



Privacy Policy

Version: 3.0

Last updated: 20 August 2026

CONTENTS

1.	Introduction	3
2.	Who we are and how to contact us	3
3.	When we act as a controller and when we act as a processor	4
4.	The personal data we collect	5
5.	Why we process your personal data, and our lawful bases	7
6.	Recruitment	8
7.	Marketing	8
8.	Who we share your personal data with	9
9.	Artificial intelligence, profiling and automated decision making	10
10.	Cookies and similar technologies	11
11.	International transfers	12
12.	Information security	13
13.	How long we keep your personal data	14
14.	Microsoft Teams	15
15.	Personal data breaches	15
16.	Your rights	16
17.	Complaints	17
18.	Children	17
19.	Changes to this policy	17
20.	Version history	17

1. INTRODUCTION

1.1 At Abstract Group Limited ("Abstract", "we", "us", "our") we take the privacy of the people whose personal data we handle seriously. This policy explains what personal data we collect, why we collect it, the lawful basis on which we process it, who we share it with, how long we keep it and what rights you have.

1.2 It applies to visitors to www.abstract-group.com, to the personnel of our customers, prospective customers, suppliers and partners, to candidates who apply to us, and to visitors to our premises.

1.3 Third-party websites reached from our website or our marketing are not covered by this policy, and we accept no responsibility for their privacy practices.

1.4 We review this policy at least annually and whenever there is a material change to our processing. The current version is always published on our website.

2. WHO WE ARE AND HOW TO CONTACT US

2.1 Abstract Group Limited is registered in England and Wales under company number 10741640. Our registered office and principal place of business is 1st Floor, Harcourt House, The Coachworks, 21 The Calls, Leeds, England, LS2 7EH.

2.2 Abstract Group Limited is the controller for the processing described in this policy. References in this policy to "Abstract Group" are to Abstract Group Limited and its group companies.

2.3 We are registered with the Information Commissioner's Office under registration reference ZB623735.

2.4 We have appointed a Data Protection Officer, who can be contacted at dpo@abstract-group.com, on 0113 524 1068, or by post at the address above. The Officer is supported by responsible colleagues in each of our operating locations.

3. WHEN WE ACT AS A CONTROLLER AND WHEN WE ACT AS A PROCESSOR

3.1 We act as a controller where we decide the purposes and means of processing. That is the processing described in this policy: our website, our marketing, our customer and supplier relationships, our recruitment activity, and the security of our own systems and premises.

3.2 We also act as a processor. In delivering managed services, DevOps consultancy and service desk support we process personal data on behalf of our customers, on their documented instructions. Where we act as a processor:

- our customer is the controller, and their own privacy notice governs that processing;
- our processing is governed by written terms agreed with that customer, including the terms required by Article 28 of the UK GDPR;
- if you wish to exercise your rights in relation to data we hold as a processor, you should contact the relevant controller. If you contact us instead, we will refer your request to them without undue delay.

3.3 This policy does not describe the processing we carry out as a processor for our customers.

4. THE PERSONAL DATA WE COLLECT

4.1 We use the following definition: personal data is any data relating to an identified or identifiable living person processed by us or our subcontractors.

HOW WE COLLECT IT

Direct interactions. You give us your identity and contact details when you complete a form or correspond with us by post, telephone or email. This includes when you request our products or services, subscribe to our publications, ask for marketing content, enter a competition, promotion or survey, give us feedback, or contact us.

Automated technologies. As you use our website we collect technical data about your device, browsing actions and patterns, using cookies, server logs and similar technologies. Section 10 explains this in detail.

Third parties and publicly available sources. We may receive personal data from website analytics providers, from data brokers, credit reference agencies and aggregators, from professional social media sources such as LinkedIn, and from publicly available sources.

WHAT WE COLLECT

Contact data. Your name, job title, employer, email address, telephone number, postal address and social media identifiers.

Communication data. The content and metadata of communications between us, including emails, website form submissions, support tickets and, where we tell you in advance, recorded calls.

Usage data. IP address, approximate geographic location, browser type and version, operating system, referral source, pages viewed and navigation paths.

Service and account data. Records relating to services we provide to your organisation, including support requests, access records and correspondence.

Transaction data. Details of orders, invoices and payments between us and your organisation.

Recruitment data. Where you apply to us, your CV, employment and education history, references, right-to-work evidence, background check results and interview records.

Premises data. Sign-in and sign-out records for staff and visitors at our offices, held for health, safety and fire evacuation purposes.

Security data. Authentication events, audit logs and device information generated when you access systems we operate.

4.2 We do not seek to collect special category data through our website. Where it is necessary, for example health information provided to support a reasonable adjustment during recruitment, we process it only on an appropriate Article 9 condition and we tell you at the point of collection.

5. WHY WE PROCESS YOUR PERSONAL DATA, AND OUR LAWFUL BASES

5.1 The table below sets out our purposes and the lawful basis for each. It is not exhaustive; where we process for a purpose not listed, we will tell you at the time.

PURPOSE	PERSONAL DATA USED	LAWFUL BASIS
Business to business collaboration and managing relationships	Contact data, communication data	Performance of a contract, or our legitimate interests in maintaining commercial relationships
Providing and supporting our services, including service desk and managed service delivery	Contact data, communication data, service and ticket data	Performance of a contract, or our legitimate interests where you are the representative of a corporate customer
Newsletter subscriptions and marketing communications	Contact data, marketing preference data	Consent, or our legitimate interests where the soft opt-in under PECR applies
Processing orders, payments and transactions	Contact data, transaction data	Performance of a contract, and legal obligation for accounting records
Recruitment and candidate assessment	Recruitment data, including CVs, employment history, references, right-to-work evidence	Our legitimate interests in deciding whether to appoint you, steps taken at your request prior to a contract, and legal obligation for right-to-work checks
Operating our website and analysing its use	Usage data	Consent for non-essential cookies, and our legitimate interests in improving and securing our website
Managing physical access to our premises, including sign-in records	Sign-in records	Our legitimate interests in the safety and security of our people, visitors and premises, and legal obligation for fire safety
Information security, fraud	Usage data, authentication and	Our legitimate interests in

PURPOSE	PERSONAL DATA USED	LAWFUL BASIS
prevention and system monitoring	audit logs, device data	protecting our systems, our people and our customers
Establishing, exercising or defending legal claims	Any relevant category	Our legitimate interests in the assertion and protection of legal rights
Complying with a legal obligation, or protecting vital interests	Any relevant category	Legal obligation, or vital interests

5.2 Where we rely on legitimate interests, we have carried out an assessment balancing those interests against your rights and freedoms. You may request a summary of that assessment using the contact details in section 2.

5.3 Where we rely on consent, you may withdraw it at any time. Withdrawal does not affect the lawfulness of processing carried out before withdrawal.

6. RECRUITMENT

6.1 We collect personal data about applicants through the application and recruitment process, either directly from candidates or from an employment agency, a referrer, a referee or a background check provider.

6.2 We use it to determine eligibility and suitability for employment, including verifying references and qualifications and checking that you are legally entitled to work in the territory where the role is based; to decide about your recruitment or appointment and the terms on which you would work for us; to prevent and detect fraud; for quality and diversity monitoring; to comply with legal and regulatory requirements; to communicate with you about the process; and to keep records of it.

6.3 It is in our legitimate interests to decide whether to appoint you to a role. We may pass your personal data to our background check providers.

6.4 We are committed to ensuring that what we collect is appropriate for these purposes and does not constitute an invasion of your privacy.

7. MARKETING

7.1 Our aim is not to be intrusive, and we undertake not to ask irrelevant or unnecessary questions.

7.2 We may send you marketing material where you have consented, or where you are an existing customer contact and we are relying on the soft opt-in permitted under the Privacy and Electronic Communications Regulations.

7.3 You can opt out at any time using the unsubscribe link in any marketing communication, or by contacting our Data Protection Officer. We will keep a minimal suppression record so that we can continue to honour your objection.

8. WHO WE SHARE YOUR PERSONAL DATA WITH

8.1 We do not sell or rent personal data.

8.2 We share personal data with the categories of recipient below. Where a recipient acts as our processor they do so under a written contract meeting the requirements of Article 28 of the UK GDPR, and may use the data only to perform their function for us.

CATEGORY OF RECIPIENT	EXAMPLES	WHERE PROCESSED
Cloud productivity, identity and hosting providers	Microsoft (Microsoft 365, Azure, Entra ID, Teams)	United Kingdom and European Union
Website, CRM and marketing platform	HubSpot	European Union
Content delivery and web security	Cloudflare	Global network, including outside the UK
Service management and ticketing	HaloPSA	United Kingdom
Monitoring and observability	Datadog (EU instance)	European Union
Email security	Barracuda Email Gateway Defense	European Union
Assistive artificial intelligence tooling	Anthropic (Claude)	United States, with multi-region processing possible
Background check and recruitment providers	Where relevant to a candidate application	United Kingdom
Professional advisers, accountants, auditors and certification bodies	Legal, accountancy and ISO certification bodies	United Kingdom
Regulators and law enforcement	Where we are under a legal obligation to disclose	United Kingdom

8.3 We may also disclose personal data where we are required to do so by law or legal process; to protect and defend our rights and property or those of our customers; to prevent fraud; to protect against abuse, misuse or unauthorised use of our systems; or to protect the personal safety or property of our customers, other persons or the public.

8.4 We may disclose personal data to a prospective purchaser of our business, subject to appropriate confidentiality protections.

8.5 A current list of our processors and sub-processors is maintained in our Approved Supplier Register and is available to customers on request.

9. ARTIFICIAL INTELLIGENCE, PROFILING AND AUTOMATED DECISION MAKING

9.1 We do not make decisions producing legal or similarly significant effects about you based solely on automated processing.

9.2 We use assistive artificial intelligence tools to support our internal work, for example to summarise documents, draft text and assist with analysis. Their use is governed by our AI Acceptable Use Policy. A person always reviews the output and remains responsible for any decision.

9.3 Where personal data is entered into these tools it is processed under contractual terms that prohibit the provider from using our data to train their models, and is subject to the transfer safeguards in section 11.

9.4 We restrict what may be placed into these tools. Special category data and customer data are not processed in this way unless a specific assessment has been completed and approved.

9.5 Our marketing and analytics platforms build a picture of how visitors interact with our website and our campaigns, which may involve tracking across devices and channels. These technologies are only used where you have consented to the relevant cookies, and you can withdraw that consent at any time.

10. COOKIES AND SIMILAR TECHNOLOGIES

10.1 A cookie is a small text file placed on your device by your browser when you visit our website. It allows our systems to recognise your browser on a return visit and helps us understand which parts of the site are used most.

10.2 We use the following categories.

CATEGORY	WHAT IT DOES AND WHETHER CONSENT IS NEEDED
Strictly necessary	Required for the website to work and for web security and bot protection. Set without consent, as permitted by law.
Statistics	Helps us understand how visitors use the website by collecting information in aggregate. Set only with your consent.
Marketing	Enables personalisation, campaign measurement and embedded content such as video. Set only with your consent.

10.3 You choose which non-essential cookies to accept through the cookie settings presented when you visit our website. If you need to change your choice, clear the cached cookies from our site in your browser and you will be presented with the selection again on your next visit.

10.4 A live report of every cookie in use on our site, including its name, provider, purpose and duration, is published in our Cookie Declaration at www.abstract-group.com/legal/cookie-declaration.

10.5 Cookies themselves do not contain personal information, but we may link information stored in cookies to personal data you submit while on our site.

10.6 Most browsers let you block or delete cookies. Blocking all cookies will affect the usability of our website and of many others.

11. INTERNATIONAL TRANSFERS

11.1 We are a United Kingdom business with operating locations in the United Kingdom, India and Romania. Personal data covered by this policy may therefore be accessed by our personnel outside the United Kingdom, including by our service desk.

11.2 Some of our processors are established outside the United Kingdom, including in the United States.

11.3 Where we transfer personal data outside the United Kingdom we do so on the basis of one of the following:

- adequacy regulations made by the Secretary of State, including transfers to the European Economic Area;
- the International Data Transfer Agreement, or the UK Addendum to the European Commission Standard Contractual Clauses, supported by a transfer risk assessment; or
- another lawful transfer mechanism permitted under United Kingdom data protection law.

11.4 A copy of the safeguards applied to a particular transfer can be obtained from our Data Protection Officer.

12. INFORMATION SECURITY

12.1 We operate an Information Security Management System certified to ISO 27001:2022 and a Quality Management System certified to ISO 9001:2015. We also hold Cyber Essentials and Cyber Essentials Plus certification.

12.2 We employ physical, administrative and technical safeguards to protect personal data from unauthorised access, improper use or disclosure, unauthorised modification, and unlawful destruction or accidental loss. These include role-based access control on a least-privilege basis, multi-factor authentication, encryption in transit and at rest, managed endpoint protection, email security filtering, monitoring and logging, and formal change management.

12.3 Access is limited to those with a legitimate need. Our employees and the third parties we engage are bound by confidentiality obligations and must observe the principles in this policy. Our staff receive information security and data protection training.

12.4 We assess our suppliers before engagement and review them periodically.

12.5 No system is completely secure, and we cannot guarantee the security of data transmitted to us over the internet.

13. HOW LONG WE KEEP YOUR PERSONAL DATA

13.1 We do not keep personal data for longer than is necessary for the purposes for which it was collected. Retention is governed by our Records Retention Schedule, and some categories are governed by statutory requirements such as those for tax and audit.

13.2 The following periods are indicative. Where a longer period is required by law, or is necessary for the establishment, exercise or defence of legal claims, we will retain the data for that longer period.

CATEGORY OF DATA	INDICATIVE RETENTION	MEASURED FROM
Enquiries that do not lead to a contract	Up to 24 months	Date of most recent contact
Customer contact and communication data	Duration of the contract plus 6 years	End of contract
Website usage and analytics data	Up to 26 months	Date of collection
Marketing preference and suppression records	For as long as needed to honour the preference	Ongoing
Unsuccessful candidate recruitment data	Up to 12 months	Date of decision
Building sign-in records	Minimum 2 years	Date of visit
Microsoft Teams content, call history and call quality data	As set by the retention policies applied to the relevant Microsoft 365 workload	Date of the meeting or call
Security, authentication and audit logs	The period necessary for security monitoring, investigation and incident response	Date of event
Statutory accounting records	6 years	End of the relevant financial year

13.3 If you would like more detail on the retention applied to a particular category, contact our Data Protection Officer.

13.4 When personal data reaches the end of its retention period it is securely deleted or destroyed.

14. MICROSOFT TEAMS

14.1 We provide employees and customers with access to Microsoft Teams. In providing that service we have access to the following personal data:

- Content: your meetings and conversations, chats, voicemail, shared files, recordings and transcriptions.
- Profile data: data shared within Abstract or within your own organisation if you are a customer, such as your email address, profile picture and telephone number.
- Call history: a record of the calls you make, which allows you to review your own call records.
- Call quality data: meeting and call diagnostics available to our system administrators, used to diagnose poor call quality and service usage issues.
- Support and feedback data: information relating to troubleshooting tickets or feedback submitted to Microsoft.

14.2 We process this data in our legitimate interests in providing the service, offering a communication platform to our internal and external users, allowing the platform to operate, and diagnostics and service improvement.

14.3 We pass personal data to Microsoft as part of operating this service. Microsoft's privacy statement explains their processing.

15. PERSONAL DATA BREACHES

15.1 We maintain an incident management process covering the identification, containment, assessment and reporting of personal data breaches.

15.2 Where a breach is likely to result in a risk to the rights and freedoms of individuals we report it to the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of it. Where the risk is high, we notify the affected individuals.

15.3 Where we become aware of a breach affecting personal data we process on behalf of a customer, we notify that customer without undue delay.

16. YOUR RIGHTS

16.1 Subject to certain conditions, exemptions and exceptions set out in data protection law, you have the following rights:

- Right of access — to confirmation of whether your personal data is being processed and, if so, to a copy of it and information about the processing.

- Right to rectification — to have inaccurate personal data corrected and incomplete data completed, and to have recipients informed of the correction.
- Right to erasure — to have your personal data erased. If it was made public we will take reasonable steps to inform other controllers and recipients of your request.
- Right to restriction of processing — to have processing limited to mere storage.
- Right to data portability — to be provided with your personal data in a reusable format and, where you ask, to have it transmitted directly to another controller.
- Right to object — to object to processing on certain grounds, and at any time to object to direct marketing.
- Right to withdraw consent — where our processing is based on consent.
- Rights in relation to automated decision making — to obtain human intervention, express your point of view, receive an explanation and challenge the decision.
- Right to complain to a supervisory authority.

16.2 To exercise any of these rights, contact our Data Protection Officer at dpo@abstract-group.com, or complete the contact form at www.abstract-group.com setting out your request.

16.3 We will require appropriate and valid proof of identity before sharing any personal data.

16.4 We will respond within one month of receiving a valid request. We may extend this by up to two further months where the request is complex or where we have received a number of requests from you, and we will tell you if we do.

16.5 We do not normally charge a fee, but we may charge a reasonable fee, or refuse to act, where a request is manifestly unfounded or excessive.

17. COMPLAINTS

17.1 If you are unhappy with how we have handled your personal data, please contact our Data Protection Officer first so that we have the opportunity to put it right.

17.2 You also have the right to complain directly to the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, by telephone on 0303 123 1113, or at ico.org.uk.

18. CHILDREN

18.1 Our website and services are directed at businesses and are not intended for children. We do not knowingly collect personal data relating to children. If you believe we have done so, please contact our Data Protection Officer and we will delete it.

19. CHANGES TO THIS POLICY

19.1 We may modify this policy from time to time to reflect changes in our business or in the way we use information. Where we do, we will publish the revised version on our website and update the version history below.

19.2 Unless we say otherwise, we will use information in accordance with the policy in effect when the information was collected. If we materially change the way we use or disclose personal data collected under an earlier version, we will notify affected individuals and provide a reasonable opportunity to object.

20. VERSION HISTORY

VERSION	DATE PUBLISHED	SUMMARY
1.0	13 April 2024	Initial issue.
2.0	14 October 2024	Second issue. Added recruitment, Microsoft Teams and expanded cookie sections.
3.0	20 August 2026	Third issue.