

Employer notices and country guide

Version 1.0, in force from 5 October 2026

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

What to tell your staff, your candidates and the people who use your speak-up channel before you switch a feature on, country by country, with templates you can adapt. Guidance, not legal advice.

Legal references

Terms of Service, article 10.3 to 10.10 · UK GDPR and Data Protection Act 2018; ICO guidance on monitoring workers · Switzerland: Code of Obligations, art. 328b; Ordinance 3 to the Labour Act, art. 26; Federal Act on Data Protection · Canada: PIPEDA; Québec: Act respecting the protection of personal information in the private sector; Alberta and British Columbia: Personal Information Protection Acts · Australia: Privacy Act 1988; Workplace Surveillance Act 2005 (NSW); Workplace Privacy Act 2011 (ACT); state surveillance devices legislation · New Zealand: Privacy Act 2020 · United States: New York Civil Rights Law § 52-c; Connecticut General Statutes § 31-48d; Delaware Code title 19, § 705; California Consumer Privacy Act

Read this first

Guidance, not legal advice

You are the employer and the controller of your staff's data: telling them what you record, and why, is your obligation, not ours. This page gathers what the laws of the countries where Omega People is offered generally ask for, and gives you texts to start from. It was last reviewed on 5 October 2026. It may be incomplete or out of date, it does not take your collective agreement, award or industry into account, and it does not replace the advice of a lawyer who knows your business. Article 10 of the Terms of Service (<https://people.omegasuiteapp.com/legal/terms>) applies.

The texts in square brackets are for you to fill in. The templates are yours to copy, change and give out under your own name.

1. What the application already prepares for you

Under **Settings -> Privacy and compliance** the application composes four notices from your company details and from the modules you use, in the language of the reader and with the rights and the complaint authority of your workspace's country:

- the notice for **job applicants**, linked from your careers page;
- the notice for **new starters**, for the form they fill in before their first day;
- the notice for **time and attendance recording**, which gains a paragraph on location as soon as you switch location on for clock-ins;
- the notice for people who use the **speak-up channel**.

You complete them with your contact details, your retention periods and anything specific to you, and you publish them. In the same place you find your record of processing, already filled in. What the application cannot do for you is the part that depends on where your staff work: the notices, acknowledgements, consents and consultations described below.

2. Your staff privacy notice

Whatever the country, a notice to employees should cover these points:

1. who you are, and whom to contact about personal data;
2. which data you hold — identity and contact details, official identifiers, contract and pay, bank details, working time, absences, documents, reviews;
3. what you use it for and, where your law works with legal bases, on which basis;
4. where the data comes from, when it does not come from the employee;
5. who receives it: payroll provider or accountant, authorities, benefit providers, and the provider of your HR software as your processor;
6. where it is stored (see section 7);
7. how long you keep it, during and after employment;
8. the rights the employee has, and how quickly you answer;
9. how to complain, to you first and then to the authority;
10. whether any decision is taken by automated means (the application takes none);
11. what monitoring takes place — time recording, location at clock-in, logs of activity.

What each country adds:

United Kingdom	State the lawful basis for each purpose and, for health and other special category data, the condition you rely on. Keep the medical detail of an absence apart from the bare record that the person was absent. Say how a worker can complain to you — since June 2026 you must acknowledge a data protection complaint within 30 days — and to the Information Commissioner's Office.
Switzerland	Process only data that concerns the employee's suitability for the job or is needed to perform the contract (Code of Obligations, art. 328b). Name the countries to which data is sent. Consent is rarely the right basis in an employment relationship.
Canada	Identify the purposes before or when you collect. Give the name or title of the person in charge of privacy. Say that the information is stored outside Canada and may be accessed by the authorities of the country where it is held. In Alberta, also say how employees can obtain your policies on service providers outside Canada. In Québec, add the right to data portability and how to withdraw consent, and remember the privacy impact assessment required before information is communicated outside Québec. Note that for most private employers outside Québec, Alberta and British Columbia no privacy statute covers employee data — a notice is still good practice.
Australia	Cover the matters in Australian Privacy Principle 5: your identity, the purposes, any law that requires the collection (for example the record-keeping rules of the Fair Work legislation), what happens if the information is not provided, who it goes to, that it is held overseas and in which country, and how to access and correct it and complain. The employee records exemption covers records of current and former employees of private-sector employers once they are held; it does not cover candidates, contractors or the act of collecting.
New Zealand	Cover the matters in information privacy principle 3: that information is being collected, why, who will receive it, your name and address, whether supplying it is required by law or voluntary and what follows if it is not supplied, and the rights of access and correction. Since 1 May 2026 principle 3A asks for the same when you obtain information about a person from someone else, such as a referee.

There is no general duty to give a privacy notice to employees. In California, employers that are a “business” under the CCPA must give employees, applicants and contractors a notice at collection listing the categories of personal information, the purposes, the retention period for each category and whether information is sold or shared. Everywhere, medical information obtained about employees must be kept confidential and apart from the personnel file (ADA, FMLA, GINA): in Omega People, keep such documents in a category that only the people who need them can open.

3. Clock-in with location

What the application does. Location is off unless you switch it on in the attendance settings. When it is on, the mobile app reads the position of the phone at the moment the employee clocks in or out — never in the background, never between the two — after the phone itself has asked the employee for permission. With each clock-in it stores the coordinates and their accuracy, the distance from the site, whether the position is inside the area you set for the site, and whether the phone reports a simulated position. Clock-ins from the browser and from the on-site kiosk record no position. You decide whether a clock-in without a position is accepted.

Before you switch it on:

1. decide why you need it — confirming presence at a site is a reason; curiosity is not — and write it down;
2. give the written notice your law requires, in advance (template in section 4), and keep proof that each employee received it;
3. offer another way of clocking in to people who do not want to use their own phone, such as the kiosk;
4. decide who may see positions and for how long you keep them;
5. where your law provides for it, carry out an impact assessment and consult employees or their representatives.

Where your staff work	What the law generally asks	Rule
United Kingdom	Tell workers before you start what is recorded, why, how it will be used and for how long; identify a lawful basis; carry out a data protection impact assessment; consult workers or their representatives; do not record location outside working time.	UK GDPR; ICO guidance “Employment practices and data protection: monitoring workers”
Switzerland	Systems meant to monitor the behaviour of employees are prohibited; recording working time is allowed. Inform employees in advance, limit location to the moment of clocking in, record why it is necessary and proportionate, and involve employees as the law on participation requires.	Code of Obligations, art. 328b; Ordinance 3 to the Labour Act, art. 26
Canada — federally regulated employers, Alberta, British Columbia	Tell employees in advance the purpose, nature and extent of the collection; collect only what is reasonable for managing the employment relationship.	PIPEDA; PIPA Alberta, s. 15; PIPA British Columbia, s. 13
Canada — Québec	Inform employees beforehand of the technology used and of how to switch the function on and off. A function that locates a person must not be active by default: in Omega People it is off until you turn it on, and each phone asks its user. Carry out a privacy impact assessment.	Act respecting the protection of personal information in the private sector, ss. 3.3, 8 and 8.1

Australia — New South Wales	Written notice at least 14 days before surveillance begins (before a new employee starts work), stating the kind of surveillance (tracking), how it is carried out, when it starts, whether it is continuous or intermittent and whether it is for a specified period or ongoing. No surveillance when the employee is not at work. Whether an app that reads a position at clock-in is “tracking surveillance” is not settled: give the notice in any case.	Workplace Surveillance Act 2005, ss. 10, 13 and 16
Australia — Australian Capital Territory	Written notice at least 14 days in advance with similar content and the purposes for which the records may be used; consultation with workers before surveillance is introduced.	Workplace Privacy Act 2011, ss. 13 and 14
Australia — other states and territories	Using a device to determine where a person is generally requires that person's consent: obtain it in writing. The Privacy Act applies to the collection where you are covered by it.	Surveillance devices legislation of each state and territory; Privacy Act 1988
New Zealand	Have a written policy that says why, when and how location is recorded; consult employees and their union before introducing it; make sure every employee knows; record only during working time.	Privacy Act 2020, information privacy principles 1 to 4; duty of good faith under the Employment Relations Act 2000
United States — New York	Written notice on hiring to employees whose telephone, email or internet use is monitored, acknowledged in writing or electronically, and posted in a conspicuous place. It is not settled whether a position read at clock-in is covered: giving and posting the notice is the prudent course.	Civil Rights Law § 52-c
United States — Connecticut	Prior written notice of the types of electronic monitoring that may take place, posted in a conspicuous place.	General Statutes § 31-48d
United States — Delaware	Notice of the monitoring of telephone, email or internet use, given once in writing and acknowledged by the employee, or shown electronically each day.	Delaware Code, title 19, § 705
United States — California	For employers that are a “business” under the CCPA: a notice at collection that lists precise geolocation among the sensitive personal information collected, with its purpose and retention period. A tracking device attached to a vehicle needs the consent of its registered owner.	California Consumer Privacy Act; Penal Code § 637.7

4. Template: notice of time recording and of location at clock-in

Give it in writing — on paper or by email — before the date in the first paragraph, have each employee acknowledge it, and where your law asks for it post a copy where everyone can see it.

1. **What we are introducing.** [Company name] records the start and the end of your working time with the Omega People software. From [date — at least 14 days after this notice where your law requires it] we will also record your location when you clock in or out from the mobile app.
2. **What is recorded.** The date and time of each clock-in and clock-out and the site or device used; from the mobile app, the position of your phone at that moment (coordinates and their accuracy), its distance from the site, whether it is inside the area set for the site and whether the phone reports a simulated position.
3. **What is not recorded.** Your position is read only at the instant you clock in or out. It is not followed during the working day, during breaks or outside working hours, and the app does not run in the background.
4. **Kind of surveillance.** Tracking, by means of the Omega People app on [your own / the company's] phone; intermittent — only at clock-in and clock-out; ongoing from the date above.
5. **Why.** To record working time accurately, to confirm presence at [site or customer premises] and to pay you correctly. [Say here whether the records may be used in disciplinary proceedings.] They will not be used for any other purpose.
6. **Who sees it, and for how long.** [Roles: for example your manager and the HR team.] Positions are kept for [period] and then deleted.
7. **Your choice.** Your phone asks for your permission before the app reads your position. If you prefer not to use your own phone, you can clock in [at the kiosk at reception / in another way].
8. **Where the data is kept.** [Use the sentence in section 7.]
9. **Your rights.** You can ask to see the records about you, to have them corrected and to raise any concern with [name or role, email address]. [Add the rights and the authority that apply in your country, as in your staff privacy notice.]
10. **Acknowledgement.** I have received and read this notice. Name — date — signature [or electronic acknowledgement].

5. Candidates

The notice for applicants should say who you are, that the data is used to assess the application, which data you ask for and why, whether you contact referees (only with the candidate's agreement), who receives the data and where it is stored, how long you keep the application of someone you do not hire, that a talent pool is optional and can be left at any time, and the rights and complaint route. Ask only for what the job requires.

In Omega People, applications of unsuccessful candidates are deleted after 12 months unless you set a different period (from 1 to 60 months) in the recruiting settings. Set it to match what you promise in your notice:

Country	How long to keep unsuccessful applications
United Kingdom	No fixed period: no longer than you need to answer a discrimination claim. The ICO's own example is six months after the decision.
Switzerland	Return or destroy the application documents once the process is over, unless the candidate agrees to a longer period.

Canada	No fixed period: long enough for the candidate to ask for access after a decision, then destroy. Keeping applications indefinitely is not allowed in Québec.
Australia	The Australian Privacy Principles apply in full to unsuccessful candidates: destroy or de-identify the information once it is no longer needed.
New Zealand	No longer than is required for the purpose for which the information may lawfully be used (information privacy principle 9).
United States	At least one year from the decision under federal anti-discrimination record-keeping rules; some employers and some states require longer. Do not set a shorter period.

6. The speak-up channel

The notice should say what can be reported and to whom; that a report can be anonymous; that the reporter's identity is kept confidential and who may know it; how the data and the rights of the person reported are handled; who may receive the report (investigators, advisers, authorities); how long it is kept; that retaliation is forbidden; and that nothing stops anyone from going to an external authority. In Omega People the reports can be opened by the owner, the administrators and the people you give that permission to: keep that circle small.

United Kingdom	The Public Interest Disclosure Act 1998 protects workers who make a qualifying disclosure, including to a prescribed person such as a regulator. There is no general duty to run a channel.
Switzerland	There is no general whistleblowing statute: data protection law and the employer's duty of care apply.
Canada	There is no general private-sector statute. The Criminal Code (s. 425.1) forbids retaliation against an employee who reports an offence to law enforcement; sector and provincial rules may add to this.
Australia	Under Part 9.4AAA of the Corporations Act 2001 it is an offence to disclose the identity of an eligible whistleblower without consent, except to ASIC, APRA, the federal police or a lawyer. Public companies and large proprietary companies must have a whistleblower policy.
New Zealand	The Protected Disclosures (Protection of Whistleblowers) Act 2022 expects the receiver to use best endeavours to keep the discloser's identity confidential and to deal with a disclosure within 20 working days.
United States	Listed companies must have procedures for the confidential, anonymous submission of concerns about accounting matters (Sarbanes-Oxley Act). Retaliation is prohibited by federal and state law, and no agreement or policy may stop a person from reporting to the SEC or another authority.

7. Template: where the data is stored

Several laws ask you to say that the data leaves the country and where it goes: Switzerland (the states concerned), Alberta and the rest of Canada (processing outside Canada and access by foreign authorities), Australia (the countries of overseas recipients) and New Zealand. You can use this sentence in all your notices:

Sentence to copy

Our HR software, Omega People, is provided by OutLine Digital Agency, established in Italy, which processes the data on our behalf under a data processing agreement. The data is stored on servers in Germany, in the European Union. It is therefore held outside [your country], it is subject to the laws of Germany, Italy and the European Union, and the courts and authorities of those countries can obtain access to it in the cases their law provides. For any question about how our provider handles your data, write to [name or role, email address].

The technical facts behind the sentence — where the servers are, who the sub-processors are, the security measures — are in the Data Processing Agreement (<https://people.omegasuiteapp.com/legal/dpa>), the Sub-processors (<https://people.omegasuiteapp.com/legal/subprocessors>) list and the Security Measures (<https://people.omegasuiteapp.com/legal/security>) page. They are what you need for a transfer assessment, including the one Québec requires.

8. Health data and other sensitive data

- Record what the law requires an employer to hold — that a person is absent, or fit for the job with certain restrictions — and not the diagnosis. Do not type a diagnosis into a free-text field.
- Keep medical certificates and similar documents where only the people who need them can open them, and say in your notice who those people are.
- Omega People does not collect fingerprints, face scans or other biometric identifiers, and you must not upload any: several laws — Illinois, Texas and Colorado in the United States, Québec, New Zealand's biometric code — attach strict conditions to them.
- National identifiers (National Insurance number, Social Security number, Social Insurance Number, tax file number, IRD number, AHV number) are for the purposes the law gives them: show them to as few people as possible.
- Before you switch on an AI feature for staff data, read the Artificial Intelligence (<https://people.omegasuiteapp.com/legal/ai>) page and tell your staff.

9. Official sources

- United Kingdom — Information Commissioner's Office, employment guidance: ico.org.uk (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/>)
- Switzerland — Federal Data Protection and Information Commissioner, data processing by the employer: [edoeb.admin.ch](https://www.edoeb.admin.ch) (<https://www.edoeb.admin.ch/en/data-processing-by-the-employer>)
- Canada — Office of the Privacy Commissioner, privacy in the workplace: [priv.gc.ca](https://www.priv.gc.ca) (https://www.priv.gc.ca/en/privacy-topics/employers-and-employees/02_05_d_17/); Québec — Commission d'accès à l'information: [cai.gouv.qc.ca](https://www.cai.gouv.qc.ca) (<https://www.cai.gouv.qc.ca>)
- Australia — Office of the Australian Information Commissioner, employee records exemption: [oaic.gov.au](https://www.oaic.gov.au) (<https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/employee-records-exemption>); NSW legislation: legislation.nsw.gov.au (<https://legislation.nsw.gov.au/view/html/inforce/current/act-2005-047>); ACT legislation: legislation.act.gov.au (<https://www.legislation.act.gov.au/a/2011-4>)
- New Zealand — Office of the Privacy Commissioner: [privacy.org.nz](https://www.privacy.org.nz) (<https://www.privacy.org.nz>); Employment New Zealand, employee privacy: [employment.govt.nz](https://www.employment.govt.nz) (<https://www.employment.govt.nz/fair-work-practices/employee-privacy>)
- United States — New York: [nysenate.gov](https://www.nysenate.gov) (https://www.nysenate.gov/legislation/laws/CVR/52-C*2); Connecticut: [cga.ct.gov](https://www.cga.ct.gov) (https://www.cga.ct.gov/current/pub/chap_557.htm); Delaware: delcode.delaware.gov (<https://delcode.delaware.gov/title19/c007/sc01/index.html>); California: oag.ca.gov (<https://oag.ca.gov/privacy/ccpa>)

The current full text is always available at <https://people.omegasuiteapp.com/legal/employer-notices?lang=en>. For

any question: amministrazione@outlinedigital.it.