lighter model proposes changes in the background; the reply never waits for it, and an update is discarded if the employee changed their notes after sending the message, so a deleted note is never written back. The employee can read, edit and delete every note, delete all of them or switch Memory off at any time, and sees which notes an automatic update wrote or changed; notes the update wrote carry a visible "AI" label. A person whose role changes keeps these rights over their notes. When Memory is off, the assistant is told so and never promises to remember. A note not created or changed within the conversation retention period is deleted automatically (B7). DB APP TEST

B9 Controls mapped to ISO/IEC 27001:2022, Annex A

HRemia is not certified to ISO/IEC 27001. The mapping helps your IT team place our controls within your own framework and supplier assessment.

Annex A control	How the platform addresses it	Section
Organisational controls		
5.15 Access control; 5.18 Access rights	Roles in the application; row-level security; officer designation changed only by the officer, failing closed	B3
5.16 Identity management; 5.17 Authentication information	One account per e-mail address; accounts created for an organisation have no password and sign in with one-time e-mail links (argon2id passwords only for accounts HRemia itself creates with one, such as its platform administrator's); only hashes of session tokens and sign-in links are stored; no second authentication factor is used	B3, B4
5.19–5.22 Supplier relationships; 5.23 Cloud services	Sub-processor list (hosting, AI providers, Cloudflare, browser push services), data processing agreements, business terms for AI providers, advance notice of changes	A4
5.24–5.28 Incident management	Breach notification to the organisation without undue delay under the DPA (GDPR art. 33(2)); audit trail for investigation	A4, B6
5.33 Protection of records	Append-only audit log for the application; special file, whose entries remain after a case's content is erased at the end of retention; legal hold; case files not deletable from the application	B6, B7
5.34 Privacy and protection of PII	Data protection by design; minimisation fact by fact; DPIA support	A4
People controls		
6.6 Confidentiality agreements	Confidentiality of HRemia's staff under the DPA (art. 28(3)(b))	A4
Physical controls		
7.1–7.14	Provided by the data-centre operator (Hetzner, Falkenstein); the server is used only by HRemia's operator but also runs its other web and e-mail services	B2
Technological controls		
8.2 Privileged access rights	The owner database role (a PostgreSQL superuser) is used in the code for start-up, sign-in, platform administration (including an organisation's AI-provider configuration and its sealed keys), the look-ups without a signed-in user (public page, tracking), background jobs (reminders, notifications, retention deletion) and the narrow server-side steps named in B3; platform staff see aggregates and each organisation's AI configuration (never the keys) in the application; the server's administrators (HRemia's operator) have full access to the host, its configuration and the backups	B3
8.3 Information access restriction	RESTRICTIVE policies; zero grants on the private schema	B3
8.5 Secure authentication	One-time e-mail links (the factor is control of the user's mailbox), argon2id, HttpOnly Secure cookies, rate-limited sign-in keyed on an address the client cannot choose; no second authentication factor	B2, B3
8.10 Information deletion	Retention periods set by the organisation per category (conversations and Memory, closed cases counted from closing, the audit trail), with a daily automatic deletion run; legal hold on a case; removal of unrelated or excessive data from a case by its handlers; crypto-shredding	B7
8.11 Data masking	Pseudonymised case export (the reporter, and the third parties the officer selects); identifying metadata stripped from evidence files; groups below 5 hidden	A2, B5
8.12 Data leakage prevention	Notifications without content; reference-only e-mails; no content in logs	B5, B6
8.13 Information backup	Encrypted daily off-site backups in the EU; restores tested	B7

Annex A control	How the platform addresses it	Section
8.15 Logging	Audit log, append-only for the application, metadata only; AI processing log per organisation and day; size-limited container logs; no access log on the web server	B6
8.20–8.21 Network security	hremia.eu and www.hremia.eu behind Cloudflare's network for protection against denial-of-service attacks, with TLS on both legs and the visitor address accepted only from Cloudflare's published ranges; database and cache only on HRemia's own internal container network, apart from the host's other services; https required for AI endpoints configured for an organisation alone	B2, A4
8.24 Use of cryptography	AES-256-GCM with envelope keys held by HRemia (no customer-managed keys or HSM, no automated key rotation); RFC 8291 push encryption	B4
8.25, 8.29 Secure development, security testing	More than 500 automated test cases, including database-level tests of the access rules	B10
8.28 Secure coding	Parameterised SQL; validated inputs; SECURITY DEFINER functions with a pinned search_path	B3

The mapping covers the Annex A controls only; HRemia does not run an information-security management system under clauses 4–10 of ISO/IEC 27001. Sign-in uses no second authentication factor, and the keys are held by HRemia (B3, B4).

B10 Evidence: the automated tests

The platform's automated tests number more than 500 test cases, from about 400 test functions (count on the release code, 28 September 2026). The tests marked DB run against PostgreSQL with the production schema applied, and check the rules in the database itself, not only through the API.

Code	Guarantee	Tests (file: test names, as in apps/api/tests)	Level
Π-1	HR cannot read conversations	<code>test_security_regressions.py: test_app_role_cannot_read_private_messages</code> , <code>test_app_role_has_no_grant_anywhere_in_the_private_schema</code> · <code>test_companion_memory.py: test_colleagues_hr_and_the_app_role_cannot_reach_the_notes</code>	DB
Π-2	Anonymous reports hold no identity and never become named; evidence files without identifying metadata	<code>test_public_reporting.py: test_an_anonymous_report_keeps_nothing_that_points_at_a_person</code> , <code>test_the_database_itself_refuses_an_anonymous_report_with_a_name</code> , <code>test_an_anonymous_report_can_never_be_relabelled_named</code> · <code>test_whistleblowing_law.py: test_the_database_keeps_the_anonymity_invariant_for_the_officers_register</code> · <code>test_security_regressions.py: test_anonymous_report_strips_department_metadata</code> · <code>test_report_attachments.py: test_photos_and_pdfs_lose_gps_exif_xmp_and_authors_before_they_are_stored</code> , <code>test_word_and_excel_files_lose_author_company_and_last_modified_by</code> , <code>test_an_anonymous_upload_keeps_no_identity_even_from_a_signed_in_browser</code>	DB
Π-3	Encryption, separate keys, record binding	<code>test_report_confidentiality.py: test_report_text_is_ciphertext_at_rest_and_plaintext_through_the_api</code> , <code>test_a_note_moved_or_made_visible_in_the_database_does_not_read</code> , <code>test_report_text_does_not_depend_on_the_chat_key</code> , <code>test_a_company_without_a_key_gets_one_that_is_stored_before_anything_is_sealed</code> · <code>test_companion_memory.py: test_enabled_memory_is_encrypted_and_reaches_only_its_owner</code> · <code>test_report_attachments.py: test_content_and_name_are_sealed_at_rest_and_do_not_open_elsewhere</code> · <code>test_tenant_ai_chain.py: test_keys_never_come_back_and_are_sealed_at_rest</code> , <code>test_a_sealed_key_does_not_open_for_another_company_or_endpoint</code>	DB
Π-4	Per-company and per-employee isolation	<code>test_companion_training_access.py: test_the_companion_never_sees_a_colleagues_results</code> · <code>test_security_regressions.py: test_named_report_rejects_cross_tenant_department</code> , <code>test_cross_tenant_duplicate_email_is_rejected</code> . The leave policy <code>companion_own_leave</code> follows the same pattern (code review, <code>ddl.py</code>)	DB
Π-6	Deadlines and escalation	<code>test_report_confidentiality.py: test_three_calendar_months_not_ninety_days</code> , <code>test_designation_releases_cases_held_by_others_and_deadline_warnings_follow_the_handlers</code> · <code>test_escalation.py: test_escalating_requires_a_reason</code> , <code>test_the_acknowledgement_clock_only_ever_tightens</code> , <code>test_the_feedback_clock_only_ever_tightens</code>	APP
Π-7	Audit	<code>test_report_confidentiality.py: test_every_inbox_listing_is_audited_with_its_count_only</code> , <code>test_the_audit_trail_and_notifications_follow_the_case_in_the_database</code> . Append-only grant: code review (<code>ddl.py</code>) · <code>test_retention.py: test_audit_trail_follows_its_period_but_a_cases_trail_stays_with_the_case</code>	DB

Code	Guarantee	Tests (file: test names, as in apps/api/tests)	Level
Π-8	Citation guard	<code>test_citation_safety.py</code> (38 test functions, 88 cases), e.g. <code>test_only_numbers_present_in_the_sources_may_be_stated</code> , <code>test_nothing_unverifiable_reaches_the_stream_at_any_token_size</code> , <code>test_legal_assurances_are_dropped</code> · <code>test_rag_cited_sources.py</code> (21 tests)	APP
Π-9	AI Act safeguards and transparency (arts 5, 50)	<code>test_ai_provenance.py</code> : <code>test_the_companion_stream_and_its_stored_reply_are_marked</code> , <code>test_the_coach_stream_is_marked</code> , <code>test_the_header_follows_the_body</code> , <code>test_the_text_itself_is_never_altered</code> , <code>test_memory_notes_are_marked_by_who_wrote_them</code> , <code>test_the_data_export_points_at_its_ai_segments</code> , <code>test_the_manifest_describes_the_scheme</code> · <code>test_whistleblowing_units.py</code> : <code>test_the_companion_never_reads_emotions_from_a_face</code> , <code>test_memory_holds_back_feelings_and_plans_against_the_employer</code> · <code>test_companion_memory.py</code> : <code>test_the_update_prompt_names_every_special_category_and_the_narrow_exception</code> , <code>test_special_category_notes_are_held_back_unless_explicitly_asked</code> · <code>test_directory_and_requests.py</code> : <code>test_the_companion_is_told_it_cannot_file_anything</code> . The notice at the start of every conversation, the permanent notice and the rule to say and remind that it is an AI: code review (<code>prompts.py</code> , <code>Companion.tsx</code>)	APP
Π-10	Each organisation's AI configuration only; calls logged by provider and model	<code>test_tenant_ai_chain.py</code> : <code>test_the_company_chain_serves_that_company_only</code> , <code>test_the_auth_dependency_sets_the_company_and_background_tasks_name_theirs</code> , <code>test_memory_updates_run_on_the_company_chain</code> , <code>test_without_the_fallback_flag_the_platform_never_sees_the_data</code> , <code>test_a_stored_key_only_goes_to_the_address_it_was_entered_for</code> , <code>test_the_processing_log_names_the_provider_and_each_company_sees_its_own</code> . Provider terms: sub-processor list	APP
Π-11	Groups of 5+; break totals	<code>test_break_rules.py</code> : <code>test_summary_drops_days_under_five_people</code> · <code>test_whistleblowing_law.py</code> : <code>test_the_compliance_centre_follows_the_companys_law_and_shows_aggregates_only</code>	APP
Π-12	Opt-in Memory	<code>test_companion_memory.py</code> : <code>test_memory_is_off_by_default</code> , <code>test_edit_delete_switch_off_and_forget</code> , <code>test_a_note_deleted_during_an_update_is_not_written_back</code> , <code>test_tutor_mode_never_reads_or_updates_memory</code> , <code>test_a_changed_role_keeps_the_right_to_see_correct_and_erase</code> , <code>test_deleting_the_account_erases_the_persons_private_data</code> , <code>test_the_update_is_metered_without_naming_the_employee</code> , <code>test_an_automatic_change_is_shown_as_new_until_seen</code> , <code>test_the_companion_is_always_told_the_memory_state</code> · <code>test_retention.py</code> : <code>test_chats_and_memory_go_only_past_the_chat_period</code>	DB
Π-13	Officer's exclusive access, κώλυμα	<code>test_report_confidentiality.py</code> : <code>test_designating_handlers_closes_cases_to_other_hr_in_the_database_itself</code> , <code>test_only_the_officer_changes_the_set_even_straight_at_the_database</code> , <code>test_designation_fails_closed_when_the_officer_is_demoted</code> , <code>test_a_handler_who_withdraws_loses_that_case_only</code> , <code>test_a_withdrawal_is_kept_and_only_another_handler_can_lift_it</code> , <code>test_a_reporter_who_is_hr_sees_their_case_only_as_its_reporter</code>	DB
Π-14	Encrypted push	<code>test_webpush.py</code> : <code>test_browser_can_decrypt_what_we_send</code> , <code>test_every_message_uses_a_fresh_key_and_salt</code> , <code>test_vapid_header_verifies_with_the_public_key</code> , <code>test_only_real_push_services_are_accepted</code>	APP
Π-15	Public page, codes	<code>test_public_reporting.py</code> : <code>test_a_named_public_report_carries_name_and_contact_and_is_followed_with_codes</code> , <code>test_the_privacy_notice_must_be_acknowledged</code> , <code>test_a_bot_filling_the_honeypot_gets_a_convincing_nothing</code> , <code>test_one_address_cannot_flood_the_inbox</code> · <code>test_ratelimit_ip.py</code> : <code>test_the_address_nginx_sets_wins_over_anything_the_client_sent</code> , <code>test_a_forged_forwarded_for_entry_is_ignored</code> · <code>test_report_reference.py</code> (5 test functions, 10 cases)	APP
Π-16	Law by country	<code>test_whistleblowing_law.py</code> : <code>test_a_company_outside_greece_is_checked_against_the_directive</code> , <code>test_the_compliance_centre_follows_the_companys_law_and_shows_aggregates_only</code> · <code>test_public_reporting.py</code> : <code>test_tracking_names_the_reports_own_company_country</code> · <code>test_whistleblowing_review.py</code> : <code>test_under_the_directive_a_report_about_the_officer_is_handled_by_the_others</code> , <code>test_the_legal_clocks_follow_the_law_and_the_acknowledgement</code>	APP
Π-17	Special file, minutes, acknowledgement, removal of excessive data	<code>test_whistleblowing_law.py</code> : <code>test_the_officer_registers_a_letter_and_the_clocks_run_from_its_receipt</code> , <code>test_minutes_are_checked_corrected_and_confirmed_by_the_reporter</code> , <code>test_a_named_in_app_reporter_sees_only_shared_minutes_even_straight_at_the_database</code> , <code>test_acknowledgement_and_feedback_are_provable_acts</code> · <code>test_whistleblowing_review.py</code> : <code>test_excess_data_is_erased_and_a_case_is_kept_only_as_long_as_decided</code> · <code>test_report_attachments.py</code> : <code>test_the_officer_attaches_the_enclosures_of_a_report_they_registered</code> , <code>test_a_handler_erases_an_excessive_file_and_retention_erases_them_all</code>	DB
Π-18	Outcome, referrals, pseudonymisation, report about the officer	<code>test_whistleblowing_law.py</code> : <code>test_closing_needs_the_outcome_and_an_archived_case_can_be_reopened</code> , <code>test_referrals_notices_and_a_pseudonymised_case_file</code> , <code>test_a_report_about_the_officer_is_only_registered_and_forwarded_to_the_ead</code> , <code>test_pseudonymisation_finds_the_name_with_or_without_accents_and_leaves_amounts_alone</code> · <code>test_whistleblowing_review.py</code> : <code>test_pseudonymised_export_covers_inflections_referral_details_and_chosen_third_parties</code> , <code>test_a_deputy_removes_a_mistaken_mark_with_a_reason_and_the_reporter_is_told</code> · <code>test_report_attachments.py</code> : <code>test_the_exported_case_file_lists_names_and_hashes_never_content</code>	APP

Code	Guarantee	Tests (file: test names, as in apps/api/tests)	Level
Π-19	Term, eligibility, compliance centre	<code>test_whistleblowing_law.py: test_the_officers_term_is_at_least_a_year_in_greece_and_hr_is_warned_before_it_ends, test_each_designee_declares_their_own_eligibility, test_the_compliance_centre_follows_the_companys_law_and_shows_aggregates_only</code>	APP
Π-20	Aggregate compliance figures	<code>test_whistleblowing_law.py: test_the_compliance_centre_follows_the_companys_law_and_shows_aggregates_only</code>	APP
—	Retention, automatic deletion, legal hold	<code>test_retention.py: test_chats_and_memory_go_only_past_the_chat_period, test_closed_cases_past_the_period_lose_their_content_held_and_open_ones_never, test_audit_trail_follows_its_period_but_a_cases_trail_stays_with_the_case, test_handlers_set_and_lift_the_legal_hold_with_a_reason_and_it_stops_deletion</code>	APP
Π-5, Π-21	EU hosting; no AI call for reports, surveys or breaks	Architecture and configuration: B1, B2. No model in case files or the evidence pack: <code>test_ai_provenance.py: test_no_model_takes_part_in_case_files_or_the_evidence_pack</code> ; the survey and break modules contain no call to an AI provider (code review). No visitor access log, and the visitor address accepted from Cloudflare only on connections from its published ranges: web-server configuration (B2)	—

Your IT team can see these tests run, or review them with us. Where a guarantee rests on configuration or on code review rather than a test, the table says so.

PART C

Questions

The ten questions legal departments ask most often, answered for any organisation, each with a pointer to the section that proves the answer; then the design boundaries a reviewer should know, and what remains the organisation's own obligation.

C1 Questions legal departments ask

C2 Design boundaries and the organisation's part

C1 Questions legal departments ask

Answers written for any organisation. Each ends with the sections that prove it. New questions are added at the end, and the numbering is kept stable.

1 Why does the Greek material cite only N. 4990/2022?

The Directive sets minimum rules (art. 25); the employer's actual obligations come from the national transposition. In Greece that is N. 4990/2022, as in force, with KYA 47312/2023 on the internal procedure. Greek-market material therefore cites the Greek law, and Greek law appears only there and on the pages of companies established in Greece; material in other languages cites the Directive.

The same rule runs inside the platform: each company records its country, and its public page shows the Greek framework and the E.A.D. as external channel for a Greek company, or the Directive and the competent authorities of the company's country otherwise. Other texts also apply: the GDPR with v. 4624/2019, v. 4808/2021 for harassment, and the AI Act with v. 5321/2026, which also repealed the AI provisions of v. 4961/2022.

Proof: [A1](#) · [A2](#) · [A3](#)

2 Has national law been taken into account for markets outside Greece?

Yes, in two layers. A **common European core** applies everywhere: the Directive's requirements for the internal channel, the GDPR and the AI Act, with deadlines computed for each case that are never later than those of the Directive or, in Greece, of N. 4990/2022 (7 working days to acknowledge; feedback within 3 months of the acknowledgement). A **national layer** follows the company's country: the legal texts shown and the competent external authority. Before each new market, local counsel reviews retention periods, anonymous-report rules, the authority, duties towards worker representatives and the language of legal documents, and the result is recorded in a country annex.

The platform does not build any country's labour law into its answers: HR records entitlements and the assistant states them without calculating; for legal questions it relies on the documents the organisation uploads, and a check removes references to articles those

documents do not contain. The oral channel, where offered, and meetings on request are organised by the organisation; the officer records them in the same special file.

Proof: [A1](#) · [A3](#) · [A6](#)

3 Which contract? Who is the controller and who is the processor?

A service agreement with a data processing agreement under art. 28(3) GDPR as an integral part, based on the standard contractual clauses of Implementing Decision (EU) 2021/915, with annexes on the processing (including art. 9 and 10 data), the technical and organisational measures, the sub-processors, the reporting channel, the AI functions, the retention programme and, where relevant, a country annex.

The **organisation is the controller** of all data processed on its behalf, including employees' private conversations, even though it cannot read them: being controller does not require access to the data (CJEU C-210/16; C-25/17). For reports, Greek law says so expressly (N. 4990/2022 art. 15 §3). **HRemia is the processor**; it is a controller only for its own customer-relationship data, its website contact form and its infrastructure's security records. The DPA forbids using the organisation's data for HRemia's own purposes, such as training or evaluating models.

Proof: [A4](#)

4 Which special-category data (art. 9 GDPR) is processed, and on what basis?

Leave: kind and dates, certificate received yes/no; no diagnosis field and no free-text note on health-related periods; basis in the employer's labour and social-security obligations (art. 9(2)(b); in Greece art. 27 §3 v. 4624/2019). **Reports:** may contain health, sex life, trade-union membership or alleged offences; our assessment is art. 9(2)(g) with the Directive and the national law, 9(2)(f), and 9(2)(b) with v. 4808/2021 for harassment. **Assistant and Memory:** the employee may raise such matters, the assistant also receives their own health-related leave data, and Memory, if the employee switches it on, keeps what they stated; the organisation decides the basis, and explicit consent fits most clearly, with the employment caveats. **Surveys:** only if the organisation asks such a question; aggregated.

The organisation chooses and documents the basis; HRemia provides a table of bases, an employee-information template and, if consent is chosen, a consent template.

Proof: [A4](#)

5 Is data anonymised, or only encrypted? Can HRemia see it?

Encrypted, not anonymised. It is personal data and is treated as such. Conversation messages, attachments, the wellbeing profile, Memory, the content of reports and their evidence files are encrypted with AES-256-GCM under keys per company, with separate keys for conversations and reports; report fields and files are bound to their record. Conversation titles, which are the first 60 characters of the employee's first message, and the file names of conversation attachments are protected by the database permissions and row-level security instead ([B4](#)).

Inside the organisation, HR, managers and administrators cannot read conversations, Memory or wellbeing profiles: the database role behind the HR screens has no grant on the schema that holds them, and row-level security confines each employee to their own data. From the moment the Y.Π.Π.A./reports officer and deputies are designated, only they can read case content, enforced by the database, and a handler with a conflict of interest withdraws from a case. Anonymous reports store no account, name, contact details, department or IP address. Our web server keeps no access log, and its error log records only critical faults; traffic passes through Cloudflare's network, which processes the IP address for protection against attacks, and the address is kept only for rate limiting, for at most 10 minutes, with no link to a report or an account.

Technically, HRemia can decrypt, because it runs the infrastructure and holds the keys on its EU server. Through the application its staff see only aggregate numbers and the organisation's AI configuration, never content or keys. HRemia has no legal basis of its own to access content; as processor it acts only on instructions, and the DPA lists the cases of technical access (support on the organisation's written request, a security incident, a legal obligation), each documented and notified where the law allows.

Proof: [B4](#) · [B3](#) · [B5](#) · [B2](#)

6 Which sub-processors are used, and where are the servers?

All platform data, database, reports, conversations and files, is stored with Hetzner Online GmbH in Falkenstein, Germany; encrypted backups also stay in the EU with Hetzner; document search runs on our own server. Answers of the AI functions come from established providers named for each organisation in the sub-processor list, with their processing agreement and retention period; under the DPA they are used on business terms, without training on the data and with limited retention. By agreement, the organisation can instead use a provider of its own choice, configured for it alone ([B8](#)). Where a provider processes outside the EEA, a Chapter V safeguard applies. Browser push services receive only end-to-end encrypted content. The addresses hremia.eu and www.hremia.eu are served through the network of Cloudflare, Inc. (USA), for DNS, protection against denial-of-service attacks and routing: Cloudflare processes the visitor's IP address and the traffic in transit, stores no platform content (it caches only static application files such as images and code), and is bound by its data processing agreement with standard contractual clauses and its certification under the EU-US Data Privacy Framework. Platform e-mails are sent from our own server in Germany and do not pass through Cloudflare.

The assistant sends the provider up to the last 24 messages of the conversation, attachments, relevant excerpts of the organisation's documents and the employee's own records listed in [B8](#); the platform never adds the employee's name or e-mail, and never sends the wellbeing profile, reports, surveys or break data.

7 Have the AI Act's measures been taken for lawful use of the assistant?

Yes, for the obligations that concern the assistant. HRemia is the provider of its AI systems and the organisation the deployer. By intended purpose, with no decisions about workers and no evaluation of learning outcomes, the systems are not high-risk under Annex III points 3 and 4.

No emotion recognition: no biometric data and no scoring of emotions, mood or burnout, and the assistant is instructed never to infer or describe anyone's emotions from a face, a photo, a posture or a voice, including in images an employee attaches (art. 5(1)(f)). Transparency (art. 50(1)): every conversation, new or reopened, starts with the notice "You're talking to an AI assistant, not a person."; a permanent notice says that it is an AI, not a doctor or therapist; the assistant says it is an AI whenever asked, never claims to be human, and reminds the employee of it in long or emotionally heavy conversations, when asked for legal or health guidance and when it points to a person (C(2026) 5054, paras 37 and 40). Marking (art. 50(2)): every text the AI generates or translates carries a machine-readable mark, with a public description of the scheme at [/v1/ai/provenance](#). AI literacy: a transparency note with instructions; the organisation runs its own literacy measures. In Greece the ΑΠΔΠΧ supervises art. 50, and AI Act breaches can be reported through the N. 4990/2022 channel.

Proof: A5 · B8

8 Which model is the assistant based on?

On large general-purpose language models of established providers, such as OpenAI, Anthropic and Google. The primary model and the fallback models, used in order only when the one before is unavailable, are named in the organisation's sub-processor list; no other AI provider is used for it. For short auxiliary tasks such as updating Memory, a lighter model of the same provider may be used; it is also named in the list. Embeddings for document search are computed locally on our server.

Models are chosen after comparative evaluation on Greek legal texts; HRemia does not train them with customer data and does not use customer data to evaluate them. By agreement, and after a comparative evaluation on scenarios the organisation sets, the organisation can use another provider or model of its choice. HRemia configures it for that organisation alone and it applies only to that organisation's data; every call is recorded, in daily totals, with the provider and model that served it, so that compliance with the sub-processor list can be shown, and the organisation's HR and DPO see this on the Compliance page. It is not a self-service setting. The conditions: business terms without training on the data, a processing agreement, and listing in the sub-processor list.

Proof: B8 · B6

9 What is the purpose of processing in the Breaks («Διάλειμμα») function?

Breaks is an optional offer of short games. Processing serves two purposes only: keeping to the daily and per-session limits the organisation sets, and giving the organisation aggregate usage figures. No AI is used. The offer is in addition to the rest breaks of working-time law (Directive 2003/88/EC, art. 4) and neither records nor replaces them.

How much time each person used is held only in the application's cache for up to two days and then deleted; the database stores only daily totals per company and game, with no identity. The organisation sees 30-day totals; days with fewer than five participants are not shown. HR can set a different daily limit for a person. The DPA and the employee-information template state that the data is not used to assess performance or for discipline.

Proof: A4 · B5

10 Is the data-minimisation principle respected?

Yes, by design in every function that collects data: the assistant reaches only the asking employee's records, enforced by RESTRICTIVE row-level policies; the employer cannot read conversations; figures only for groups of five or more; breaks stored as totals; anonymous reports hold no identifying fields and the database rejects one that would; no IP addresses or user agents in the database and no access log on our web server (for Cloudflare, see question 6); multiple-choice surveys stored without identity or timestamp; no diagnosis for health-related leave; notifications without content; local document search.

Storage limitation is a separate principle. The organisation sets the retention period (default 24 months), with separate periods, if it chooses, for conversations and Memory, for closed reports and for the audit trail; at the end of each period the data is deleted automatically. For reports the specific rules apply: an open case is never deleted; the reports officer or a deputy can keep a case until the proceedings are over, or place it on legal hold while an investigation or proceedings are pending, which keeps it beyond the organisation's period (and suspends any date they record for the case); the case's entry in the special file stays. Employees can also delete their Memory notes themselves at any time. Deleted data remains in the encrypted backups until their cycle ends, up to about six months. A DPIA is mandatory for this processing, and HRemia supports it.

Proof: A4 · B5 · B7

C2 Design boundaries and the organisation's part

Facts about the design that a legal or IT reviewer should have in view, and what remains the organisation's own obligation.

Design boundaries

1. **Encrypted, not anonymised.** Conversations, Memory, reports and their evidence files are personal data, protected by encryption and access control, and treated as personal data (B4).
2. **HRemia holds the keys.** The keys are kept on HRemia's server in the EU and, for disaster recovery, in its encrypted off-site backup, so HRemia can technically decrypt the data. As processor it acts only on the organisation's documented instructions under the DPA; technical access is limited to the cases the DPA lists, each documented and notified where the law allows (A4, B4). The keys are not customer-managed.
3. **Sign-in.** Accounts created for an organisation sign in with a one-time link sent to the user's e-mail address, valid for 20 minutes and usable once; no password is stored for them and no second factor is used, so an account is as secure as its user's mailbox (B3).
4. **Server set-up.** A dedicated server at Hetzner in Falkenstein, Germany, not shared with other Hetzner customers; it also runs the operator's other websites and e-mail service, and HRemia is separated from them by its own containers, database and internal network. hremia.eu and www.hremia.eu reach it through Cloudflare's network, for protection against denial-of-service attacks, with TLS on both legs; e-mail does not pass through Cloudflare (B2, A4 point 8).
5. **Oral reports.** Audio recordings are not stored on the platform; the minutes are, and the reporter checks, corrects and confirms or signs them (A2).
6. **Pseudonymised export.** It replaces the reporter's name, contact details and account, also in the free text, and the other persons the officer selects; names elsewhere in the free text are not detected automatically, so the officer reviews third-party names before the file is sent (Directive art. 22(2); in Greece, N. 4990/2022 art. 21 §2).
7. **Other member states.** The Directive's common core is built in; national specifics are confirmed per member state with local counsel before launch in that market and recorded in a country annex (A1).

What remains the organisation's own duty

- Designate the Υ.Π.Π.Α./reports officer and deputies; in Greece, notify the Labour Inspectorate.
- Adopt the internal reporting procedure; carry out the DPIA.
- Place a prominent link to the public page on the company website; post the information at the workplace.
- Decide on oral reporting and meetings; acknowledge, follow up and give feedback in time.
- Set the retention periods and, for each closed case, decide how long it is kept; place a case on legal hold while an investigation or proceedings are pending.
- Choose the lawful bases, inform employees, and consult worker representatives where the law requires.
- Protect reporters from retaliation. The law's protection is conditional (Directive art. 6; in Greece, N. 4990/2022 art. 7).

Questions about this annex: hello@hremia.eu; for data-protection matters: dpa@hremia.eu. The annex is updated with each release; the edition date is on every page.