Questions and answers

HRemia platform · Data protection, the reporting system and the Artificial Intelligence Act

September 2026

The questions below are those asked by the legal and IT departments of organisations evaluating HRemia. For each question we set out the legal framework, how HRemia applies it and the document that substantiates it.

How you can check every statement. Every statement is substantiated in HRemia's "Legal & Technical Compliance Annex". The statements in this document carry a claim code [Π-n] and a reference to a section of the Annex (for example, "Annex B3"). In section 0 of the Annex, a table maps each code to the section that describes the mechanism and how it is verified. In particular:

- Part A covers the legal framework and the allocation of responsibilities;
- Part B, which is also addressed to your IT department, describes the technical and organisational measures and lists the automated tests (more than 500) that verify each guarantee (section B10);
- the final part brings together, in generic form, the answers to the questions in this document.

Greece, in brief. The platform covers the technical requirements of Law 4990/2022 (ν. 4990/2022) and Joint Ministerial Decision (ΚΥΑ) 47312/2023 (ΚΥΑ 47312/2023) for the reports officer (Υπεύθυνος Παραλαβής και Παρακολούθησης Αναφορών, Υ.Π.Π.Α.). This is documented in the Annex's matrix (section A2), article by article (Law 4990/2022, Articles 6–17 and 21–23; ΚΥΑ 47312/2023, Articles 2–5). For each requirement, the matrix states the platform function, how it is verified and the part that remains with the organisation.

Compliance with the law remains your organisation's obligation (Annex A6). In particular, the organisation:

- designates the reports officer and notifies the Labour Inspectorate of the designation (Law 4990/2022, Article 9(1) and (11) and Article 25);
- adopts the internal reporting procedure (ΚΥΑ 47312/2023, Article 3(6));
- places a link to the platform in a prominent position on its website (ΚΥΑ 47312/2023, Article 2(3)) and posts information at the workplace (Article 10(2)(α) of Law 4990/2022);
- carries out a DPIA (question 10);
- protects reporters from retaliation (Article 17 of Law 4990/2022).

The platform facilitates each of these steps (question 2), but is no substitute for them.

Purpose of this document. The answers describe how the service operates for every organisation that uses it. They do not replace the assessment your organisation will carry out as controller; we support that assessment with the documents listed at the end.

Abbreviations used:

- GDPR: Regulation (EU) 2016/679.
- AI Act: Regulation (EU) 2024/1689.
- DPA: data processing agreement.
- SCCs: Standard Contractual Clauses.
- DPIA: data protection impact assessment.
- ΑΠΔΠΧ: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, the Hellenic Data Protection Authority.
- Υ.Π.Π.Α.: Υπεύθυνος Παραλαβής και Παρακολούθησης Αναφορών, the reports officer.
- Ε.Α.Δ.: Εθνική Αρχή Διαφάνειας, the National Transparency Authority.
- Annex: HRemia's Legal & Technical Compliance Annex.

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

Legal framework. Directive (EU) 2019/1937 lays down minimum rules (Article 25). The employer's specific obligations are set by the national transposing law. In Greece, that law is Law 4990/2022 (Government

Gazette A' 210), as in force, together with KYA 47312/2023 (Government Gazette B' 6944/11.12.2023), which specifies the internal reporting procedure in detail. For Greece, Law 4990/2022 governs, among other things:

- the designation of a reports officer in private-sector entities with 50 or more employees (Article 9(1));
- the procedure (Article 10):
  - submission in writing, orally or through an electronic platform, and a meeting with the reports officer on request (paragraph 1);
  - acknowledgement of receipt within 7 working days (paragraph 2(γ));
  - feedback to the reporter within 3 months of the acknowledgement of receipt (paragraph 2(ζ));
- the conditions for the protection of reporters (Article 7);
- confidentiality (Article 14);
- data processing (Article 15);
- record-keeping (Article 16);
- penalties: for infringements of the law committed for the benefit or on behalf of a legal person, an administrative fine of EUR 10,000 to EUR 500,000 (Article 23(5)).

How HRemia applies it.

- **Why the Greek brochure cites only Greek law.** The Greek material is the edition for the Greek market, which is why it refers to Greek law. Under our policy, Greek law appears only:
  - in material for the Greek market;
  - on the pages of companies established in Greece.

  Material for other markets refers to the Directive, not to Greek law.
- **The rule also applies within the platform.** Each company records its country and has a public reporting page (hremia.eu/{language}/speak-up/{company}) that requires no account [Π-15]. This means that former employees, applicants and external collaborators can also submit reports (Article 6 of Law 4990/2022; Article 4 of the Directive). The page is available in 10 languages, including Greek and English (KYA 47312/2023, Article 2(3)). The company's country determines [Π-16]:
  - the legal texts the page displays;
  - the external authority to which it refers: for companies established in Greece, the National Transparency Authority (Ε.Α.Δ.); for companies in other member states, the competent authorities of their country;
  - the archive grounds offered to the reports officer;
  - the check run by the compliance centre (question 2): for Greek companies against Law 4990/2022 and KYA 47312/2023, for all others against the Directive.
- **Protection is conditional.** The public page informs the reporter that the prohibition of retaliation applies when the conditions of the law are met (Article 7 of Law 4990/2022; Article 6 of the Directive). The platform neither assesses nor guarantees the reporter's protection.
- **Other applicable texts.** Law 4990/2022 is not the only Greek text relevant to the platform. The following also apply:
  - the GDPR and Law 4624/2019, in particular Articles 22 and 27 (special categories of data and data in the employment context);
  - Law 4808/2021, for reports of violence and harassment at work, the application of which Law 4990/2022 leaves unaffected (Article 9(14)). The public page accepts such reports as a separate subject; the reports officer forwards them to the competent person in your organisation and, if they do not contain a breach within the scope of Article 4 of Law 4990/2022, archives them as out of scope (KYA 47312/2023, Article 4(1)(ββ));
  - the AI Act and Law 5321/2026 (Government Gazette A' 114/20.7.2026), which implements it. Law 5321/2026:

- designates the Hellenic Data Protection Authority (ΑΠΔΠΧ) as market surveillance authority, among other things for the transparency obligations under Article 50 of the AI Act (Article 3(1));
- brings infringements of the AI Act within the scope of Law 4990/2022 (Article 20);
- repealed, with effect from 20 July 2026, Chapter B of Part A of Law 4961/2022 (Articles 3–14), including the obligation under Article 9 to inform employees about the use of AI (Article 26). This is why we do not refer to Law 4961/2022.

Supporting documentation.

- Annex A1 (legal framework) and A2 (matrix for Greece).
- Greek country annex to the DPA (with the contract proposal).

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

Legal framework. We agree that national rules differ. By way of example:

- **Reports.** Directive 2019/1937 leaves certain matters to the member states, such as whether there is an obligation to accept anonymous reports (Article 6(2)). The transposing laws also differ on retention periods, deadlines and penalties. Examples:
  - Germany: Hinweisgeberschutzgesetz;
  - Italy: D.Lgs. 24/2023;
  - Spain: Ley 2/2023;
  - Romania: Law 361/2022.
- **Employee data.** The GDPR allows more specific national rules (Article 88), subject to the conditions laid down by the Court of Justice of the European Union (CJEU) in Case C-34/21.
- **Worker representatives.** Informing or consulting them about technical systems in the workplace is governed by national labour law (for example, in Germany, § 87(1) no. 6 BetrVG). The AI Act expressly preserves national provisions that are more favourable to workers (Article 2(11)).

How HRemia applies it. Yes, it has been taken into account. The platform distinguishes two layers.

- **(a) A common European core, in all countries.** It comprises:
  - the Directive's requirements for the internal channel: confidentiality, exclusive access for the handlers, the option of reporting anonymously, record-keeping;
  - the GDPR;
  - the AI Act.

  For each case, the platform calculates two deadlines, using the organisation's calendar and time zone, and reminds the handlers of them [π-6]: the acknowledgement of receipt and the feedback to the reporter. It applies the limits of the law that governs the company and never sets a date later than them:
  - for companies established in Greece, Law 4990/2022: 7 working days for the acknowledgement (Saturdays, Sundays and nationwide public holidays are not counted) and 3 months from it for the feedback (Article 10(2)(γ) and (ζ));
  - for companies in other Member States, the Directive: 7 days for the acknowledgement and 3 months from it for the feedback (Article 9(1)(b) and (f)).

  If no acknowledgement is sent, the 3 months run from the end of the acknowledgement period. Stricter national rules of other Member States are recorded in the country annex (see below).

  The acknowledgement of receipt and the feedback are recorded as separate acts, with their date and author, so that they can be proven. To escalate a case, the handler must give a reason. Escalation shortens the deadlines and transfers the case to an independent handler [π-6]:
  - where handlers have been designated, to the reports officer or, if the reports officer is already handling the case, to a deputy;

  - where none have been designated, to the organisation's Data Protection Officer (DPO).
- **(b) A national layer, based on the country each company records.** The country determines the legal texts displayed and the competent external authority (question 1).

  For Greece, Law 4990/2022 and KYA 47312/2023 apply; the matrix is in Annex A2. For the other member states, Annex A3 maps the articles of the Directive to the platform's functions. Before the service is offered in each new market, local counsel reviews the national layer, and the result is recorded in a country annex. The review covers:

  - retention periods;
  - the rules on anonymous reports;
  - the competent authority;
  - obligations to inform or consult worker representatives;
  - the language of the legal documents.

  For your organisation, the Greek annex applies.
- **Tools for the reports officer (for companies established in Greece).** They include:
  - exclusive access to cases for the reports officer and their deputies, with the option of withdrawal for conflict of interest (κώλυμα; question 5) [Π-13];
  - a special file of reports (KYA 47312/2023, Article 3(6); Article 16 of Law 4990/2022) [Π-17]. Every report is registered with a number, whatever the channel: the platform, a letter, an email to the reports officer's dedicated address, telephone or a meeting. Deadlines run from the actual time of receipt;
  - minutes of an oral report or meeting (Article 16(2)–(5) of Law 4990/2022; KYA 47312/2023, Article 3(3)). The reporter checks them, requests corrections and confirms them electronically; the confirmation is recorded as a simple electronic signature (Article 3(10) of Regulation (EU) 910/2014), and your organisation decides whether it also wants a signature on paper. Alternatively, the reports officer records that the minutes were signed outside the platform or that the reporter refused to sign them. Once shared with the reporter, the minutes are not deleted;
  - provable acknowledgement of receipt and feedback to the reporter (Article 10(2)(γ) and (ζ) of Law 4990/2022) [Π-17];
  - closing and reopening a case [Π-18]:
    - closing on one of the archive grounds of the KYA (Article 4(1)(β)) or by referral;
    - reopening an archived case when new evidence emerges, while the previous outcome remains in the history;
  - pseudonymised export of the case file for referral to a competent body within the organisation or to an external body, with a referral log (Article 10(2)(δ) of Law 4990/2022; KYA 47312/2023, Article 4(1)–(2)). Every export is recorded in the case history. The export replaces the reporter's identity automatically. The reports officer can also select persons concerned or third parties, whose name and contact details are replaced by a pseudonym; because other details in the text may still identify people, the officer reviews the text before it is sent (Article 21(2) of Law 4990/2022) [Π-18];
  - a dedicated route for a report concerning the reports officer themselves or one of their deputies: the case allows only its registration and its referral to the E.A.Δ., with notice to the reporter (KYA 47312/2023, Article 4(3), which also covers reports against the body that investigates reports) [Π-18];
  - recording of the reports officer's term of office (at least one calendar year, Article 9(6)), with a notification to HR 30 days before it ends [Π-19];
  - a declaration by the reports officer personally and by each deputy that no statutory impediment applies to them and that their other duties do not affect their independence (Article 9(9) and Article 10(3));
  - an A4 poster with a QR code for the workplace, and embed code for placing the reporting page on the organisation's website.

- **Whistleblowing compliance centre [Π-19].** The “Whistleblowing compliance” screen checks the organisation's configuration against the law of its country.
  - **What the platform can see, it checks itself:** the reports officer's designation, term of office and eligibility declaration, the dedicated email address, the public page, the information on the Ε.Α.Δ., compliance with the deadlines.
  - **What it cannot see, the organisation declares,** with a date and supporting evidence: the link on the website, the notice posted at the workplace, the notification to the Labour Inspectorate, the internal procedure, the DPIA. Every declaration is recorded in the audit log [Π-7].
  - **Metrics and evidence pack.** It provides 12-month metrics and a printable evidence pack for an auditor or for the Labour Inspectorate. For Greece, the pack includes the details required for notifying the Labour Inspectorate of the reports officer (Article 9(11)). It contains no report content and no information about reporters. Categories with fewer cases than the organisation's anonymity threshold (at least 5) are not shown [Π-20].
- **Labour law in the HR functions.** The platform does not build in the legislation of any country and does not calculate statutory entitlements:
  - Leave entitlements are recorded by the employer. The digital assistant is instructed to state the recorded data without performing calculations.
  - For legal and regulatory questions, the assistant relies on the documents the organisation itself uploads (internal regulations, policies, collective agreements).
  - An automated check removes from the answers any references to articles not contained in those documents [Π-8].
  - For anything the documents do not cover, the assistant directs the employee to HR.

  In this way, differences in national labour law are reflected through each organisation's own documents, not through a single built-in rule.
- **Oral channel.** The organisation sets up the oral channel, if it offers one (for example, a telephone line), and arranges meetings on request (Article 10(1) of Law 4990/2022). Telephone reports and meetings are registered by the reports officer in the platform's special file, with minutes that the reporter checks and confirms. The reporter can request a meeting from the public page. The reports officer registers oral reports and minutes in the platform's special file, as described above.
- **File attachments.** The reporter can attach documents and photographs to their report. Before storage, the platform automatically removes metadata that could identify them (for example, the GPS location of a photograph or the author of a document), and the files are stored encrypted with the organisation's report key [Π-3].

Supporting documentation.

- Annex A2 (Greece), A3 (the Directive, for companies in other member states) and A6 (allocation of responsibilities, with a checklist).
- Greek country annex to the DPA (with the contract proposal).
- DPIA support pack (with the contract proposal).

3. Which contract is provided for? Who is the controller and who is the processor?

Legal framework.

- GDPR: Article 4(7) and (8), Articles 28 and 29.
- Guidelines 07/2020 of the European Data Protection Board (EDPB) on the concepts of controller and processor.

The contract we propose.

- **(a) A software-as-a-service (SaaS) agreement.**

- **(b) A DPA under Article 28(3) GDPR, forming an integral part of that agreement.** It is based on the SCCs between controllers and processors set out in Implementing Decision (EU) 2021/915 (Article 28(7) GDPR). It describes the subject matter, duration, nature and purpose of the processing, the types of data and the categories of data subjects, and includes all the obligations of Article 28(3):
  - processing only on your documented instructions, including with regard to transfers outside the European Economic Area (EEA) (point (a));
  - a confidentiality commitment from personnel (point (b));
  - the security measures of Article 32 (point (c));
  - conditions for sub-processors (point (d));
  - assistance in responding to requests from data subjects exercising their rights and in meeting the obligations under Articles 32–36 (points (e) and (f));
  - deletion or return of the data at the end of the service (point (g));
  - making available the information needed to demonstrate compliance and facilitating audits, as well as informing you immediately if, in our opinion, an instruction of yours infringes the GDPR (point (h)).
- **Annexes to the DPA:**
  - description of the processing, expressly addressing the data covered by Articles 9 and 10 GDPR;
  - Technical and Organisational Measures (TOMs), namely Part B of the Annex;
  - sub-processor list;
  - reporting channel;
  - AI functions;
  - retention and deletion programme;
  - Greek country annex.

Where a sub-processor processes data outside the EEA, the transfer relies on a safeguard under Chapter V GDPR (see question 6). In the event of any discrepancy between the general texts on our website and the signed DPA with its annexes, the DPA and its annexes prevail.

3.1 Your organisation is the controller. This applies to all data the platform processes on your behalf: data of employees, of reporters and of persons named in reports.

- For reports, this is expressly provided by Article 15(3) of Law 4990/2022.
- The same applies to employees' private conversations with the digital assistant:
  - the organisation decides to make the service available to its employees and determines its purpose;
  - the organisation has no access to the content, but being controller does not presuppose access to the data (CJEU, C-210/16, Wirtschaftsakademie Schleswig-Holstein, paragraph 38; C-25/17, Jehovan todistajat, paragraph 69);
  - for employees' requests (access, erasure, etc.) concerning their conversations, HRemia assists you on your instructions, without disclosing the content to HR (Article 28(3)(e)).

HRemia is an independent controller only for:

- the contact and invoicing details relating to our business relationship;
- the contact form on its website;
- the security records of its infrastructure.

The DPA expressly prohibits HRemia from using your organisation's data for its own purposes, such as training or evaluating models (Article 28(3)(a) GDPR; see also Article 28(10)).

3.2 HRemia is the processor.

- **Sub-processors.** The providers HRemia uses are sub-processors (Article 28(2) and (4) GDPR). Each is bound by a processing agreement providing at least the same level of protection as the DPA. For the large providers, these are their standard agreements, which are listed in the sub-processor list. HRemia remains fully liable to you for their performance.

- **Change of sub-processor.** The DPA provides for general written authorisation, with prior written notice to you of any change, given within a notice period set in the DPA, and a right to object. In the event of an objection:
  - the parties seek an alternative provider within a dedicated configuration for your organisation (see question 8);
  - if this is not feasible, your organisation has the right to terminate.

For data protection matters: dpa@hremia.eu.

Supporting documentation.

- Proposed DPA and sub-processor list (with the contract proposal).
- Annex A4 (roles under the GDPR).

4. Which special categories of data (Article 9 GDPR) are processed, and on what legal basis?

Legal framework.

- Special categories of data require, cumulatively, a legal basis under Article 6 and a condition under Article 9(2) GDPR (CJEU, C-667/21, Krankenversicherung Nordrhein).
- The concept also covers data that indirectly reveals a special category (CJEU, C-184/20; C-252/21).
- The legal basis is chosen and documented by the organisation, as controller (Articles 5(2) and 24 GDPR).

Below, for each category of data, we set out our assessment and how the platform supports it. The full table of legal bases per function is in Annex A4.

(a) Leave

- **Data:** the type of leave (sick, maternity, parental), the dates, and whether a medical certificate was provided and its date. This is health data; maternity leave also reveals pregnancy.
- **What is not stored:**
  - the platform has no diagnosis field;
  - no comment from the employee is stored on health-related leave requests;
  - no comment from HR is stored when the corresponding periods are recorded.
- **HR note:** HR's decision on a leave request may be accompanied by a short free-text note. We recommend that it contain no health data.
- **Legal basis:**
  - Article 6(1)(b) and (c) GDPR;
  - Article 9(2)(b) GDPR and Article 27(3) of Law 4624/2019: the processing is necessary for the performance of the employer's obligations under labour and social security law in respect of such leave, with the measures of Article 22(3), second sentence, of the same Law.

(b) Reports

- **Data:** reports may contain:
  - health data;
  - data concerning sex life (for example, in harassment complaints);
  - trade union membership;
  - data covered by Article 10 GDPR (allegations of offences).
- **Legal basis:**
  - Article 6(1)(c) GDPR, in conjunction with Articles 9 and 15(2) of Law 4990/2022, for obliged entities. For organisations without such an obligation, Article 6(1)(f);
  - in our assessment, Article 9(2)(g) (substantial public interest, as established by the Directive and Law 4990/2022). We note that Law 4990/2022 does not expressly regulate special categories of data;
  - Article 9(2)(f) (establishment, exercise or defence of legal claims);
  - for incidents of violence and harassment, also Article 9(2)(b) in conjunction with Law 4808/2021;

  - for data covered by Article 10 GDPR, Law 4990/2022 in conjunction with the Directive. We recommend that this be specifically documented in the DPIA.
- **Protection:** the measures protecting reports are described in question 5:
  - encryption [Π-3];
  - exclusive access for the reports officer, and withdrawal for conflict of interest [Π-13];
  - anonymous reports [Π-2].

(c) Private conversations with the digital assistant, attachments, Memory and the "wellbeing profile"

- **Data:**
  - the employee may voluntarily raise health (including mental health), family, trade union or religious matters;
  - to answer the employee's questions, the assistant also receives the employee's own leave data, including health-related leave periods (see question 6). This purpose differs from the leave management described in point (a); the Article 9 condition you choose for the assistant must therefore also cover this data;
  - **Memory (optional)** [Π-12]:
    - By default, the assistant sees only the current conversation.
    - Only the employee personally can switch Memory on, from the "What your assistant remembers" screen in their account or from the conversation; that is also where they view and manage their notes.
    - If the employee personally switches Memory on, the assistant keeps a short list (up to 25 items) of things the employee has mentioned that will help them in later conversations: for example, their role or a situation they are seeking help with.
    - The employee can view, correct and delete any item, or the whole list, at any time.
    - Because the list contains what the employee personally mentioned, it may also include special categories of data. It is therefore subject to the same legal-basis analysis as the conversations;
  - the wellbeing profile is completed by the employee personally, is stored encrypted and is not sent to the AI provider.
- **Legal basis — the decision is your organisation's.** Our assessment:
  - for an optional support tool, the conditions of Article 9(2)(b) and (h) are difficult to apply. No labour-law obligation requires the tool, and it does not involve the provision of health care by a professional bound by professional secrecy (Article 9(3));
  - the condition that fits most clearly is explicit consent (Article 9(2)(a)), subject to the heightened requirements of the employment context:
    - consent must be freely given (recital 43 GDPR; EDPB Guidelines 05/2020, paragraphs 21–22);
    - in Greece, written or electronic form, clearly distinguishable from the employment contract, with express reference to the special categories of data and with information on the purpose and on the right to withdraw consent (Article 27(2) and (3) of Law 4624/2019).
- **How the platform supports your decision.** If you choose explicit consent, the organisation collects it, using our template, before giving the employee access to the assistant. In particular:
  - use of the assistant is optional, and Memory is switched off until the employee personally switches it on;
  - HR, managers and the organisation's administrators have no access to the content of conversations or to Memory. This is enforced at database level (see question 5) [Π-1];
  - the organisation does not see who uses the assistant or how much; it sees only aggregate data. Non-use is therefore not visible. Refusing consent must have no adverse consequences for the employee, and the template says so expressly;
  - if you choose explicit consent, we provide you with a template consent and information form (Articles 7 and 13 GDPR; Article 27(2) and (3) of Law 4624/2019). The organisation collects it before

giving the employee access to the assistant. If consent is withdrawn, the employee stops using the assistant, and on your instructions we delete their conversations and Memory.

(d) Surveys

- They accept only multiple-choice answers, with no free text.
- Special categories of data arise only if the organisation asks a question on such a matter (for example, about health).
- Results are shown only in aggregate, for groups of at least 5 people [Π-11].

Supporting documentation.

- DPIA support pack (with the contract proposal), including:
  - a table of legal bases per category of data;
  - an employee-information template (Articles 13–14 GDPR);
  - an explicit-consent template, if you choose that basis.
- Annex A4 (legal bases per function).

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

Legal framework.

- Data is anonymised only if it can no longer be linked to a person by means reasonably likely to be used (recital 26 GDPR).
- Encryption is a security measure (Article 32(1)(a) GDPR). For anyone who holds the means of re-identification, such as the keys, the data remains personal data (see, on pseudonymised data, CJEU, C-413/23 P, EDPS v SRB, 4 September 2025).

Answer: the data is not anonymised; it is encrypted. It is personal data and we treat it as such.

What is encrypted at application level [Π-3]:

- **The employee's private space:**
  - the content of messages in private conversations;
  - the content of attached files;
  - Memory items;
  - the wellbeing profile.

  The title of each conversation (the first 60 characters of its first message) and the names of attached files are not encrypted at application level; they are protected by the same database access restrictions described below.
- **Reports:**
  - the subject, the text and the messages of the case;
  - the reporter's name and contact details, where given;
  - the questionnaire on the public page;
  - the minutes;
  - the texts of referrals;
  - the reasons given for withdrawals for conflict of interest (κώλυμα);
  - the files attached to the report and their names;
  - the closing texts.

Other data (leave and employment records, the contact directory, the organisation's documents, training, surveys, announcements and user accounts) is not encrypted at application level; it is protected by database permissions and per-company isolation (Annex B3, B4).

How encryption works [Π-3]:

- encryption uses AES-256-GCM, with separate keys for each company;

- each company has one key for conversations and a separate key for reports, so that managing one does not affect the other;
- each encrypted report field is bound to its specific record, so that it cannot be moved to another. Likewise, each Memory item is bound to the employee to whom it belongs;
- company keys are protected by a master key, which HRemia holds on its server in the EU and, for disaster recovery, in the encrypted backup.

Who can read what.

- **Private conversations, Memory and wellbeing profile.** HR, managers and the organisation's administrators cannot read them:
  - the database account through which the HR screens operate has no permissions at all on the schema where they are stored [Π-1];
  - row-level security rules separate each company's data and confine each employee to their own data [Π-4].
- **Reports.** From the moment the organisation designates a reports officer and deputies, only they, within the organisation, have access to the content of cases (Article 14 of Law 4990/2022) [Π-13]:
  - exclusive access is enforced by the database, not only by the application;
  - after the first designation, only the reports officer (or, if no reports officer is in post, a deputy) can change who handles reports; this too is enforced by the database. Every change is recorded, and those affected are notified;
  - a handler with a conflict of interest declares a withdrawal (κώλυμα) for the specific case (Article 9(8)(γ) of Law 4990/2022). From that moment, the database returns no data from that case to them. Only another handler can lift the withdrawal, and its record, with the reason, remains permanently in the case file;
  - until a reports officer is designated, HR administrators and the organisation's DPO have access. For this reason:
    - designating the reports officer is one of the first steps in activating your organisation;
    - we recommend publishing the link to the reporting page after the designation.
- **Anonymous reports** [Π-2]:
  - they store no user account, name or contact details; this is enforced by a database CHECK constraint;
  - nor do they store a department or IP address;
  - the reporter follows the case using the report number and an access code, which is shown to them once and stored only as an argon2 hash.
- **IP addresses.** The platform's web server keeps no access log of visitors' IP addresses. Traffic to the platform passes through the Cloudflare network, which processes the IP address to protect against attacks (question 6). The IP address is held temporarily only to protect against abuse (rate limiting), is deleted automatically within 10 minutes and is not linked to any report or account [Π-2].
- **Audit log** [Π-7]:
  - actions on cases and settings are recorded in an audit log;
  - the application's account can only add entries to it, not change or delete them;
  - entries relating to a case are visible only to its handlers.
- **In transit.** Users' connections to the platform are encrypted (TLS) along the whole route: to Cloudflare and from Cloudflare to our server, with our server's certificate validated. Connections to the AI providers in your organisation's configuration are also encrypted (TLS); this is a condition for activating your organisation (question 6).

Can HRemia see the data? Technically, yes. HRemia manages the infrastructure and holds the keys on its server in the EU, so it can technically decrypt the data. That is why we speak of encryption and not of anonymisation. In particular:

- through the application, HRemia staff see only aggregate figures per organisation and its configuration (for example, its AI providers), never content;
- encryption applies to storage: for the assistant to answer, the conversation content is decrypted on the server and sent to the AI provider (see question 6). Reports are never sent to an AI provider [n-21].

Legal basis.

- **For your organisation:** the legal bases set out in question 4.
- **For HRemia:** it has no legal basis of its own to access the content. As processor, it processes data only on your instructions (Articles 28(3)(a), 29 and 32(4) GDPR). The DPA lists exhaustively the cases of technical access:
  - support at your written request;
  - handling a security incident;
  - a legal obligation.

  Every such access is documented and notified to you, where the law permits.

Supporting documentation. Technical and Organisational Measures (Part B of the Annex). In particular:

- B3: access control, with the names and rules of the database policies;
- B4: encryption and key management;
- B5: anonymity measures;
- B6: audit log and logging;
- B10: the automated tests that verify the above.

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

Legal framework.

- **Sub-processors:** Article 28(2) and (4) GDPR (authorisation, notification, objection, flow-down of obligations). According to EDPB Opinion 22/2024, the controller must know the identity of all sub-processors.
- **Transfers outside the EEA** (Chapter V, Articles 44–46 GDPR): where they occur, they rely on one of the following bases:
  - an adequacy decision, for example Implementing Decision (EU) 2023/1795 (EU–US Data Privacy Framework) for certified entities;
  - appropriate safeguards, such as the SCCs in Implementing Decision (EU) 2021/914, with a transfer impact assessment.

Platform storage: in the EU [n-5].

- All customer data is stored with Hetzner Online GmbH in Falkenstein, Germany: database, reports, conversations and files.
- The server is dedicated (it is not shared with other Hetzner customers) and also hosts our operator's other web and email services; HRemia runs in its own containers, with its own database and internal network (Annex B2).
- Encrypted backups are also kept in the EU, with Hetzner.
- Search in the organisation's documents (computation of vector embeddings) runs locally on our server, with no third-party provider.

Processing by AI models [n-10].

- **Hosting.** The AI models are not hosted at Hetzner.
- **Providers and terms.** For your organisation, answers are generated by models of established providers, which are named in the sub-processor list together with their processing agreement. The providers operate on paid business terms, under which:
  - they do not use the data to train their models;

  - they retain it only for a limited period, stated for each provider in the sub-processor list.
- **Condition for activation.** Your organisation is activated only when the providers in its configuration operate on these terms, over a TLS connection, and have been entered in the sub-processor list; its data is not sent to any other AI endpoint.
- **Location.** Depending on the provider, processing may take place outside the EEA. In that case, one of the Chapter V safeguards mentioned above applies.

What is sent to the AI provider when the employee uses the assistant:

- up to the last 24 messages of the conversation, including the current one;
- the message's attachments;
- the relevant excerpts from the organisation's documents;
- the employee's own leave data, including health-related leave periods and the medical-certificate indicator, as well as their leave requests and the decisions on them;
- the employee's own employment record, as entered by HR: date of appointment, position, contract type and end date, category, grade and salary step, end of probation, permanent appointment, recognised prior service and HR's note;
- the HR contact directory;
- the employee's list of courses;
- if the employee has switched Memory on [Π-12]:
  - their Memory list;
  - after each answer, the current list, the employee's new message and the assistant's immediately preceding answer, so that the list can be updated. This does not apply to the training assistant.

The following are not sent:

- the employee's name and email address (although the content may identify them);
- the wellbeing profile;
- data of other employees, apart from HR's contact details.

For the other AI functions, the following are also sent to the same provider:

- the material HR uploads for drafting quiz questions;
- the texts of announcements and questions for automatic translation;
- the course material, for the training assistant.

Reports, surveys and “Breaks” data are never sent to an AI provider [Π-21].

Sub-processor	Service	Place of processing	Data	Safeguards
Hetzner Online GmbH (Germany)	Hosting of the platform, the database and the files	Falkenstein, Germany	All platform data	Within the EU; agreement under Article 28 GDPR
Hetzner Online GmbH	Encrypted backups	Within the EU	Database backups	Within the EU; agreement under Article 28 GDPR
AI model providers, primary and fallbacks (established providers such as OpenAI, Anthropic and Google; those used for your organisation are named in the DPA's sub-processor list)	Generating answers of the digital assistant and the training assistant, updating Memory, drafting quizzes, translation; the fallbacks only when the previous one is unavailable	Depending on the provider, as stated in the sub-processor list	As described above	Paid business terms; processing agreement; no model training; limited retention; outside the EEA: adequacy decision or SCCs in Implementing Decision (EU) 2021/914
Browser push notification services (depending on the employee's browser and device; described in the sub-processor list)	Delivery of push notifications, only if the employee allows them on their device	Depending on the provider	Only end-to-end encrypted content and delivery metadata; notifications on sensitive matters carry only generic text	The provider has no access to the content [Π-14]
Cloudflare, Inc. (USA)	DNS service, protection	Cloudflare's network, as	The visitor's IP address	Cloudflare's data

	against distributed denial-of-service (DDoS) attacks and routing of traffic to our server, for the addresses hremia.eu and www.hremia.eu	a rule at the point closest to the visitor	and the traffic while in transit; it stores no platform content (it temporarily caches only static application files, such as images and code)	processing agreement with SCCs; certification under the EU–US Data Privacy Framework

Other flows.

- **Email.** Platform emails (sign-in links, notifications) are sent from our own server in Germany. Escalation messages carry only the case number.
- **YouTube videos.** If your organisation embeds YouTube videos in a course, the employee's browser connects directly to YouTube during playback. This is a content choice made by the organisation, not a sub-processor of HRemia.

Supporting documentation.

- Sub-processor list, as an annex to the DPA (with the contract proposal). For each sub-processor it states:
  - legal entity and registered office;
  - place of processing;
  - categories of data;
  - processing agreement;
  - transfer mechanism.
- Annex B1 (architecture and data flows per transit point), B2 (hosting, network, TLS) and B8 (AI processing per function).

7. Have the measures required by Regulation (EU) 2024/1689 been taken for lawful use of the assistant?

Legal framework. The AI Act has been in force since 1 August 2024 and applies in stages:

- **from 2 February 2025:** prohibited practices (Article 5) and AI literacy (Article 4);
- **from 2 August 2025:** obligations of providers of general-purpose AI models (Articles 53 and 55);
- **from 2 August 2026:** transparency obligations (Article 50). Specifically for the machine-readable marking under Article 50(2), Regulation (EU) 2026/1744 gives systems placed on the market before 2 August 2026 until 2 December 2026 (Article 111(4)); a system first placed on the market later must comply from the time it is placed on the market;
- **from 2 December 2027:** obligations for the high-risk systems listed in Annex III, as postponed by Regulation (EU) 2026/1744.

Roles.

- HRemia is the “provider” (Article 3(3)) of the AI systems it makes available under its own name:
  - the digital assistant, including its Memory;
  - the training assistant;
  - quiz question drafting;
  - content translation.
- These systems are built on general-purpose AI models of third-party providers, which bear the obligations of Articles 53 and, where applicable, 55. HRemia does not train or fine-tune models.
- Your organisation is the “deployer” (Article 3(4)).

Answer: Yes, for the obligations concerning the assistant. The measures HRemia has taken [n-9]:

- **Intended purpose and classification** (Article 3(12), Article 6, Annex III, points 3 and 4).
  - **What the systems do not do.** They are not intended for decisions about workers: recruitment, evaluation, promotion, termination of employment, allocation of tasks, or monitoring of

performance and behaviour. Nor are they intended for evaluating learning outcomes: quiz scores are calculated arithmetically, not by AI. The platform does not take decisions producing legal effects for employees (Article 22 GDPR).

- **Classification.** Given this purpose, the systems do not fall within the high-risk systems of Annex III, points 3 (education and vocational training) and 4 (employment).
- **Contract.** The intended purpose and the prohibited uses are set out expressly in the AI annex to the contract. If a deployer modifies the intended purpose in such a way that the system becomes high-risk, the deployer itself assumes the provider's obligations (Article 25(1)(c)).
- **Note on the brochure.** Annex III of the Regulation classifies certain AI systems for personnel management as high-risk; HRemia's systems, given their intended purpose, do not fall within them. In the brochure, legal and technical claims carry a claim code [n-n] referring to the Annex.

- **Prohibited practices (Article 5).**
  - **Emotion recognition.** The platform collects no biometric data (voice, camera images, keystroke patterns). It does not detect or score the emotions, mood or burnout of any employee. It therefore does not fall within the prohibition of emotion recognition in the workplace (Article 5(1)(f); Commission Guidelines on prohibited AI practices, C(2025) 5052, paragraphs 244–251 and 257). For wellbeing, the organisation receives only aggregate data, from categories that employees themselves choose [n-11].
  - **Memory.** Memory does not change this position [n-12]. It records only what the employee personally states. The mechanism that updates it is instructed not to record assessments or inferences about the employee's emotions, health or personality, and an automated test verifies that the instructions prohibit this.
  - **Manipulation and exploitation of vulnerabilities** (Article 5(1)(a) and (b)). The assistant is instructed:
    - not to make diagnoses;
    - to refer to professional help and to support lines in a crisis;
    - not to take decisions on employment matters.
- **Transparency (Article 50(1) and (5)).**
  - The chat screen permanently displays, below the input field: “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 state that it is an AI system whenever asked and never to claim to be human, as called for by the Commission's guidelines on Article 50 (C(2026) 5054 of 20 July 2026, paragraph 40). The permanent on-screen notice does not depend on the model's answers.
  - As recommended by the same guidelines (paragraphs 37 and 40), every conversation, new or existing, begins with the notice “You're talking to an AI assistant, not a person.” before any answer from the model. In sensitive contexts, such as when the employee expresses emotional distress or seeks legal or health guidance, or when the assistant refers them to a human, the assistant is instructed to remind them that it is an AI system. The permanent notice remains visible throughout the conversation.
  - The assistant is also instructed to state honestly that it cannot see previous conversations, beyond what Memory retains if the employee has switched it on. It does not pretend to remember.
- **Content marking (Article 50(2)).** Every text generated by AI carries a machine-readable marking: an “ai_generated” flag and provenance data in the platform's data, an “X-AI-Generated” header in the application programming interface (API) responses, marking in the page elements and in exports, and a public description of the marking scheme. This marking is based on metadata. Beyond marking, the Commission's guidelines also call for a means of detection available to those exposed to the content, as well as robustness to the extent technically feasible (C(2026) 5054, paragraphs 69–72, 75–76 and 80–86); we keep the adequacy of the solution under review against the code of practice under Article 50(7).

- **AI literacy (Article 4, as amended by Regulation (EU) 2026/1744).** The transparency note accompanying the contract includes instructions for use for your administrators and employees. The note supports your own measures to promote AI literacy.
- **Deployer obligations.** The obligations of Article 26, such as informing workers' representatives (paragraph 7), concern only high-risk systems and do not apply here. The specific information obligation under Article 9 of Law 4961/2022 has been repealed (question 1). The obligation to inform employees under Articles 13–14 GDPR still applies, and we recommend that the information expressly cover the AI assistant and Memory. We provide you with a template (with the contract proposal).
- **Greek law.** In Greece, the competent market surveillance authority for the obligations under Article 50 is the ΑΠΔΠΧ (Article 3(1) of Law 5321/2026). In addition, infringements of the AI Act can now be reported through the Law 4990/2022 channel (Article 20 of Law 5321/2026). The public reporting page provides for this as a reporting area.

Supporting documentation.

- AI Act transparency note (with the contract proposal). It covers:
  - roles;
  - intended purpose and prohibited uses;
  - models and providers;
  - the measures under Articles 4, 5 and 50.
- Annex A5 (AI Act) and B8 (AI processing).
- AI annex to the DPA (with the contract proposal).

8. Which model is the digital assistant based on?

Legal framework.

- The model provider is a sub-processor (Article 28(2) and (4) GDPR).
- It owes the system provider the documentation required by Article 53(1)(b) of the AI Act.

Answer [Π-10].

- **Type of models.** The assistant is based on general-purpose large language models from established providers, such as OpenAI, Anthropic and Google, on business terms under which the data is not used for training.
- **Your organisation's configuration.** It specifies a primary model and fallback models, used in order only when the previous one is unavailable. All are named, together with their provider, in the DPA's sub-processor list. No other AI provider is used for your organisation. The vector embeddings for document search are computed locally, on our server (question 6) [Π-5].
- **Other functions.** The same models are used for the training assistant, quiz question drafting and translation. For short auxiliary tasks, such as updating Memory, a lighter model from the same provider may be used; it is also listed in the sub-processor list.
- **Choice of models.** Models are selected after comparative evaluation on Greek legal texts. HRemia does not train them with customer data and does not use customer data to evaluate them.
- **A model of your choice.** By agreement, and after comparative evaluation on scenarios you define, your organisation can use another provider or model of its choice.
  - The configuration is set up per organisation by HRemia and applies exclusively to your organisation's data; for each call, the provider and model that served it are recorded, so that compliance with the sub-processor list can be demonstrated.
  - Conditions: business terms without use of the data for training, a processing agreement and entry of the provider in the sub-processor list.

Supporting documentation.

- Sub-processor list and AI transparency note (with the contract proposal).

- Annex B8 (AI processing: what is sent per function).

9. What is the purpose of the processing in the “Breaks” function?

Legal framework.

- The purpose limitation principle (Article 5(1)(b) GDPR).
- Legal basis:
  - legitimate interests (Article 6(1)(f)), with a documented balancing test (recital 47); or
  - performance of a contract (point (b)), where the benefit is provided for in the terms of employment.
- No special categories of data are involved.

Purpose. “Breaks” is an optional benefit offering short games for breaks. The data processing serves exclusively two purposes:

- enforcing the daily time limit and the per-session limit set by your organisation;
- providing the organisation with aggregate usage data.

No AI is used. The benefit is in addition to the breaks provided for by working-time legislation (Article 4 of Directive 2003/88/EC) and neither records nor replaces them.

How HRemia applies it [Π-11].

- **Individual data.** The time each employee has used is held only in the application's cache, for up to 2 days, and is deleted automatically.
- **Database.** Only daily totals per organisation and game are stored, with no employee identity.
- **What the organisation sees.** 30-day totals. Days with fewer than 5 participants are not shown.
- **Individual limit.** HR can set a different daily limit for a specific employee.
- **Purpose limitation.** The DPA and the employee-information template state expressly that this data is not used for performance evaluation or for disciplinary purposes.

Supporting documentation.

- The DPA annex describing the processing, and the employee-information template (with the contract proposal).

10. Is the data minimisation principle respected?

Legal framework.

- Article 5(1)(c) GDPR (data minimisation).
- Article 25(1) and (2) GDPR (data protection by design and by default).
- EDPB Guidelines 4/2019.
- For the reporting channel, Article 15(4) of Law 4990/2022.

Answer: Yes. Minimisation is applied by design in every function that collects data:

- **Digital assistant.** Each conversation has access only to the personal records of the employee asking (leave, employment details, training) and to the HR contact directory [Π-4].
  - RESTRICTIVE row-level security policies enforce this at database level. As a result, other employees' leave, requests, employment records and training results are technically inaccessible, even to a query that omitted the relevant filter.
  - The data transmitted to the AI provider is listed in question 6.
- **Private conversations.** HR and the employer have no access, owing to the database permissions (question 5) [Π-1].
- **Memory.** It is switched off by default (question 4). If the employee switches it on, it keeps up to 25 short items, which the employee controls and can delete at any time [Π-12].

- **Aggregate data.** The organisation receives only aggregate data, with a minimum group size of 5 people [Π-11], for:
  - surveys;
  - culture and wellbeing trends;
  - "Breaks".

  For use of the assistant, it sees only total figures. For each AI call a technical usage record is kept (date, model, token counts, employee and conversation, no content) for cost control and provider accountability; it is not shown per person on any of the organisation's screens.
- **"Breaks".** Only aggregate data is stored (question 9).
- **Anonymous reports.** They store no data identifying the reporter (although the content may identify them): no account, name, contact details, department or IP address. The database rejects an anonymous report that would carry an account, name or contact details [Π-2].
- **Report content.** Within the organisation, only the reports officer and their deputies have access, from their designation (question 5) [Π-13].
- **Compliance centre and evidence pack.** They use only case dates and codes, never text or information about reporters (question 2) [Π-20].
- **IP addresses.** The web server keeps no access log of IP addresses (for Cloudflare, see question 6). Neither IP addresses nor the browser identifier (user agent) are stored in the database.
- **Surveys.** Multiple choice only, with answers stored without the employee's identity and without a timestamp.
- **Health-related leave.** There is no diagnosis field. No free-text comments are stored on the employee's request or on HR's recording of the period (for HR's note on the decision, see question 4).
- **Notifications.** Notifications on sensitive matters carry only generic text, and escalation messages only the case number.
- **Document search.** The computation is performed locally, with no third-party provider; only the relevant excerpts are sent to the AI provider.

Storage limitation (Article 5(1)(e) GDPR). This is a separate principle:

- **Retention period.** The organisation sets the retention period in the platform (default 24 months).
- **Automatic deletion.** At the end of the retention period, data is deleted automatically, by data category (for example conversations, Memory, closed reports and the audit log), with periods set by the organisation. Specific rules apply to reports (Articles 15(4) and 16 of Law 4990/2022): open cases are never deleted, and the reports officer can place a case on legal hold while an investigation or court proceedings are pending.
- **The employee's rights.** In addition, the employee can delete their Memory items themselves at any time, from the "What your assistant remembers" screen (question 4).
- **Backups.** Deleted data remains in the encrypted backups until the end of their cycle, about six months.

DPIA. For your organisation, carrying out a DPIA is mandatory (Article 35(1) and (4) GDPR; list in ΑΠΔΠΧ Decision 65/2018, Government Gazette B' 1622/10.5.2019: item 1.3 expressly names whistleblowing systems and is sufficient on its own; item 3.1, on AI applications, applies in combination with a criterion of the 1st or 2nd category). We support you in accordance with Article 28(3)(f) GDPR. Where appropriate, the views of workers' representatives are also sought (Article 35(9)). You can record completion of the DPIA in the compliance centre, with a date and supporting evidence.

Supporting documentation.

- Technical and Organisational Measures (Annex B3 on access, and B7 on backups, retention and deletion).
- Retention and deletion programme (annex to the DPA, with the contract proposal).
- DPIA support pack (with the contract proposal).
- Annex A4 (minimisation, storage limitation, data subjects' rights).

Related documents

Also available for download at hremia.eu:

1. **Legal & Technical Compliance Annex (English edition).** It contains:
   - section 0: scope, how to read the Annex, and the table of claim codes [n-n];
   - Part A (legal):
     - A1: legal framework;
     - A2: the matrix for Greece, article by article, for Law 4990/2022 and KYA 47312/2023;
     - A3: the matrix for Directive 2019/1937;
     - A4: GDPR;
     - A5: AI Act;
     - A6: allocation of responsibilities between the platform and the organisation, with a checklist;
   - Part B (technical): the technical and organisational measures (B1–B9) and the automated tests that verify them (B10). Part B also serves as the TOMs annex to the DPA;
   - Part C: answers to questions from legal departments, and the limits of the design together with what remains the organisation's responsibility.
2. **HRemia Client Brochure, 5th edition.** Its legal and technical claims carry claim codes [n-n] that refer to the Annex.

With the contract proposal we also send you:

- **Proposed DPA under Article 28 GDPR**, based on the SCCs between controllers and processors set out in Implementing Decision (EU) 2021/915, with its annexes:
  - description of the processing, including the data covered by Articles 9 and 10;
  - TOMs (Part B of the Annex);
  - sub-processor list: for each sub-processor, legal entity and registered office, place of processing, categories of data, processing agreement and retention period, and the mechanism for transfers outside the EEA, where there is a transfer (adequacy decision or SCCs in Implementing Decision (EU) 2021/914);
  - reporting channel;
  - AI functions (intended purpose and prohibited uses);
  - retention and deletion programme;
  - Greek country annex.
- **DPIA support pack:** data flows, table of legal bases, assessment of risks and measures, an employee-information template (Articles 13–14 GDPR) that also covers the AI assistant and Memory, and an explicit-consent template, if you choose that basis.
- **Transparency note on Regulation (EU) 2024/1689:** roles, intended purpose and prohibited uses, models and providers, the measures under Articles 4, 5 and 50, instructions for use.

For any clarification, we are available for a video conference with your legal department, your Data Protection Officer and your IT department: hello@hremia.eu.

The HRemia Team