

Data Processing Agreement

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 process, as your processor, the personal data of your employees, candidates and other staff that you put in Omega People: what we may do with it, what we may not, and how transfers are covered.

Legal references

Regulation (EU) 2016/679 (GDPR), art. 28 and Chapter V · Commission Implementing Decision (EU) 2021/914 (standard contractual clauses) · UK GDPR and the International Data Transfer Addendum to the EU standard contractual clauses · Swiss Federal Act on Data Protection (nFADP), arts. 9 and 16 · California Consumer Privacy Act (CCPA) and other US state privacy laws, where applicable · Canada: PIPEDA; Québec: Act respecting the protection of personal information in the private sector, ss. 17 and 18.3; Alberta and British Columbia: Personal Information Protection Acts · Australia: Privacy Act 1988, Australian Privacy Principles 8 and 11 and Part IIIC (notifiable data breaches) · New Zealand: Privacy Act 2020, s. 11 and information privacy principles 5 and 12

Preamble

This Agreement supplements the Terms of Service (<https://people.omegasuiteapp.com/legal/terms>) and governs the processing of personal data that OutLine Digital Agency (**the Processor**) carries out on behalf of the customer (**the Controller**) in providing Omega People.

It constitutes the contract required by GDPR art. 28(3) and, where the Controller is subject to them, by art. 28 of the UK GDPR, art. 9 of the Swiss Federal Act on Data Protection, section 18.3 of Québec's Act respecting the protection of personal information in the private sector, and the US state privacy laws that require a written contract with a service provider or processor. It is concluded when the Controller accepts it on opening its first workspace and remains in force for as long as the Processor processes personal data on the Controller's behalf.

Processor	OutLine Digital Agency (sole trader), Via Dalmazia 36, 76125 Trani (BT), Italy — VAT IT08978680729
Controller	The customer, as identified in the account and in the business details entered in the application.
Privacy contact	amministrazione@outlinedigital.it

Terms such as “personal data”, “processing”, “controller”, “processor” and “personal data breach” have the meaning given in the GDPR; where another law applies, they include the equivalent terms of that law (for example “business” and “service provider” under the CCPA).

Who decides what

The Controller is the employer. It decides which data to collect about its employees, candidates and other staff, for what purposes, on which legal basis and for how long, and it is the Controller that informs them (its own staff privacy notice). The Processor provides the tool and makes none of those decisions. This means the Processor cannot delete data at the request of an individual, and the Controller cannot shift onto the Processor the choice of collecting data it should not have collected.

1. Processing on documented instructions

1. The Processor processes personal data **only on the Controller's documented instructions**. These are: this

Agreement, the Terms of Service, the service documentation, and the settings the Controller configures in the application (users, roles and permissions, the modules it switches on, clock-in and location rules, public pages, integrations, retention periods).

2. The Processor does not process the data for its own purposes, does not disclose it to third parties, does not use it for commercial analysis or to train artificial-intelligence systems.
3. If a legal obligation requires the Processor to carry out further processing, it informs the Controller before doing so, unless the law prohibits this on important grounds of public interest.
4. The Processor immediately informs the Controller if, in its opinion, an instruction infringes data protection law.

2. Confidentiality of authorised persons

The Processor ensures that the persons authorised to process the data — staff and contractors — are bound by a duty of confidentiality that survives the end of their engagement, receive instructions, and have access only to the data they need for their task.

Support staff access customer workspaces only through the **logged temporary access** described in section 8.

3. Security measures

The Processor implements the technical and organisational measures described in **Annex B** and on the Security Measures (<https://people.omegasuiteapp.com/legal/security>) page, which form part of this Agreement.

The measures may be updated over time provided that the level of security is not reduced. Material changes are notified to the Controller with the same notice period as for sub-processors.

4. Sub-processors

The Controller gives the Processor **general authorisation** to engage other processors, on the following conditions.

1. The current list is published on the Sub-processors (<https://people.omegasuiteapp.com/legal/subprocessors>) page.
2. Each sub-processor is bound by contract to data protection obligations equivalent to those of this Agreement; the Processor remains liable for their performance as for its own.
3. The addition or replacement of a sub-processor is notified to the Controller at least **30 days** in advance, by email and prominently in the application.
4. Within that period the Controller may object on reasonable, documented data protection grounds. If it objects, the parties look in good faith for an alternative; if none is practicable, the Controller may terminate without penalty with effect from the date of the change.

Sub-processor	Activity	Country
IONOS SE	Servers and storage: hosts the application, the workspace databases, uploaded files (employee documents, payslips, receipts, attachments) and backups.	Germany
Aruba S.p.A.	Relays the service's outgoing email: invitations to employees and team members, password resets, messages to job candidates, emails sent by the automation rules the customer sets up, and subscription emails. Messages contain the recipient's name and email address and the content of the message.	Italy

Stripe Payments Europe, Limited

Collects subscription payments and issues receipts. It processes only the billing details of the subscriber (company name, address, VAT number, billing email, card details — which never pass through our servers). With them it receives the name of the workspace, the sign-in email address of its owner and our internal reference numbers. It has no access to the data stored in workspaces.

Ireland

The authoritative version is the one kept up to date at </legal/subprocessors>

(<https://people.omegasuiteapp.com/legal/subprocessors>): this table is a courtesy copy as at the date this document was generated.

Services you connect are not our sub-processors

If the Controller connects Omega People to other services — an e-signature provider (Yousign) with its own account and API key, an artificial-intelligence provider with its own key, or webhooks called by its automation rules — the data sent to them goes there on the Controller's instruction and under the Controller's contract with that provider. Those providers are the Controller's processors, not the Processor's sub-processors. In the application, under **Settings -> Privacy and compliance**, the Controller finds its record of processing already filled in, the list of the services it has connected and the privacy notices for its employees and candidates.

5. Assistance with data subject requests

The application gives the Controller the tools to answer the requests of its employees, former employees and candidates itself, without waiting for anyone: search, export of all the data held about one employee, rectification, deletion, and a log of changes to personnel data. Employees with self-service access can see their own attendance, leave, shifts, documents and payslips directly.

If an employee, candidate or other data subject contacts the Processor directly, the Processor **does not act** on the request and forwards it to the Controller without delay, telling the individual that the controller is their employer (or the company they applied to).

Where the application's tools are not enough, the Processor provides reasonable technical assistance, at its own cost if the need arises from a malfunction.

6. Personal data breaches

1. The Processor notifies the Controller **without undue delay and in any event within 48 hours** of becoming aware of a personal data breach affecting the data processed on its behalf, and aims to do so within 24 hours. A first notice is given even when not all the information is available yet; the rest follows in stages, as it becomes known.
2. The notification describes the nature of the breach, the categories and approximate number of individuals and records concerned, the likely consequences and the measures taken or proposed, so that the Controller can assess whether and when to notify the competent authorities and individuals within the deadlines of the law that applies to it (for example 72 hours under the GDPR and UK GDPR, or "as soon as possible" or "as soon as practicable" under the Swiss nFADP, PIPEDA and the Australian and New Zealand schemes).
3. The Processor documents every breach and gives the Controller the cooperation it needs to meet its obligations towards authorities and individuals.
4. Notifying authorities and individuals remains the Controller's responsibility: the Processor does not do so on its behalf.

7. Impact assessments and prior consultation

Taking into account the nature of the processing and the information available to it, the Processor assists the

Controller with data protection impact assessments and any prior consultation of an authority, by providing technical documentation on the architecture, the security measures and the data flows of the service.

When an impact assessment is worth doing

HR software processes data about people who depend on the Controller for their living, and several features of Omega People deserve attention: **clock-in with geolocation**, which records where an employee is when they clock in or out; **health data** in sick-leave certificates, medical-check records and incident reports; **performance reviews and disciplinary records**; the **speak-up channel**; and any use of **AI features** on employee data. In many countries these are also regulated by employment and workplace-monitoring law (informing staff in advance, consulting employee representatives or a works council). The application points this out under **Settings -> Privacy and compliance**, but the assessment is carried out by the Controller.

8. Support access to the workspace

- It takes place only at the Controller's request, or for technical work needed to keep the service running or to fix a fault.
- It uses a **dedicated temporary access** created inside the workspace that expires automatically after **15 minutes**: it neither uses nor knows the credentials of the Controller's users.
- While it lasts, that access has the permissions of an administrator of the workspace: this is what makes it possible to see a problem as the Controller sees it. The person who uses it is bound by confidentiality (section 2) and looks only at what the request requires.
- It is **recorded and visible to the Controller**: each access is logged with who opened it, when, for how long and why; the Controller's account owner receives an email as soon as it starts, and the Controller's owners and administrators can consult the log at any time under Settings -> Support access. During the access, exports, file downloads and changes to passwords, sign-in addresses and API keys are blocked, and any attempt is shown in the log.

9. Audits and demonstrating compliance

The Processor makes available to the Controller all information necessary to demonstrate compliance with this Agreement and allows audits, including inspections, by the Controller or an auditor it appoints.

1. Audits require at least 15 days' notice, take place during business hours and must not affect the continuity of the service or the confidentiality of other customers' data.
2. **One audit per calendar year** is allowed, plus further audits after a personal data breach or at the reasoned request of a supervisory authority.
3. The Controller's auditor must not be a competitor of the Processor and must sign a confidentiality undertaking.
4. The cost of additional audits requested by the Controller is borne by the Controller, unless the audit reveals a breach by the Processor.

The Processor keeps a record of the processing it carries out on the Controller's behalf (GDPR art. 30(2)) and cooperates, on request, with the supervisory authorities in the performance of their tasks.

10. International transfers

The Processor processes the data within the European Economic Area: the infrastructure is hosted by IONOS SE in Germany, and its sub-processors are in the European Union. **It does not transfer the data to third countries**, except to make it available to the Controller and its users wherever they are.

1. **From the EU to the Controller.** Where the GDPR applies to making data available to a Controller that is not covered, for that data, by an EU adequacy decision, the parties agree the EU standard contractual clauses (Commission Implementing Decision (EU) 2021/914), **Module Four** (processor to controller), which are incorporated into this Agreement by reference. Article 23 of the Terms of Service determines the governing law and courts; the details of the processing are those in Annex A. For those clauses: the docking clause (clause 7) does not apply; clauses 14 and 15 apply only if the Processor combines the data received from the Controller

with personal data it has collected in the European Union, which it does not do; Italian law governs them (clause 17) and the courts of Italy have jurisdiction (clause 18); the parties are those named in the preamble and Annex I is Annex A to this Agreement. Making data available to a Controller in the United Kingdom, Switzerland or New Zealand relies on the European Commission's adequacy decisions for those countries, for as long as they remain in force; the same holds for a Controller in Canada to the extent that PIPEDA applies to the data concerned, and for a Controller in the United States to the extent that it is certified under the EU-U.S. Data Privacy Framework for that data. In every other case Module Four applies.

2. **United Kingdom.** For a Controller subject to the UK GDPR, transfers to the Processor rely on the UK's adequacy regulations for the European Economic Area. Should these cease to apply, the parties agree the EU standard contractual clauses (Module Two) together with the **UK International Data Transfer Addendum** issued by the Information Commissioner, incorporated by reference.
3. **Switzerland.** For a Controller subject to the Swiss nFADP, transfers to the Processor rely on the Federal Council's recognition of the adequacy of the countries concerned. Should this cease to apply, the parties agree the EU standard contractual clauses with the adaptations required for Switzerland: the FDPIC is the competent supervisory authority for transfers under Swiss law, and "Member State" includes Switzerland for the purpose of individuals' rights.
4. If a transfer outside the EEA ever becomes necessary for a sub-processor, the Processor gives notice under section 4 and makes it only with one of the safeguards of Chapter V of the GDPR, stating it in the sub-processor list.
5. Transfers resulting from services connected by the Controller (for example an AI provider or an e-signature provider established outside the EEA) are made under the Controller's responsibility.
6. **Requests from authorities.** If a court or public authority asks the Processor for access to the Controller's data, the Processor checks that the request is lawful, contests it where there are reasonable grounds to do so, hands over only what is strictly required and, unless the law forbids it, tells the Controller beforehand.

11. United States: service-provider terms

Where the Controller is a "business" subject to the California Consumer Privacy Act (CCPA) or a "controller" subject to another US state privacy law, the Processor acts as its **service provider** (or processor). The Controller discloses the personal information to the Processor only for the limited and specified business purpose of providing the service described in Annex A, and the Processor:

- does not sell or share the personal information, and does not use it for cross-context behavioural or targeted advertising;
- does not retain, use or disclose it for any purpose — including a commercial purpose — other than providing the service under the contract, nor outside the direct business relationship with the Controller;
- does not combine it with personal information that it receives from another source or collects from its own dealings with the individual, except as those laws allow a service provider to do;
- complies with the obligations those laws place on service providers and processors, and gives the personal information the level of privacy protection they require, including the security measures in Annex B;
- notifies the Controller **within five business days** if it determines that it can no longer meet those obligations;
- lets the Controller take reasonable and appropriate steps to make sure that the information is used consistently with the Controller's own obligations (sections 3 and 9) and, on notice, to stop and remedy any unauthorised use;
- helps the Controller answer the requests of individuals (section 5), and binds its sub-processors, by written contract, to the same obligations (section 4);
- keeps the information confidential, and deletes or returns it when the service ends (section 13).

No protected health information, no biometric identifiers. The Processor is not a "business associate" under HIPAA and has not signed a business associate agreement: the service must not be used to hold the protected health information of a health plan or of a health-care provider. Records that an employer keeps in its role as employer — a sick-leave certificate, a fitness-for-work note — are not protected health information; the confidentiality

rules for employees' medical records (for example under the ADA, the FMLA and GINA) are for the Controller to apply, using the access permissions of the service. The service does not collect fingerprints, scans of face or hand geometry, voiceprints or other biometric identifiers — the camera is used only to read a QR code and to photograph documents — and the Controller must not upload any.

Security incidents. Section 6 also covers the notice that US state laws require from a company that maintains data on behalf of its owner.

12. Canada, Australia and New Zealand

For a Controller subject to one of the laws below, the Processor processes the data only to provide the service, protects it with the safeguards described in this Agreement and assists the Controller as described in sections 5 to 9. In addition:

Canada (PIPEDA, and the Personal Information Protection Acts of Alberta and British Columbia)

The Controller remains accountable for the personal information it entrusts to the Processor for processing. The Processor uses it only for the purposes of the service, gives it protection comparable to that which the Controller must provide, and tells the Controller under section 6 of any breach of security safeguards, so that the Controller can assess whether there is a real risk of significant harm, report it and keep its record of breaches. **The information is stored and processed outside Canada** — in the countries shown in the sub-processor list (<https://people.omegasuiteapp.com/legal/subprocessors>) — where it is subject to the law of those countries and may be accessed by their courts and authorities under that law; telling the individuals so, and naming those countries where the law requires it (as in Alberta), is the Controller's responsibility.

Québec

This Agreement is the written contract required by section 18.3 of the Act respecting the protection of personal information in the private sector. The Processor uses the personal information only to carry out the service; applies the measures in Annex B to protect its confidentiality; does not keep it after the contract has ended (section 13); notifies the Controller's person in charge of the protection of personal information **without delay of any violation or attempted violation**, by any person, of an obligation concerning the confidentiality of the information; and allows that person to carry out any verification relating to confidentiality (section 9). Before information is communicated outside Québec, the Controller must carry out the privacy impact assessment required by section 17 of that Act: the Processor gives it the information it needs — where the data is stored, who the sub-processors are, the security measures, and the legal framework that applies in the European Union.

Australia	The Controller keeps effective control of the personal information: it decides who may access it and can access, change, retrieve and delete it at any time; the Processor handles it only to store it and make it available to the Controller and its users, and binds its sub-processors to the same obligations. On that basis, providing the information to the Processor is intended to be a <i>use</i> by the Controller rather than a <i>disclosure</i> for the purposes of Australian Privacy Principle 8; whether it is one is for the Controller to assess. If the Processor has reasonable grounds to suspect unauthorised access to the information, its unauthorised disclosure or its loss, it notifies the Controller under section 6, so that the Controller can complete its assessment within the 30 days that the Notifiable Data Breaches scheme allows; the parties agree that any notification to the Office of the Australian Information Commissioner and to individuals is made by the Controller.
New Zealand	The Processor holds the personal information as the Controller's agent, for safe custody and processing, and does not use or disclose it for its own purposes: under section 11 of the Privacy Act 2020 the information is treated as held by the Controller, which remains responsible for it, and sending it to the Processor is not a disclosure outside New Zealand under information privacy principle 12. The Processor notifies privacy breaches under section 6, so that the Controller can notify the Privacy Commissioner and the people affected as soon as practicable where serious harm is likely.

13. What happens at the end

1. The Controller can export the data itself, in open formats, throughout the relationship.
2. When the contract ends, the workspace remains accessible in read-only mode for **30 days**, to allow export.
3. After that period the Processor **deletes** the personal data without undue delay, and in any case within the following 30 days; copies in backups cease to exist as the rotation runs its course, at the latest about three months after the deletion. Data is kept longer only where EU or Member State law requires it.
4. On request, the Processor confirms deletion in writing.
5. Statutory retention of employment, payroll, working-time and health-and-safety records is an obligation of the Controller as employer: the Controller exports what it must keep before the export window closes. The Processor does not act as the Controller's archive after the contract ends.

14. Order of precedence

In case of conflict, the standard contractual clauses (where they apply) prevail over this Agreement, and this Agreement prevails over the Terms of Service as regards personal data. Liability is governed by the Terms of Service.

Annex A — Details of the processing

Subject matter	Provision of an online human-resources management service: personnel records, time and attendance, shifts, leave and absences, documents and e-signature, expenses, payroll preparation, recruiting, training, health and safety, performance reviews, speak-up channel, internal communication.
Duration	The term of the service contract, plus the 30-day export window.

Retention during the term	Data is kept for as long as the Controller keeps it in the workspace. The Controller decides the retention periods and deletes records itself (for example former employees, unsuccessful candidates, closed speak-up reports, for which an automatic clean-up after a period chosen by the Controller can be switched on). During the term the Processor deletes workspace data on its own initiative only in the cases the application provides for and the Controller can adjust: applications of unsuccessful candidates are deleted after the period set in the recruiting settings (12 months by default), and registrations of mobile devices that have not been used for 180 days are removed.
Nature and purpose	Collection, recording, organisation, structuring, storage, retrieval, consultation, transmission to the services configured by the Controller, erasure — solely to run the application as the Controller has configured it.
Frequency	Continuous, for as long as the service is used.

Categories of data subjects — depending on how the Controller uses the service:

- employees, workers, apprentices, trainees and other staff of the Controller, including **former staff** whose records the Controller keeps;
- **job candidates** who apply through the Controller's careers page or whom the Controller enters;
- contractors, agency workers and other people the Controller manages in the workspace;
- the Controller's owners, administrators and managers who use the service;
- **emergency contacts** indicated by employees, and family members where the Controller records them (for example in documents supporting family-related leave);
- people who send a report through the speak-up channel (who may remain anonymous) and people named in a report;
- other people named in documents, messages, expense claims, incident reports and notes.

Categories of personal data:

Category	Examples	Where it appears
Identification and contact data	name, date and place of birth, gender, home address, email address, phone number, emergency contact	Employee records, self-service area
Official identifiers	national insurance, social-security or tax numbers, identity-document number and expiry date	Employee records, onboarding
Employment data	job title, department, site, manager, contract type and dates, probation, notice, termination date and reason, skills, equipment assigned	Employee records, contracts, org chart, equipment
Pay and financial data	salary and pay items, bank account details, expenses and reimbursements, benefits, payslips uploaded by the Controller	Payroll preparation, expenses, benefits, documents
Working-time data	clock-in and clock-out times, timesheets, shifts, availability, overtime, on-call duty, hours by project	Attendance, shift planning, projects

Location data	the position of the device at the moment of clocking in or out (coordinates, accuracy, whether it is inside the area set for the site), only if the Controller switches on location for clock-ins. There is no continuous tracking.	Attendance
Leave and absence data	type, dates and reason of absences, balances, supporting documents	Leave and absences
Performance and development data	reviews, self-assessments, goals, training attended and certificates, survey answers (anonymous where the Controller sets them so)	Performance, training, surveys
Disciplinary data	allegations, the employee's reply, outcome	Employee records
Candidate data	name, contact details, CV and covering message, stage of the selection, notes and rating	Recruiting, careers page
Speak-up reports	content of the report and of the follow-up messages, attachments, names of the people concerned. The reporter is not identified by the system: access to the follow-up is by a code shown once, of which only a fingerprint is stored.	Speak-up channel
Documents and free text	contracts, signed documents, certificates, letters, messages in the team chat, announcements and comments, files in the shared storage	Documents, chat, announcements, storage
Usage and security data	sign-ins, sessions, devices registered for the mobile app or the kiosk, log of changes to personnel data	Activity and audit logs
Special categories (GDPR art. 9) and similar sensitive data	health data (sick-leave certificates and reasons for absence, occupational-health checks with their outcome and restrictions, workplace accidents and injuries); data that may reveal trade-union membership (absences for union activity or strikes); any other sensitive data — for example about religion, ethnic origin, disability or criminal records — that the Controller chooses to record or that appears in the documents it uploads	Leave and absences, health and safety, documents, payroll preparation

Special categories: the Controller decides, and answers for it

An HR system holds special categories of data by its nature. Whether to record them, on which legal basis (for example the employer's obligations under employment, social-security and health-and-safety law), who may see them and for how long is decided by the Controller, which is responsible for keeping them to the minimum necessary: record that an employee is unfit or absent, not the diagnosis, wherever the law does not require more. The Processor does not ask for, read or use this data for any purpose other than storing it and showing it to the users the Controller has authorised.

Annex B — Security measures

The technical and organisational measures adopted by the Processor are described in full on the Security Measures (<https://people.omegasuiteapp.com/legal/security>) page, which forms part of this Agreement. In brief: a separate database for each workspace, encryption of traffic in transit, encryption at rest of the credentials of connected services and of the API key of an AI provider, passwords stored only as a hash, role- and permission-based access control, with speak-up reports restricted to case handlers designated by the Controller's account owner and every access to them logged, an append-only log of changes to personnel data, temporary and logged support access, daily backups of the databases, event logging.

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