

Employee privacy notice template

Every UK employer must give workers privacy information at the time their personal data is collected, under Article 13 of the UK GDPR. There is no exemption for small employers. The notice must say who you are, what you use the data for and your lawful basis, who you share it with, how long you keep it and what rights the person has. Since 19 June 2026 it must also tell people they have the right to complain to you, and you must acknowledge a complaint within 30 days. Since 30 September 2026 the regulator is the Information Commission, which has replaced the Information Commissioner.

Download the notice ? PDF • edit the [bracketed] parts

What does an employee privacy notice say? The template

Replace each [bracketed placeholder] and delete what does not apply. The notice describes what you actually do, so check each clause against your real systems before you publish it.

1. Who we are

[Company name] ("we") is the controller of the personal data we hold about you as a job applicant, employee, worker or contractor. Our address is [address]. Questions about this notice or your data go to [name or role, email]. [Our data protection officer is [name, contact details].]

2. What we collect

Identity and contact details; date of birth; National Insurance number; bank details; right to work documents; your contract, job, pay, pension and benefits; working hours, attendance, holiday and other leave; performance, training, disciplinary and grievance records; next of kin and emergency contacts; [photographs, CCTV images, door access and IT system logs]. We also hold some special category data: information about your health, including sickness absence, fit notes and occupational health reports, and [equality monitoring data; trade union membership where you pay subscriptions through payroll]. Where a role requires it, we hold the result of a criminal record check.

3. Where it comes from

Most of it comes from you. Some comes from your manager, from referees and former employers, from [recruitment agencies], from the Home Office when we check your right to work, from the Disclosure and Barring Service, from HMRC, from your doctor or our occupational health provider with your knowledge, and from our own systems.

4. Why we use it, and our lawful basis

To perform your contract: paying you, providing benefits, managing hours, leave and performance. To comply with our legal obligations: tax and National Insurance, pensions, right to work checks, health and safety, statutory pay and leave, and equality law. For our legitimate interests in running the business safely and fairly: planning work, managing conduct and capability, keeping our premises and systems secure, and defending legal claims. We rely on consent only where you have a genuine choice, and you can withdraw it at any time by telling [role].

5. Special category and criminal record data

We use health and other special category data because it is necessary for our obligations and rights in the field of employment, such as paying sick pay, making reasonable adjustments and keeping people safe at work. We keep an appropriate policy document that explains how we protect this data and how long we keep it. You can ask [role] for a copy.

6. Who we share it with

[Payroll provider]; [pension provider]; [benefits providers]; [HR and IT system suppliers]; [occupational health provider]; our professional advisers and insurers; HMRC and other public bodies where the law requires it; and a prospective buyer of the business under a duty of confidence. Suppliers who process your data for us do so under a written contract and only on our instructions. We do not sell your data.

7. Transfers outside the UK

[We do not transfer your data outside the UK.] [Some of our suppliers store data in [countries]. Those transfers are protected by [UK adequacy regulations / the International Data Transfer Agreement / the UK Addendum to the standard contractual clauses].]

8. How long we keep it

We keep your data for as long as you work for us and then for the periods in our retention schedule, which you can see at [location]. In outline: most personnel records for [six years] after you leave; payroll records for at least three years after the end of the tax year; right to work copies for two years after you leave; unsuccessful applicants' records for [six months].

9. Whether you have to give it

Some information is required by law or by your contract, including proof of your right to work, your National Insurance number and bank details. Without it we may be unable to employ you or pay you. We will tell you when something is optional.

10. Automated decisions

[We do not make decisions about you based solely on automated processing.] [We use [system] to [purpose]; a person reviews the outcome and you can ask for that review.]

11. Your rights

You can ask us for a copy of your data, to correct it, to erase it or to restrict how we use it; you can object to processing based on our legitimate interests; and in some cases you can ask for your data in a portable form. Ask [role, email]. We will respond without undue delay and within one month, which the law allows us to extend by two further months where a request is complex.

12. How to complain

If you are unhappy with how we have handled your personal data, you have the right to complain to us. Use [the form at location / email address]. We will acknowledge your complaint within 30 days and tell you the outcome without undue delay. You also have the right to complain to the Information Commission (ico.org.uk).

13. Changes

This notice was last updated on [date]. We will tell you about any significant change before it takes effect.

What must a privacy notice contain by law?

Article 13 of the UK GDPR sets the list, and it must be provided "at the time when personal data are obtained". The table maps each item to a clause above.

- Article 13 item - Clause
- Controller's identity and contact details; data protection officer if there is one - 1
- Purposes and lawful basis; the legitimate interests relied on - 4, 5
- Recipients or categories of recipients - 6
- International transfers and safeguards - 7
- Retention period, or the criteria used to set it - 8
- The data subject's rights, including withdrawing consent - 4, 11
- The right to complain to the controller (new from 19 June 2026) - 12
- The right to complain to the regulator - 12
- Whether providing the data is a statutory or contractual requirement, and the consequences of not providing it - 9
- Automated decision-making - 10

What changed in 2026?

Three things, all from the Data (Use and Access) Act 2025, and all now in force.

- A complaints procedure is compulsory (19 June 2026). Section 164A of the Data Protection Act 2018 requires a controller to make it easy to complain, for example with an electronic form, and to "acknowledge receipt of the complaint within the period of 30 days beginning when the complaint is received". The regulator's guidance is blunt: "You must have a process for handling data protection complaints within your organisation - there are no exemptions to this."
- The notice must mention it (19 June 2026). Article 13 now lists "the right to make a complaint to the controller". The duty applies to complaints received on or after that date.
- The regulator has a new name (30 September 2026). The office of Information Commissioner was abolished and its functions transferred to the Information Commission. A notice that tells staff to complain to "the Information Commissioner" is now out of date. The website is still ico.org.uk.

One change helps employers. Since 5 February 2026 the time limit for a subject access request is set out in a new Article 12A, and the clock stops while you wait for clarification you reasonably need. The subject access request guide covers the process.

Which lawful basis should an employer use?

The regulator's employment guidance names contract, legal obligation and legitimate interests as "the lawful bases that are most likely to be relevant in an employment records context". It warns against consent: "You should avoid relying on consent unless you are confident you can demonstrate it is freely given", because "as an employer, you will generally be in a position of power over your workers."

Health data needs two more things: the employment condition in Article 9(2)(b), and the matching condition in Schedule 1 of the Data Protection Act 2018, which applies only if "the controller has an appropriate policy document in place". Every employer that records sickness absence is in that position.

Do you also need a record of processing?

Usually, yes. Article 30 requires a written record of processing activities. Organisations employing fewer than 250 people are excused only for processing that is occasional, low risk and free of special category data. The regulator's wording is that smaller organisations "need only document processing activities that: are not occasional"; "are likely to result in a risk to the rights and freedoms of individuals"; or "involve special category data or criminal conviction and offence data". Payroll and HR records are regular and include health data, so they must be documented at any size.

Start from your HR data retention schedule: the same list of record types, with purpose, lawful basis, recipients and retention against each, is most of an Article 30 record.

How do you use the notice well?

- Give it at the right moment. Applicants need a version when they apply; employees need the full notice with their offer or on day one. Put it in the new starter checklist.
- It is a notice, not a contract. Do not ask people to sign that they agree. Record that they have received it.
- Name your real suppliers and periods. A notice copied from a template with the placeholders left vague fails the test of telling people what happens to their data.
- Check whether you owe the data protection fee. It is £52 a year for an organisation with a turnover of no more than £632,000 or no more than 10 staff, £78 for turnover up to £36 million or no more than 250 staff, and £3,763 above that. Processing only for staff administration, accounts and your own marketing is exempt.
- Review it yearly and whenever you change a payroll, HR or monitoring system.

A free template from CoDash - codash.co.uk/templates. Edit it to match how your company actually works, and take advice on anything unusual.