

Security Measures

Version 2.1, in force from 5 October 2026

OutLine Digital Agency (sole trader), Via Dalmazia 36, 76125 Trani (BT), Italy — VAT IT08978680729

How we protect your personnel data: separate workspaces, encryption, access control, change log, backups — including what we do not do yet.

Legal references

Regulation (EU) 2016/679 (GDPR), art. 32 (security of processing) ·
Regulation (EU) 2016/679 (GDPR), art. 25 (data protection by design and by default)

1. One database per workspace

This is the most important measure, and one that few cloud applications adopt because it costs more: **each workspace has its own database**, not a “customer” column inside shared tables.

The difference shows on the day something goes wrong. With shared tables, a query that misses the customer filter shows everyone’s data; here no such query exists, because other customers’ data lives in another database. The same goes for backups, which can be restored one workspace at a time without touching anyone else.

2. Encryption

What	How
Traffic to the website and the application	HTTPS with automatically renewed certificates. Unencrypted traffic is redirected.
User passwords	Never stored in readable form or with reversible encryption: only a hash computed with script , with a random salt for each user and constant-time comparison. Not even we can read them or tell you what they are.
Session tokens	The database keeps only a fingerprint of the token, never the value stored in the cookie.
Credentials of connected services (for example the API key of your e-signature provider) and the API key of your AI provider	Encrypted at rest with AES-256-GCM , using a key kept separate from the data. Someone who obtained a copy of the database would not obtain those credentials.
Codes of the speak-up channel	The code that lets a reporter follow up on a report is shown once and never stored: the database keeps only a fingerprint of it. A report has no field that links it to an employee.

The threat model, honestly

Encrypting credentials protects against database dumps and backups ending up where they should not — by far the most likely incident. It does not protect against a complete compromise of the server, where the key can still be read: that would need an external key-management service, which we do not use today. We would rather say so than let you assume otherwise.

3. Access control

- Sign-in with personal credentials — an email address, or the address the company assigns to the employee, and a password; repeated failed attempts are slowed down and blocked; sessions expire and can be ended.
- The session cookie is **HttpOnly** (cannot be read by scripts), **Secure** (sent only over encrypted connections) and **SameSite=Lax** (not sent with requests from other sites).

- **Roles and permissions:** owner, administrators, operators with permissions set module by module (for example a manager who sees only their own team), and employees, who see only their own data in the self-service area.
- **Restricted access to the most sensitive areas:** the reports of the speak-up channel can be opened only by the case handlers the account owner designates (by default, the owner alone) — not by administrators as such; every access to a report, including reading it, is recorded in the workspace's audit log; absence reasons marked as confidential are hidden from those who do not need them.
- **A log of changes to personnel data** — pay, contracts, balances, timesheets, documents, access — records who changed what and when. Entries can be added but not edited.
- Invitations sent to employees expire, and use a different code from the links for quick access without an account.
- Support access uses a **temporary user that expires after 15 minutes**, with administrator permissions for as long as it lasts; every access is logged with who, when, how long and why, the workspace owner is emailed as soon as it starts, and owners and administrators can read the log under Settings -> Support access; exports, downloads and credential changes are blocked during the access.
- A workspace's data can only be reached from within that workspace: there is no screen, not even for us, that shows the personnel data of several customers together.

4. Infrastructure

- Servers at IONOS SE in Germany, in the European Union.
- The database is not exposed to the internet: it listens only on the server itself.
- Private pages (the application, the admin console, onboarding, APIs) are excluded from search-engine indexing.
- Scheduled jobs run on an internal channel protected by a shared secret: without that secret the endpoint refuses every request instead of staying open.
- Outgoing calls to the webhooks of automation rules are restricted by default to public addresses, so that the service is not used to reach internal networks; an administrator of the workspace can change this restriction for its own rules.
- Operating-system and dependency updates are applied regularly; releases go through a verified build, not manual changes on the server.

5. Backups and restore

- **Daily** backup of all databases, compressed; the size of each copy is checked when it is made.
- **Rotation: 7 daily, 4 weekly and 3 monthly copies.** Older copies are deleted automatically.
- Copies are kept on the same European infrastructure, with permissions limited to the system user that produces them.
- Restores are **per workspace**: one customer can be rolled back without touching the others.
- Restores are carried out by hand. We undertake to test the procedure at least twice a year, on a copy: a backup that has never been restored is not a backup.

What this means for you

If you delete something important by mistake, the useful window for recovering it in daily detail is normally seven days. The sooner you write to us, the more likely we can recover everything: write to amministrazione@outlinedigital.it with the workspace name and, if you know it, when it happened.

6. How the software is written

- User input is validated before it is saved; database queries are parameterised and cannot be manipulated from outside.
- Operations that write data go through server-side actions with role checks: they cannot be reached by calling an address by hand.
- Links that work without signing in (kiosk, quick access for an employee) use **unguessable codes** that can be

revoked: regenerating a code immediately invalidates the previous one.

- Secrets are not in the code but in the server's environment variables.
- Before every release, automated checks verify that the features work and that configurations are consistent.

7. If something happens

Personal data breaches are notified to the customer **within 48 hours** of our becoming aware of them, with the information needed to assess notification to the authorities. The procedure is set out in section 6 of the Data Processing Agreement (<https://people.omegasuiteapp.com/legal/dpa>).

If you find a vulnerability, write to amministrazione@outlinedigital.it. We undertake to reply within 5 business days and not to take action against anyone who reports in good faith, without accessing other people's data, without degrading the service and without disclosing the problem before it is fixed.

8. What we do not do (yet)

A list of measures without its limits is advertising. These are the things that are **not** in place today, so that you know them before rather than after:

- **Two-factor authentication:** not available. Use a long password that you do not use elsewhere, and a password manager.
- **Encryption of the whole database at rest:** not enabled. Passwords and the credentials of connected services are protected; the rest of the data — including health data and bank details you record — is protected by access control and system isolation, not by encryption. The API key of an AI provider, if you enter one, is encrypted like the credentials of connected services.
- **Certifications** (ISO/IEC 27001, SOC 2): we have none. We do not claim standards we have not been audited against.
- **IP address restrictions and a per-user sign-in log visible to the customer:** not available.
- **Backups of files, and copies kept elsewhere:** not in place. The backups cover the databases; they are kept on the same server, protected by file permissions and not encrypted, and no copy is kept at another site. The files you upload — attachments, documents — are stored on the server and are not part of the backups: keep your own copy of the files you could not afford to lose.
- **Separate database credentials for each workspace:** not in place. Each workspace has its own database, but the application reaches all of them with the same database account.

When one of these is implemented, it will move to the sections above and the version of this document will go up.

9. Your part

At least half of the security of HR software is decided outside the software:

- use strong passwords and do not reuse those of other services;
- create one user per person: shared accounts make it impossible to know who did what;
- grant the minimum permissions needed — few people need to see pay, health data or disciplinary records — and **remove access immediately** when someone leaves;
- designate one or two trusted people as case handlers of the speak-up channel (Settings -> Speak-up channel) and nobody else;
- regenerate kiosk and quick-access links if you suspect they have circulated, and remove kiosk devices you no longer use;
- keep the devices you sign in from up to date;
- export regularly the data you could not afford to lose.

The current full text is always available at <https://people.omegasuiteapp.com/legal/security?lang=en>. For any question: amministrazione@outlinedigital.it.