

The BTR Hub Limited

Privacy Notice

Version 3.1 | Effective date: 17 October 2026 | Next review: October 2027

1. Introduction

The BTR Hub Limited ("The BTR Hub", "we", "us" or "our") is a limited company registered in England and Wales under company number 14078258.

We respect your privacy and are committed to protecting your personal data. This Privacy Notice explains how we collect, use, store and share personal data, the lawful bases on which we process it, how long we retain it, and the rights available to you under applicable data protection law.

Our registered address is 2nd Floor, Fairchild House, Redbourne Avenue, London, N3 2BP.

The BTR Hub Limited is the data controller for the personal data covered by this Privacy Notice, including the personal data of recruitment candidates and our own training records. Occasionally, when a business client sends its own trainees to us, we process those trainees' data on the client's behalf as its processor; in that case the client is the controller and its own privacy information also applies. We have appointed a Data Protection Lead who oversees data protection matters and enquiries. Contact details are provided in section 11.

1.1 Purpose of this Privacy Notice

This Privacy Notice applies to personal information we collect directly from you, through our website and online services, or from third parties. It explains:

- what personal data we collect;
- how and why we use it;
- the lawful bases on which we rely;
- how long we keep it;
- how we protect it;
- who we share it with;
- international transfers of personal data; and
- your rights in relation to your personal data.

Our website and services are not directed specifically at children and we do not knowingly collect children's personal data through our general website services except where this is necessary and appropriate in connection with a training, recruitment or other service and suitable safeguards are in place.

1.2 Third-party links

Our website may contain links to third-party websites, services, plug-ins or applications. Clicking those links or enabling those connections may allow third parties to collect or process information about you. We do not control third-party websites and are not responsible for their privacy notices. We encourage you to read the privacy information provided by any third party whose website or service you use.

2. Personal Data We Collect

Personal data means information relating to an identified or identifiable individual. Depending on your relationship with us and the services you use, we may collect, use, store and transfer the following categories of personal data:

- **Identity Data** – including name, title, date of birth and, where relevant, gender.
- **Contact Data** – including telephone number, email address, billing address and delivery or postal address.

- **Financial Data** – including bank account and sort code where required. Payment card information used for online bookings is processed by our payment provider and we do not receive or store your full payment card details.
- **Transaction Data** – including details of payments to and from you and products, courses and services purchased from us.
- **Technical Data** – including IP address, browser type and version, device information, operating system and other technical information associated with use of our website and online services.
- **Profile Data** – including account details, where applicable, and purchases or bookings made by you.
- **Usage Data** – information about how you use our website, products and services.
- **Marketing and Communications Data** – including your marketing preferences, communication preferences and records of relevant communications.
- **Online Booking Data** – information provided when you make a course booking through our online booking system, including your selected course, course date, attendee details, booking preferences, promotional or voucher codes used and information relating to your booking.

We may also collect information when you request a call back, contact us, interact with us, are referred to us by a third party, apply for employment or recruitment opportunities, or provide feedback.

2.1 Candidate and Recruitment Data

Where you apply for a role with us, register as a candidate, or use our recruitment services, we may collect additional information where relevant to the role or service, including:

- name, contact details, date of birth, nationality and citizenship information;
- photograph and identification information;
- emergency contact or next-of-kin information where necessary;
- copies of driving licences, passports or other identity documents where required for identity, eligibility or compliance checks;
- education, qualifications, skills, languages and employment history;
- current job title, sector, availability and employment preferences;
- referee details and information supplied by referees;
- immigration or right-to-work information;
- remuneration and employment information where relevant;
- financial or tax information where necessary for the service or relationship;
- video recordings where an interview process involves recording and an appropriate lawful basis applies;
- criminal conviction information where lawfully required for a particular role or safeguarding purpose; and
- information supplied by clients, job sites, referees or other relevant third-party sources.

Where appropriate, candidates may also receive additional privacy information specific to the recruitment process.

2.2 Special Category and Criminal Offence Data

Certain information is afforded additional protection under data protection law, including information about health, racial or ethnic origin, religious or philosophical beliefs, trade union membership, genetic or biometric data used for identification, and sex life or sexual orientation.

We only process special category data where it is necessary and where an appropriate condition under data protection law applies. Depending on the circumstances, this may include explicit consent or processing necessary in connection with employment, social security or social protection law.

Criminal offence data is processed only where permitted by law and where necessary, for example for roles requiring appropriate DBS or other safeguarding checks.

If you make a data protection complaint that includes special category information (for example about your health), we rely on the condition for the establishment, exercise or defence of legal claims (UK GDPR Article 9(2)(f)). If a complaint includes criminal offence information, we rely on the legal claims condition in the Data Protection Act 2018, Schedule 1, Part 3, paragraph 33. We use only the information needed to deal with your complaint.

For contractor candidate screening we rely on: Article 9(2)(g) with DPA 2018 Schedule 1, paragraph 6 (statutory purposes, for Equality Act 2010 reasonable adjustments in training and onboarding) and paragraph 18 (safeguarding of children and individuals at risk, for fitness to drive where driving is part of the role, and safe participation in practical training); and, for criminal offence data, Schedule 1 paragraphs 18, 10 (preventing or detecting unlawful acts) and 6. We do not rely on consent for this processing. Our Appropriate Policy Document explains how we protect this information.

We do not ask customers to provide unnecessary special category, criminal offence or identity-document information through our general online course booking system.

Course delegates: our booking form does not ask about health. If you choose to tell us by email about reasonable adjustments, accessibility requirements or learning support needs, this may include health or disability information. We use it only to make adjustments for your course, and we share it only with your trainer. Our lawful bases are contract (UK GDPR Article 6(1)(b)) and legal obligation (Article 6(1)(c): our duty as a service provider to make reasonable adjustments, Equality Act 2010 section 29(7)). For health or disability information we rely on Article 9(2)(g) with DPA 2018 Schedule 1, paragraph 6 (statutory purposes – Equality Act 2010 duties), as set out in our Appropriate Policy Document.

2.3 Contractor Candidates (Screening and Introduction)

We screen independent contractor candidates for roles requiring DBS or heightened background checks (for example, safeguarding or patient transport roles) and introduce suitable candidates to our clients. The client engages the candidate directly and is responsible for its own checks and records after handover, including right-to-work checks. We do not monitor candidates' work after handover.

For this screening we may collect: name, contact details and date of birth; identity and eligibility-to-work information; where driving is part of the role, driving licence details and the result of a DVLA licence check; criminal record declarations and enhanced DBS check information (including barred list checks where the role is eligible); limited health information (any health condition or disability that may affect training or onboarding, so that we can make reasonable adjustments, and, where driving is part of the role, whether the candidate meets the driving medical standards; any further health assessment is carried out by the client that engages the candidate); references; training records; and signed documents. We share the results of our screening with the client the candidate is introduced to, limited to what the client needs. Contractor candidates receive a separate pre-screening form with this information.

3. How You Can Control Your Data

Where we send electronic direct marketing, you can unsubscribe using the link provided in the communication or contact us using the details in section 11. You can also ask us to update your communication preferences at any time.

Where we rely on your consent as the lawful basis for processing your personal data, you may withdraw that consent at any time. Withdrawal of consent does not affect the lawfulness of processing carried out before consent was withdrawn.

Withdrawal of consent does not necessarily require us to delete all information we hold about you. We may continue to retain or process personal data where another lawful basis applies, including where this is necessary to perform a contract, comply with a legal or regulatory obligation, establish or defend legal claims, or meet legitimate business record-keeping requirements.

Please tell us if your personal information changes so that we can keep our records accurate and up to date.

4. How We Use Your Personal Data

We use personal data only where we have a lawful reason to do so. Depending on your relationship with us, this may include:

- providing and managing access to our website and services;
- supplying training, recruitment and other products and services;

- processing and administering course bookings, including booking confirmations, course information, joining instructions and communications relating to a booking;
- processing payments and maintaining transaction records;
- responding to enquiries, requests and communications;
- administering pre-recruitment and recruitment activities;
- carrying out appropriate compliance, eligibility, identity or safeguarding checks;
- providing online forms, electronic signature and document-execution services through our own systems;
- administering our customer and candidate relationships;
- analysing use of our website and services and obtaining feedback to improve them;
- maintaining the security and integrity of our systems and services; and
- meeting legal, regulatory, accounting and contractual obligations.

4.1 Information Received from Third Parties

We may receive personal data from third parties and public sources where appropriate, including:

- analytics and search providers such as Google;
- payment and transaction service providers such as Stripe;
- recruitment platforms, job sites, clients and referees;
- identity, compliance and background-check providers where relevant; and
- publicly available sources where lawful and appropriate.

4.2 Direct Marketing

Where permitted by law, we may send you information about our courses, services, news and offers. Where consent is required for electronic marketing, we will obtain it separately from any acceptance of booking terms or other contractual terms.

Marketing choices are optional. You can withdraw consent or opt out of marketing at any time by using the unsubscribe facility in our emails or contacting us. Opting out of marketing will not prevent us from sending service messages that are necessary to administer a booking, course, contract or other existing relationship.

We comply with the Data Protection Act 2018, UK GDPR and the Privacy and Electronic Communications Regulations 2003, as amended, in relation to direct marketing.

4.3 Electronic Signature Processing

We use electronic signature functionality to facilitate execution of documents. This may involve processing names, email addresses, signatures, IP addresses and signing audit information.

We store information collected through our online forms and electronic signature system (DocuSeal) on our own server hosted by DigitalOcean in London, UK. DigitalOcean acts as our hosting processor, and the data stays in the UK. Notifications relating to document signing may be delivered using trusted third-party email providers.

5. Lawful Bases for Processing

We process personal data lawfully, fairly and transparently. The lawful basis we rely upon depends on the purpose of the processing and may include:

- **Consent** – where you have given clear consent for a specific purpose, for example certain marketing activities, recorded interviews or processing requiring explicit consent.
- **Contract** – where processing is necessary to enter into or perform a contract with you, including processing course bookings, providing training services and administering relevant recruitment or employment services.
- **Legal obligation** – where processing is necessary for us to comply with the law, including certain employment, tax, accounting, safeguarding or DBS-related obligations, and handling data protection complaints (section 164A Data Protection Act 2018).
- **Legitimate interests** – where processing is necessary for our legitimate business interests or those of a third party and those interests are not overridden by your rights and freedoms.

Our legitimate interests may include maintaining accurate records; operating, securing and improving our website and systems; developing and administering our products and services; responding to general complaints (data protection complaints are handled under our legal obligation); understanding service usage and customer needs; administering recruitment services; preventing fraud or misuse; and carrying out appropriate business analysis.

6. Storage and Retention of Personal Data

We do not keep personal data for longer than is necessary for the purpose for which it was collected, taking account of legal, regulatory, tax, accounting, contractual and operational requirements.

Retention periods vary according to the type of information and our relationship with you. Further details are set out in our [Data Retention Policy](#).

Key periods include:

- Contractor candidate screening records (including DBS check, health and eligibility-to-work information), other than the signed pre-screening form: deleted 6 months after handover to the client;
- unsuccessful or withdrawn candidates: deleted after 6 months (other than the signed pre-screening form);
- signed documents, including your signed pre-screening form (which contains your self-declared criminal record and health answers): kept whole for 6 years from signature; training records (including learner records): 6 years from the date of the training. DBS certificate information is never kept for more than 6 months, and we do not keep copies of DBS certificates;
- adjustment and accessibility information for course delegates: deleted once the course has finished, unless it is needed for a complaint or an incident record;
- our CRM (recruitment and trainee records): basic contact and progress details only, kept for 1 year for reporting. The CRM does not hold criminal record or health information. Client contacts in our sales CRM are kept for the duration of the contract plus 6 years.

Even where information is no longer required for the original purpose, we may retain limited information where necessary to comply with a legal or regulatory obligation, establish or defend legal claims, or maintain appropriate business records.

6.1 Data Security

We use appropriate technical and organisational measures designed to protect personal data against unauthorised access, alteration, disclosure, loss or destruction. Access to personal data is limited to authorised personnel and service providers who require it for legitimate purposes.

Staff with access to personal data receive appropriate data protection training. Where third parties process personal data on our behalf, we require appropriate contractual and security arrangements.

The BTR Hub has obtained Cyber Essentials certification.

6.2 Electronic Signature Data

Where documents are signed using our electronic signature systems:

- we store information collected through our online forms and electronic signature system (DocuSeal) on our own server hosted by DigitalOcean in London, UK, so the data stays in the UK; DigitalOcean acts as our hosting processor;
- documents may be temporarily stored on that server;
- completed documents are transferred to and stored within our internal systems;
- documents are retained in accordance with our Data Retention Policy; and
- documents remaining on the signing system are deleted periodically and at least annually.

7. Who We Share Personal Data With

We share personal data only where necessary for legitimate business purposes, to provide our services, administer our relationship with you, comply with legal obligations, or where otherwise permitted by law. We do not sell personal data to unconnected third parties.

Service providers may process personal data on our behalf. We require processors to protect personal data appropriately and to process it only for authorised purposes and in accordance with applicable contractual and legal requirements.

Third party	Purpose	Privacy information
Willo	Screening and interview processes	Willo privacy policy
Checks Direct	DBS checks	Checks Direct privacy policy
uCheck	DBS and compliance checks	uCheck applicant privacy policy
Healthier Business Group / HB Compliance	E-learning and compliance services	Provider privacy policy
Microsoft 365	Email, documentation, storage and Microsoft Teams	Microsoft Privacy Statement
Google Workspace	Document storage and related services where used	Google Privacy Policy
monday.com	Recruitment and trainee records (our CRM) and operational workflow management	monday.com privacy/GDPR information
Freshsales (Freshworks)	Sales CRM: client and new business contacts and enquiries, including our website enquiry forms (no criminal record or health information)	Freshworks Privacy Notice
Online forms and DocuSeal	Our online forms (for example applications and references) and electronic signatures, on our own server	Operated by The BTR Hub; supporting infrastructure providers are listed separately
DigitalOcean	Cloud hosting: our own server for our online forms and electronic signature system (DocuSeal), in London, UK	DigitalOcean Privacy Policy
SendGrid (Twilio)	Email delivery for documents and notifications	Twilio Privacy Notice
Pro-Trainings	Training registration, accreditation and certification	Pro-Trainings Privacy Policy
Bookeo	Online course booking, booking administration and customer communications	Bookeo Privacy Policy
Stripe	Online payment processing	Stripe Privacy Policy

We may also share personal data where necessary with professional advisers such as lawyers, accountants, auditors, bankers and insurers; HM Revenue & Customs, regulators and other public authorities; the Disclosure and Barring Service (DBS), if the law requires us to make a barring referral; IT and system administration providers; and parties involved in a sale, transfer, merger or reorganisation of all or part of our business.

Some providers may act as independent controllers for particular processing activities rather than solely as processors. Where this applies, their own privacy information explains how they process personal data.

7.1 Online Booking and Payment Providers

We use Bookeo to manage online course bookings, reservations and associated customer communications. When you make a booking through Bookeo, information such as your name, contact details, selected course, session information, attendee details and booking information may be processed through Bookeo on our behalf.

We use Stripe to process online card payments. Payment information is transmitted securely to the payment provider. The BTR Hub does not receive or store your full payment card number or security code. We may receive limited payment and transaction information needed to confirm and reconcile payment, administer refunds and maintain accounting records.

Information collected for a course booking is used to administer that booking and provide the service you have requested. Any optional marketing choice is handled separately from the information required to complete your booking.

8. International Transfers

Some of our service providers operate internationally or use infrastructure located outside the United Kingdom. This means personal data may in some circumstances be processed outside the UK.

Where personal data is transferred to a country that has not been recognised as providing an adequate level of protection, we take steps to ensure that an appropriate transfer mechanism or safeguard is in place where required by law. This may include the UK International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses, an applicable adequacy regulation, or another lawful safeguard.

We periodically review relevant supplier arrangements and data-processing terms as part of our data protection and supplier-management processes.

9. Cookies and Information Collected Automatically

When you use our website, certain technical and usage information may be collected automatically. This can include pages viewed, time spent on pages, referring pages, browser and device information, approximate location derived from technical information, and IP address.

We use cookies and similar technologies for purposes such as operating our website, remembering preferences, understanding website usage and, where you have consented, analytics or marketing.

We obtain consent before placing non-essential cookies where required. You can change your cookie preferences using the cookie controls provided on our website. Further information is available in our Cookie Policy.

Aggregated or anonymised information may be used to understand website performance, visitor trends and service usage. Where information has been irreversibly anonymised so that an individual can no longer be identified, it is not personal data.

10. Your Data Protection Rights

Depending on the circumstances, data protection law gives you rights in relation to your personal data, including the right to:

- request access to personal data we hold about you;
- request correction of inaccurate or incomplete personal data;
- request erasure of personal data in certain circumstances;
- request restriction of processing in certain circumstances;
- object to processing based on legitimate interests in certain circumstances;
- object at any time to processing for direct marketing;
- request transfer of certain personal data to you or another organisation where the right to data portability applies; and
- withdraw consent at any time where we rely on consent.

These rights are subject to legal conditions and exemptions and do not always require us to delete or stop processing information.

You will not normally have to pay a fee to exercise your rights. We may, however, charge a reasonable fee or refuse a request where permitted by law if it is manifestly unfounded or excessive.

We may request information necessary to verify your identity before acting on a request. We aim to respond to valid requests within one month. Where a request is particularly complex or numerous, the law may permit additional time, in which case we will tell you.

You also have the right to complain about how we handle your personal data – see section 12.

11. How to Contact Us

If you have questions about this Privacy Notice, our use of your personal data, or wish to exercise a data protection right, please contact our Data Protection Lead. Email is the best way to reach us:

- **Email (preferred):** compliance@thebtrhub.com (for a rights request, please put 'Data subject request' in the subject line)

- **Telephone:** 020 8080 4990 (Option 4)
- **Post:** Data Protection Lead, The BTR Hub Limited, 2nd Floor, Fairchild House, Redbourne Avenue, London, N3 2BP

You can also make a request in another way, for example to any member of our team; it will be passed to our Data Protection Lead at compliance@thebtrhub.com and handled in the same way.

12. How to Complain

If you are unhappy with how we have handled your personal data, please tell us. The best way to make a data protection complaint is by email. You can complain to us by:

- emailing compliance@thebtrhub.com (please put 'Data protection complaint' in the subject line);
- telephoning 020 8080 4990 (Option 4); or
- writing to our Data Protection Lead at the address in section 11.

You can also raise a complaint with any member of our team, who will pass it to our Data Protection Lead at compliance@thebtrhub.com on the same working day. You do not need to use any particular words or form.

What happens next

- We will acknowledge your complaint within 30 days of receiving it, and usually much sooner.
- We will look into your complaint without undue delay, make appropriate enquiries, and keep you informed of our progress.
- We will tell you the outcome without undue delay, explaining what we found and any action we have taken.

If you are complaining on behalf of someone else, we will ask for evidence that you are authorised to act for them. We will only ask for proof of identity if we need it to be sure who you are. Our Data Protection Complaints Policy & Procedure, which explains the process in more detail, is available on request.

Complaining to the ICO

You also have the right to complain to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection. We would welcome the chance to put things right first, and the ICO may ask whether you have raised your concern with us, but you can contact the ICO at any time.

Information Commissioner's Office

4th Floor, No.3 Circle Square, 5 Hawkshaw Street, Manchester, M1 7BL

Telephone: 0303 123 1113

Website: ico.org.uk/make-a-complaint

13. Changes to This Privacy Notice

We may update this Privacy Notice from time to time to reflect changes in our services, systems, suppliers, legal requirements or data-processing activities. The current version will be published on our website and the date at the beginning of this notice will show when it was last updated.

Where a change materially affects how we use personal data, we will take appropriate steps to bring the change to the attention of affected individuals where required.