Defensio SECaaS — Privacy Notice

Version 1.3 · in force from 31 July 2026 · supersedes v1.2 Issued under Regulation (EU) 2016/679 (GDPR), Articles 13 and 14.

1. Data Controller

Fidem S.r.l., Via Don G. B. Tessari 14/A, 37030 Lavagno (VR), Italy — VAT ID **IT04438280234**. Privacy contact: **info@defensio.technology**. Formal / certified correspondence on data-protection matters (PEC): **fidemsrl@pecitaly.eu**. **Data Protection Officer:** Fidem has assessed Art.37 GDPR and has **not designated a Data Protection Officer**, considering that the conditions of Art.37(1) are not met for its activities. Data-protection enquiries are handled by the contacts above. *(Note for internal review: because breach monitoring involves systematic monitoring of data subjects, this assessment should be revisited with counsel if the scale of that activity grows — see the DPIA.)*

2. Scope

This notice covers the **Defensio SECaaS application** (app.defensio.technology): external attack-surface scanning, vulnerability assessment, and data-leak (breach) monitoring. Cookies on the marketing sites are covered by the Cookie Policy.

3. Data, purposes and legal bases

Data	Purpose	Legal basis (Art.6)
Company name, contact person, work email (login), phone, billing address, country, VAT number	Provide the service, authenticate, invoice	Contract 6(1)(b)
Password (bcrypt hash)	Authentication	Contract 6(1)(b)
Consent records (document version + hash, IP, user-agent, timestamp)	Evidence of lawful consent and scanning authorisation	Legal obligation 6(1)(c) / legitimate interest 6(1)(f)
Monitored email addresses + breach	Alert the customer when a monitored address	Legitimate interest 6(1)(f); **the customer is**

Data	Purpose	Legal basis (Art.6)
metadata	appears in a known breach	**controller** and Fidem is **processor** for this activity (§8)
Scan targets and scan results (may incidentally include personal data exposed by the target)	Perform authorised security scanning	Contract 6(1)(b) / legitimate interest 6(1)(f)
Stripe customer/subscription/invoice IDs, amounts, status	Payments and tax	Contract 6(1)(b) / legal obligation 6(1)(c)
Security and audit logs (incl. signup attempts by IP)	Security, abuse prevention, auditability	Legitimate interest 6(1)(f) / legal obligation 6(1)(c)

We never store payment card data (Stripe-hosted checkout; PCI DSS SAQ-A).

Automated decision-making (Art.13(2)(f)/14(2)(g)): we make **no** solely-automated decisions producing legal or similarly significant effects. Data-leak monitoring is systematic monitoring of email addresses against external breach datasets; its output is an **informational alert to the customer**, not a decision about the monitored individual.

Legitimate interests (Art.13(1)(d)): a balancing test has been carried out and is available on request. The interests are: breach monitoring — enabling the customer to protect their organisation; scan results — delivering the assessment the customer requested; logs — platform security, integrity and lawful operation. You may object at any time (§9).

4. Breach-monitoring data (Art.14)

When a customer monitors an email address we query **Have I Been Pwned (HIBP)** and store breach **metadata only** — the categories of data are **breach source, title, date and occurrence count**. We do **not** store breached passwords or credentials. - **Source (Art.14(2)(f)):** HIBP, whose datasets derive from previously-disclosed, publicly-reported breach corpora. - Monitored individuals may be third parties who are not our users. The **customer decides** what is monitored and warrants entitlement to do so (VAPT Authorization Agreement); Fidem acts on the customer's instructions as **processor**. - **Notice to those**

individuals is the customer's responsibility as controller; Fidem relies on Art.14(5) where direct notice would involve disproportionate effort for data originating from public breach corpora.

5. Retention

- **Account data:** for the life of the account, then deleted, except accounting/invoice records retained **10 years** (Italian Civil Code art. 2220).
- **Scan and breach results:** while the subscription is active and the target/monitored address remains configured; deleted within **30 days** of the target or monitored address being removed, or of the subscription ending, whichever is earlier.
- **Raw payment-webhook payloads:** purged at **90 days** (IDs, status and timestamps retained).
- **Security/audit logs: 12 months**.
- Erasure requests are honoured across all systems (§9), except records we must keep by law.

6. Recipients and sub-processors (Art.28)

Application: - **Stripe Payments Europe** — payments, subscriptions, tax (EU; DPA via Stripe Services Agreement). - **my.host.it (Aruba group)** — hosting of the application and database (EU datacentre). - **Have I Been Pwned (HIBP)** — breach lookups (see §7 on transfers). - **Aruba SDI** — transmission of electronic invoices (company, VAT, contact details). - **Cloudflare Turnstile** — signup anti-abuse challenge (IP + token), once activated.

Marketing site (defensio.technology): **Google (Ireland/LLC)** — Google Analytics 4 only (no advertising or profiling), loaded **only after cookie consent** (Consent Mode v2, default denied); see the Cookie Policy. *(The former saas.defensio.technology site was retired on 31 July 2026.)*

We do not sell personal data.

7. International transfers

Application data is hosted in the EU. **Breach lookups transfer the monitored email address outside the EEA:** the address is sent to HIBP's breachedaccount endpoint to perform the search (HIBP's privacy-preserving k-anonymity mode applies only to password lookups, not to email searches, so the address itself must be disclosed to the provider). **HIBP is operated from outside the EEA and is not covered by an EU adequacy decision**, so this transfer requires an Art.46

safeguard (**Standard Contractual Clauses**). Fidem must have that safeguard in place with the provider; until it is, breach lookups are a documented transfer risk. Other sub-processors are EU-based or covered by their own adequacy/SCC arrangements.

8. Controller and processor roles

Fidem is **controller** for account, authentication, billing and platform-security data. For **what a customer scans or monitors** (targets, monitored email addresses and their results) the **customer is controller and Fidem is processor**, under the Data Processing Agreement in Schedule 1 of the Terms of Service.

9. Your rights (Art.15–22)

Access, rectification, erasure, restriction, portability, and **objection** (including to any processing based on legitimate interest). Where processing rests on **consent, you may withdraw it at any time** — withdrawal does not affect prior lawful processing. Requests: **info@defensio.technology** (or PEC **fidemsrl@pecitaly.eu**). We reply within one month, extendable by two further months for complex or numerous requests (we will tell you within the first month) (Art.12(3)). You may complain to the **Garante per la protezione dei dati personali** (garanteprivacy.it) or your local EU supervisory authority.

10. Security

TLS in transit; bcrypt-hashed passwords; strict per-tenant isolation; access on a least-privilege basis; encrypted database connectivity; monitoring, alerting and audit logging; documented incident response. Fidem's controls are **aligned with ISO/IEC 27001, 27017 and 27018**, with **CSA STAR Level 2 attestation targeted** (alignment does not itself constitute third-party certification).

11. Changes

This notice is versioned; material changes require renewed acceptance at next login. **Current version: 1.3.**