

Privacy Policy

Version 2.1, in force from 5 October 2026

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

What personal data we collect when you visit the website or open an Omega People account, why, for how long, and what you can ask us. If you are an employee of a company that uses Omega People, your employer is responsible for your data.

Legal references

Regulation (EU) 2016/679 (GDPR), arts. 13 and 14 · United Kingdom: UK GDPR, Data Protection Act 2018 (including s. 164A on complaints) and Data (Use and Access) Act 2025 · Switzerland: Federal Act on Data Protection (FADP), arts. 19 and 25 · Canada: PIPEDA; Québec: Act respecting the protection of personal information in the private sector (Law 25); Alberta and British Columbia: Personal Information Protection Acts · Australia: Privacy Act 1988 and Australian Privacy Principles 1, 5, 8, 12 and 13 · New Zealand: Privacy Act 2020, information privacy principles 3, 6 and 7 · United States: state privacy laws, including the California Consumer Privacy Act (CCPA), where applicable · Apple App Store Review Guidelines, 5.1.1; Google Play User Data policy

In short

This policy covers **the website and the Omega People account of the business that subscribes**. It does not cover the data a business puts inside its workspaces — the records of its employees, candidates and other staff: that data belongs to the business, which decides about it, and we process it only on its instructions — see the Data Processing Agreement (<https://people.omegasuiteapp.com/legal/dpa>).

Are you an employee or a candidate?

If your employer uses Omega People — or you applied for a job through a careers page built with it — **your employer (or the company you applied to) is the controller of your data**, not us. It decides what is recorded about you and for how long, and it is the one to ask if you want to see, correct or delete your data. Its own privacy notice tells you how; we act only as its processor.

- Your data is stored on servers of IONOS SE in **Germany**, in the European Union. Only subscription payment data handled by Stripe may also be processed in the United States (see section 6).
- We use no advertising or profiling cookies, no third-party analytics, and we do not sell or rent personal data to anyone.
- Every workspace lives in its **own separate database**: there is no shared table containing all customers' data.
- You can ask us at any time to see, correct or delete your data by writing to amministrazione@outlinedigital.it.

1. Who is responsible for your data

The controller is **OutLine Digital Agency**, which provides the service under the brand Omega People.

Controller	OutLine Digital Agency (sole trader), Via Dalmazia 36, 76125 Trani (BT), Italy — VAT IT08978680729
Registered office	Via Dalmazia 36, 76125 Trani (BT), Italy
Privacy contact	amministrazione@outlinedigital.it
General contact	amministrazione@outlinedigital.it · +39 327 609 2869

Data protection officer	Not appointed. The conditions of GDPR art. 37 are not met: processing personal data is not our core activity, it is not carried out on a large scale and it does not involve regular and systematic monitoring of individuals. Privacy requests go to the contact above.
Representatives	We are established in the European Union, so we need no representative there. We have not appointed a representative in the United Kingdom (UK GDPR art. 27). We have not appointed a representative in Switzerland: the conditions of art. 14 of the Federal Act on Data Protection (large-scale, regular and high-risk processing as a controller) are not met. You can always contact us directly at amministrazione@outlinedigital.it , in English, German or French.

2. Two different roles

We process personal data in two situations that the law keeps separate. Which one applies decides whom you should contact.

1. **We are the controller** when you visit the website, open an account, subscribe, or write to us for support. Here we decide what to collect and why: this is what this policy describes.
2. **We are a processor** (or *service provider*) when a business uses Omega People to manage its staff: employee records, attendance, leave, documents, payroll preparation, recruiting and everything else it keeps in its workspace. There the business — the employer — is the controller, not us: we provide the software and process that data only to run it, following the employer's instructions. If you are an employee, former employee, candidate or contractor of a business that uses Omega People, **your requests go to that business**, which is the only one that can decide about your data.

A concrete example

If your employer keeps your clock-ins, leave requests and payslips in Omega People, or a company receives the application you sent through its careers page, the controller of that data is that company. We cannot show you or delete those records at your request — and we must not be able to: it would mean accessing a customer's personnel data without its instruction. If you write to us, we tell you so and pass your request on to the company.

3. What we collect and why

Data	Purpose	Legal basis (GDPR)	Retention
First and last name, email address, password (stored only as a hash, never in readable form), preferred language — for every person who signs in, including employees whom their employer has given self-service access	Creating your account, signing you in, linking you to the workspaces you belong to	Performance of a contract — art. 6(1)(b)	Until the account is deleted — at your request, or together with the workspace — and for no more than 30 days after that
Name of the business, country, time zone, answers given during onboarding	Setting up the workspace for your organisation	Performance of a contract — art. 6(1)(b)	As long as the workspace exists

IP address, browser type, date and time of access, pages served; the version and platform of the mobile app, if you use it; the IP address from which a password reset is requested	Running the website, protecting it from abuse and intrusion, investigating incidents	Legitimate interest in security — art. 6(1)(f); recital 49	12 months
Acceptance of terms and policies: document, version, date, IP address, browser	Being able to prove when you accepted what	Legal obligation of accountability — arts. 5(2) and 7(1); performance of a contract	10 years after the contract ends
Billing details: company name, VAT or tax number, address, billing email	Issuing and keeping invoices	Legal obligation — art. 6(1)(c) (tax and accounting law that applies to us)	10 years
Subscription and payment data: plan, amounts, dates and outcome of charges, refunds, type and last four digits of the payment method (never the full number, which only Stripe sees)	Collecting fees, handling renewals, cancellations, the money-back guarantee and refunds, defending ourselves in a dispute	Performance of a contract — art. 6(1)(b); legal obligation — art. 6(1)(c); legitimate interest in defending legal claims — art. 6(1)(f)	10 years after the contract ends
Contract sent as a PDF, its digital fingerprint and the record of sending	Giving you the contract on a durable medium and being able to prove what was agreed	Performance of a contract — art. 6(1)(b); legal obligation — art. 6(1)(c)	10 years after the contract ends
Messages you send us for support and our replies	Answering and keeping track of what was done	Performance of a contract — art. 6(1)(b)	24 months after the request is closed
Log of support access to your workspace	Being able to show you who entered, when and for how long	Legitimate interest in accountability; contractual obligation towards you	24 months

Where a period in the table has ended, the data is deleted at our next periodic review — which we carry out at least every six months — unless a legal obligation or a pending dispute requires us to keep it longer.

What we do not do

We do not profile users, we do not take automated decisions that produce legal effects on you (GDPR art. 22), we do not use your data to train artificial-intelligence models, we do not do behavioural advertising, and we neither buy nor sell lists.

4. When we enter your workspace

To solve a problem, our support may need to see the application as you see it. This access is not a permanent privilege and does not use your credentials:

- it happens only when you ask for help, or when a fault in the service has to be fixed;
- a **dedicated temporary access** is created inside your workspace and expires on its own after 15 minutes;
- while it lasts it has the permissions of an administrator of the workspace — which is what lets us see the problem as you see it — so the person who uses it looks only at what your request requires;
- every access is recorded with who opened it, when, for how long and why; the owner of the workspace receives an email as soon as it starts, and 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.

Anyone who uses this access is bound by a duty of confidentiality. What they see inside a workspace is the

employer's data, processed under the Data Processing Agreement (<https://people.omegasuiteapp.com/legal/dpa>).

5. Who we share data with

We do not disclose or transfer data to third parties for their own purposes. Only authorised staff of OutLine Digital Agency, bound by confidentiality, and the providers we need to run the service, engaged as processors, can access it.

The complete and current list of providers that process data contained in your workspaces is on the Sub-processors (<https://people.omegasuiteapp.com/legal/subprocessors>) page.

To **collect subscription fees** we use **Stripe Payments Europe, Limited** (Dublin, Ireland), which receives the data needed for payment — name, email, billing address, VAT number and payment-method details — and processes it partly as our processor and partly as an **independent controller** for its anti-money-laundering, anti-fraud and regulatory obligations, under its own privacy policy (stripe.com/privacy). **Service emails** — contract, receipts, trial and renewal notices — are sent from our mailbox and relayed by Aruba S.p.A. (Italy).

Together with those details Stripe receives the name of the workspace, the sign-in email address of its owner, the language of the account and our internal reference numbers, so that each payment can be matched to its subscription.

We may also disclose data to courts or regulators where the law requires it. In that case, unless an order forbids it, we tell you.

6. Where your data is stored and international transfers

The infrastructure is entirely in the European Union: servers of IONOS SE in Germany. Our service providers are in Germany, Italy and Ireland. **The data in your workspaces and your account is not transferred outside the European Economic Area by us.**

The one exception concerns subscription **payment data**: Stripe may also process it through Stripe, Inc. (United States), which participates in the EU-U.S. Data Privacy Framework, on the basis of the European Commission's adequacy decision of 10 July 2023 (GDPR art. 45) and, as a fallback, the standard contractual clauses (GDPR art. 46).

Our customers are outside the European Union, so personal data travels **from your country to the EU** when you use the service, and back to you when you access it. The United Kingdom and Switzerland recognise the EU as providing an adequate level of protection; the European Commission, for its part, has recognised the United Kingdom, Switzerland, New Zealand and — for organisations subject to PIPEDA — Canada. For everyone else we protect the data according to the GDPR, which gives a level of protection at least comparable to that of your local law; where the law requires an instrument for sending an organisation's data back to it, the Data Processing Agreement (<https://people.omegasuiteapp.com/legal/dpa>) provides one. In the countries where your data is processed — Germany, Italy and Ireland and, for payment data, the United States — courts and public authorities can obtain access to it in the cases, and with the safeguards, that their law provides.

Services you connect yourself

If you connect external services to Omega People — an e-signature provider (Yousign) with your own account, an artificial-intelligence provider with your own key, or webhooks called by your automation rules — the data you choose to send goes to them under the terms of your own contract with that provider, and may leave the EEA. Choosing and checking those providers is your responsibility.

Maps use the public services of **OpenStreetMap**: when an administrator asks the application to locate a site, the **address of the site** is sent to OpenStreetMap's search service (Nominatim); when an administrator views or adjusts the position of a site, the map images are loaded by their browser directly from OpenStreetMap's servers, which therefore see that browser's IP address; and a manager who chooses to view the position of a clock-in on the map opens openstreetmap.org at those coordinates, with no name attached. OpenStreetMap is operated by the OpenStreetMap Foundation (United Kingdom) under its own privacy policy.

7. How we protect it

Technical and organisational measures are described in full on the Security Measures (<https://people.omegasuiteapp.com/legal/security>) page. In brief: traffic encrypted in transit, passwords stored only as a hash with a strong algorithm, credentials of connected services encrypted at rest, **a separate database for each workspace**, role-based permissions, a log of changes to personnel data, logged and time-limited support access, daily backups.

8. Your rights

These rights concern the data for which we are the controller (section 3). For the data your employer keeps about you in its workspace, contact your employer. You can exercise your rights at any time by writing to **amministrazione@outlinedigital.it**. We reply within one month, which may be extended by two further months for complex requests (GDPR art. 12(3)), free of charge unless a request is manifestly unfounded or excessive. We may need to verify your identity before acting.

- **Access** (art. 15): find out what data we hold and get a copy.
- **Rectification** (art. 16): have inaccurate or incomplete data corrected.
- **Erasure** (art. 17): have it deleted, where we are not legally required to keep it.
- **Restriction** (art. 18): have it frozen instead of deleted, for example while you contest its accuracy.
- **Portability** (art. 20): receive it in a machine-readable format. The owner and the administrators of a workspace can export all of its data themselves, whenever they like.
- **Objection** (art. 21): object to processing based on legitimate interest, explaining your situation.

As we are established in Italy, our lead supervisory authority is the **Italian Data Protection Authority** (Garante per la protezione dei dati personali, Piazza Venezia 11, 00187 Rome, Italy — [gpdp.it](https://www.gpdp.it) (<https://www.gpdp.it>)). You can also complain to the authority of your own country, listed in the next section.

If you are unhappy with the way we have handled your data or a request, tell us at **amministrazione@outlinedigital.it**: we acknowledge every complaint within 30 days, look into it and tell you the outcome.

9. Notes for your country

The GDPR applies to everything we do, wherever you are. The law of your own country may give you further rights: the notes below say what they are, how quickly we answer and where you can complain. They concern the data for which we are the controller (section 3).

United Kingdom

The UK GDPR and the Data Protection Act 2018 give you the rights described in section 8; we answer within one month. If you are unhappy with how we have handled your data, complain to us first at **amministrazione@outlinedigital.it**: we acknowledge a complaint within 30 days, look into it without undue delay and tell you the outcome. You can also complain to the Information Commissioner's Office (ico.org.uk/make-a-complaint (<https://ico.org.uk/make-a-complaint/>)) or go to court. Data sent from the United Kingdom to our servers is covered by the United Kingdom's adequacy regulations for the European Economic Area.

Switzerland	Where the Federal Act on Data Protection (FADP) applies, you have the right to be told which data we hold about you — free of charge and normally within 30 days —, to have it corrected or deleted, to receive the data you gave us in a commonly used electronic format, and to object to its processing. Your data is processed in Germany, Italy and Ireland, which Switzerland recognises as providing adequate protection, and — for payment data handled by Stripe — in the United States, on the basis described in section 6. You can report a matter to the Federal Data Protection and Information Commissioner, Feldeggweg 1, 3003 Berne (edoeb.admin.ch (https://www.edoeb.admin.ch)), and bring a claim before the civil courts.
Canada	PIPEDA and, where they apply, the private-sector privacy laws of Québec (the Act respecting the protection of personal information in the private sector, as amended by Law 25), Alberta and British Columbia give you the right to access the personal information we hold about you, to have it corrected, to withdraw your consent subject to legal or contractual restrictions, and to challenge the way we comply. In Québec you can also ask to receive computerised information you provided in a structured, commonly used technological format, and to have information de-indexed or no longer disseminated where the law provides for it. We answer within 30 days. Your information is stored and processed outside Canada — in Germany, Italy and Ireland and, for payment data, in the United States — where it is subject to the laws of those countries and may be accessed by their courts and authorities. Our website uses no technology that identifies, locates or profiles you. The person in charge of the protection of personal information is the owner of OutLine Digital Agency, Via Dalmazia 36, 76125 Trani (BT), Italy, amministrazione@outlinedigital.it. You can complain to the Office of the Privacy Commissioner of Canada (priv.gc.ca (https://www.priv.gc.ca/en/report-a-concern/)), in Québec to the Commission d'accès à l'information (cai.gouv.qc.ca (https://www.cai.gouv.qc.ca)), or to the Information and Privacy Commissioner of Alberta or of British Columbia.
Australia	Where the Privacy Act 1988 applies to us, this page is our privacy policy under the Australian Privacy Principles. You can ask for access to the personal information we hold about you and for its correction; we respond within 30 days and do not charge for the request. For a general enquiry you may contact us without saying who you are; to open an account we need to know. We hold your information in Germany, Italy and Ireland and, for payment data, in the United States: the recipients there are not bound by the Australian Privacy Principles, but by the GDPR or by the safeguards described in section 6. If you think we have breached the Principles, write to us at amministrazione@outlinedigital.it: we reply within 30 days. If you are not satisfied, you can complain to the Office of the Australian Information Commissioner, GPO Box 5288, Sydney NSW 2001 (oaic.gov.au (https://www.oaic.gov.au/privacy/privacy-complaints)).

New Zealand

Where the Privacy Act 2020 applies to us, you can ask us to confirm whether we hold personal information about you, to give you access to it and to correct it; if we do not agree to a correction, you can ask us to attach to the information a statement of the correction you asked for. We decide on a request within 20 working days. Your information is held in Germany, Italy and Ireland, under the GDPR. Our privacy officer is the owner of OutLine Digital Agency, reachable at amministrazione@outlinedigital.it. If you are not satisfied with our reply, you can complain to the Office of the Privacy Commissioner ([privacy.org.nz](https://www.privacy.org.nz) (<https://www.privacy.org.nz/your-rights/making-a-complaint-to-the-privacy-commissioner/>)).

United States

There is no general federal privacy law. We do not sell personal information, do not share it for cross-context behavioural advertising, do not use it for targeted advertising or profiling, and use sensitive information — your password, in hashed form — only to sign you in. The categories of personal information we collect, the purposes and the retention periods are those in section 3: identifiers and contact details, account and billing records, payment records, and internet activity in our access logs. We collect them from you or from your organisation and disclose them only to the service providers named in section 5. We are below the thresholds at which the California Consumer Privacy Act and the other state privacy laws apply to a business; even so, whichever state you live in, you can ask us to tell you what we hold about you, to give you a copy, to correct it or to delete it. Write to amministrazione@outlinedigital.it, yourself or through an agent you have authorised in writing: we reply within 45 days and never treat you differently for asking. If we decline a request you can ask us to review the decision, and you can contact the Attorney General of your state. For the data that our customers keep in their workspaces we act as their service provider or processor (see the Data Processing Agreement (<https://people.omegasuiteapp.com/legal/dpa>)).

A summary, not a limit

These notes sum up the main points. They do not limit any right that the law of your country gives you and that cannot be waived.

10. If you do not provide the data

Name, email and password are needed to create the account: without them we cannot provide the service. Billing details are needed to activate a paid subscription. Everything else we ask for ourselves is optional. What your employer asks you to provide inside its workspace is a matter between you and your employer.

11. Cookies

The website and the application use **only strictly necessary cookies**, which do not require your consent. The details — name, purpose and duration of each — are in the Cookie Policy (<https://people.omegasuiteapp.com/legal/cookies>).

12. Children

Omega People is a service for businesses: it is not intended for children and we do not knowingly collect children's data to open an account. If we discover that an account has been opened by a child on their own initiative, we close it and delete the data. Where a business employs young workers or apprentices as the law of its country allows, it is

that business, as employer, that decides whether to record them and give them access.

13. Changes to this policy

Each version has a number and an effective date, and previous versions remain available on request. If a change concerns purposes or legal bases, we tell you by email and when you sign in, at least **30 days** in advance.

14. The mobile apps

The Omega People apps for iOS and Android (com.omegasuiteapp.people) are another way of reaching the same account. You sign in with an account that already exists — an account cannot be created, and nothing can be bought, in the apps — and they show the same data as the web application. What is described in the rest of this policy applies to them too; this section adds what is specific to a phone.

Permission	When the app asks for it	What happens to the data	If you refuse
Location (while the app is in use)	Only if your employer has switched on location for clock-ins: the position of the device is read at the moment you clock in or out , to check that you are at your place of work.	The coordinates, their accuracy, the distance from the site, whether you are inside the area set for the site and whether the device reports a simulated position are stored with the clock-in, in your employer's workspace. The app never reads your position in the background or at any other time.	No position is read. Depending on how your employer has set up clock-ins, you may then have to clock in another way, for example at the on-site kiosk.
Camera	To scan the QR code shown by the workplace kiosk when you clock in, and to photograph a receipt or a certificate you attach to a request.	The photo is uploaded to the workspace only when you attach it. When a QR code is scanned, only the code is read: no image is kept or sent.	You can still attach an existing file, and clock in another way.
Photos and files	To attach to a request, an expense claim, a chat message or a shared folder an image or a file that is already on your device.	Only the items you pick are uploaded. The app cannot read the rest of your library.	Nothing is attached.

- **What stays on the device.** The sign-in token and the code that locks the app, if you set one, are kept in the protected storage of the operating system; your profile, your preferences, the last screen shown and any clock-in waiting to be sent while you were offline (with its position, if location is on) are kept in the app's own storage. Signing out or uninstalling the app removes them.
- **What the app sends us.** What you see and do in the application, as on the web, plus the version of the app and whether it runs on iOS or Android. It sends no device name, model, advertising identifier or contact list.
- **Notifications.** The apps do not use push notifications today. If they are added, your device will ask you first, and this section and the Sub-processors (<https://people.omegasuiteapp.com/legal/subprocessors>) page will be updated beforehand.
- **The QR-code scanner.** The scanner uses Google's ML Kit library, which reads the code on the device. Google states that the library sends it technical diagnostics about how the scanner performs — device model and operating system, app version, a per-installation identifier that is not meant to identify a person, error codes — and no images. It is the only third-party component in the app that sends data to anyone other than us.
- **No tracking.** We do not track you across other companies' apps and websites, and the apps show no advertising.
- **Children.** The apps are business tools for the staff of our customers. They are not directed at children.

Who decides about your clock-ins

Whether location is recorded when you clock in is decided by your employer, who is the controller of that data and must tell you about it in its own notice. We only store it for your employer. Location recording is switched off unless your employer turns it on, and your phone always asks you before the app reads a position.

15. Deleting your account and your data

You can ask at any time for your Omega People account, and the data linked to it, to be deleted — whether you use the website or the mobile apps. It costs nothing.

On the web, without signing in. Go to people.omegasuiteapp.com/delete-account (<https://people.omegasuiteapp.com/delete-account>) and enter the email address you sign in with. We send a confirmation link to that address, valid for 24 hours; the page it opens tells you what will happen to your account in particular, and nothing is deleted until you press the confirmation button. The page gives the same answer whether or not an account exists with the address you enter.

From your profile. Once signed in to the website, choose **Delete my account** from the profile menu (the option is also at the bottom of **My profile**) and confirm with your password, without waiting for an email. This also works if you sign in with an address your company gave you (ending in .omegasuiteapp.com), which cannot receive email. If you only use the mobile app, use the page above or sign in to the website.

By email. You can also write to amministrazione@outlinedigital.it with the subject “Delete my account”, from the email address of the account. We may ask you to confirm that the request really comes from you.

- **You were given access by an organisation** — as an employee, a manager or an administrator. Your sign-in account is deleted straight away: name, email address, password, sessions, linked email addresses, the devices registered for notifications and your personal settings. The records about you inside the organisation's workspace — employee profile, contracts, attendance, leave, documents, payslips — are not deleted: they belong to the organisation, which is the controller of that data and may have to keep some of it for periods set by law. We forward your request to it at once, by email to the owner of the workspace and with a notice in the application, and it decides — within the limits of the law — what to erase. For those records you can also contact your employer directly.
- **You own a workspace.** While a workspace is attached to your account, the account cannot be deleted, because the workspace belongs to your organisation's subscription. First cancel the subscription in Settings -> Subscription: when it ends, the workspace stays read-only for 30 days and is then deleted with its database and files, as article 14 of the Terms of Service (<https://people.omegasuiteapp.com/legal/terms>) says — it also covers backups. If someone else should take over the workspace instead, write to us and we will transfer the ownership. We record your request and email you these steps; once no workspace is attached to your account, you can ask again.
- **You have no workspace.** The account is deleted as soon as you confirm.
- **What we keep.** Only what the law requires us to keep, or what we need to defend a legal claim, for the periods in section 3: invoices and accounting records, the documents of the subscription and the record of contractual acceptances — which, once the account is deleted, is no longer linked to your name but only to a fingerprint (hash) of your email address — and a record of the deletion request itself, linked only to that fingerprint. Backup copies are overwritten within 30 days.

Timelines. Requests made on the web page or from your profile are carried out as soon as you confirm, and we confirm by email when it is done (if the address can receive email). Requests sent by email are carried out within 30 days.

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