

Acceptable Use 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 Omega People may not be used for, and the rules that matter most when the data you manage is that of your own staff.

Legal references

Terms of Service, articles 10 and 13 · Regulation (EU) 2016/679 (GDPR), arts. 5, 6 and 9 · Anti-spam laws of the Customer's country (for example CAN-SPAM Act, CASL, UK PECR, Australian Spam Act 2003, New Zealand Unsolicited Electronic Messages Act 2007, Swiss Unfair Competition Act)

1. The principle

Omega People is for managing your staff lawfully and fairly. Any use that harms others — your employees first of all — breaks the law or puts the shared infrastructure at risk is prohibited, and entitles the Provider to suspend the service under article 13 of the Terms of Service (<https://people.omegasuiteapp.com/legal/terms>).

2. Prohibited uses

- Processing personal data without a valid legal basis, or for purposes other than those for which it was collected; storing data about employees or candidates that you may not lawfully hold.
- Monitoring or tracking staff covertly, or in ways that the law of your country does not allow (see section 4).
- Using the service to discriminate, to retaliate against someone who has raised a concern, or to try to identify the author of an anonymous report or survey answer.
- Uploading content that is unlawful, defamatory, infringes someone else's copyright or trademarks, or constitutes an offence.
- Sending unsolicited communications through automation rules, webhooks or messages to candidates (see section 3).
- Attempting to access workspaces, data or accounts that are not yours; probing, scanning or testing the security of the infrastructure without written authorisation.
- Circumventing technical limits, quotas, access controls or licensing mechanisms — including by subscribing to a band lower than the number of employees you manage.
- Using the service to generate abnormal load, to mine cryptocurrency or to resell its resources to third parties.
- Reselling, sublicensing or giving access to the service to anyone other than your own users.
- Using the AI features to produce unlawful, misleading or harmful content, to screen candidates, to assess or profile employees, or to take decisions about people without human involvement.
- Storing data that the service is not designed to hold: payment-card numbers, protected health information subject to HIPAA, fingerprints, face scans or other biometric identifiers.
- Using the service in breach of export-control or sanctions law, or giving access to it to anyone covered by article 27 of the Terms of Service (<https://people.omegasuiteapp.com/legal/terms>).
- Giving access to children: the service is a work tool, for people who are old enough to work under the law that applies to you.

3. Messages to people outside your organisation

Omega People itself sends only service messages (invitations, password resets, the emails of the rules you set up). When you write to candidates from the recruiting module, or use automation rules or webhooks to send messages to people outside your organisation, **you are the sender**, and you must comply with the anti-spam and privacy law of

the countries where the recipients are. In practice:

- send marketing messages only to people who have agreed to receive them, or where the law of their country allows it without consent;
- identify yourself clearly as the sender and give a working contact address;
- include an easy, free way to unsubscribe in every marketing message, and honour it promptly;
- keep a record of how and when each person agreed.

4. Your staff: monitoring, location, health data and the speak-up channel

You use Omega People on people who depend on you for their living. You are their employer and the controller of their data; these rules are the minimum, and the law of your country may ask for more.

- **Tell your staff first.** Before you start recording clock-ins, locations, reviews or anything else about your employees, give them your own privacy notice saying what you record, why and for how long. The application helps you prepare one under **Settings -> Privacy and compliance**, but giving it — and, where the law requires it, informing or consulting employee representatives, a union or a works council — is up to you.
- **No covert monitoring.** Attendance, timesheets, activity on the mobile app and reports show when and how much a person works. Use them for the purposes you have declared — recording working time, paying correctly, planning — and not to keep staff under hidden or continuous surveillance.
- **Location only at clock-in, and only if you need it.** If you switch on location for clock-ins, the application records the position of the device at the moment of clocking in or out, and nothing in between. Switch it on only where there is a real need (for example to confirm presence at a site), tell your staff, and do not use it to follow people's movements or their private life. Do not require staff to use a personal phone where the law gives them the right to refuse; the on-site kiosk is the alternative.
- **Health data: the minimum.** Sick-leave certificates, occupational-health checks and incident reports contain health data. Record what the law requires you to hold as an employer — as a rule, that a person is absent or fit for the job, not the diagnosis — restrict who can see it, and do not keep it longer than necessary.
- **Other sensitive data.** Do not record information about religion, ethnic origin, political opinions, sexual orientation, trade-union membership or criminal records unless a law requires or clearly allows you to, and never to treat people differently.
- **The speak-up channel is confidential.** Give access to reports only to the people responsible for handling them, protect the identity of the reporter and of the people named, do not try to find out who sent an anonymous report, and do not retaliate. If the law of your country sets deadlines for acknowledging and answering a report, meeting them is your responsibility.
- **Surveys.** Where a survey is set as anonymous, do not try to trace answers back to individuals — for example by surveying groups so small that people can be recognised.
- **Former employees.** When someone leaves, remove their access, and delete their record once the retention period that applies to you has passed.
- **Check what your country asks for before you switch a feature on.** Some laws require a written notice given in advance, an acknowledgement signed by each employee, a notice posted in the workplace, or the agreement of the employee or of their representatives, before working time, location or the use of work devices is recorded. The Employer notices (<https://people.omegasuiteapp.com/legal/employer-notices>) page gathers the main ones, with templates you can adapt. They are guidance, not legal advice.

5. Careers pages and other public pages

- Your careers page and application forms must show **your own privacy notice**: you are the controller of the applications you collect.
- Ask candidates only for the information you need to assess them for the job. Do not ask for information that the equal-treatment law of your country forbids you to take into account.
- Do not keep unsuccessful candidates' data longer than your notice says, and delete it when they ask, unless the law requires you to keep it.

- Do not use public pages to collect payment-card details, passwords or other credentials, and do not publish content on your careers page or website that is unlawful or misleading.

6. Reporting abuse

Anyone who believes that content made available through Omega People is unlawful can report it to **amministrazione@outlinedigital.it**, stating the exact address of the page, the reason and their contact details. Reports are examined without delay; the person reporting receives a reply on the outcome, and the customer concerned is informed of any measure taken and may contest it.

7. What happens if the rules are broken

Depending on how serious it is: a request to remove content, removal of the specific content, suspension of the workspace, termination of the contract. Except in an emergency or where an authority orders otherwise, the Customer is warned first and given the chance to put things right.

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