



Privacy Policy For Human Talent (UK/EEA)

November 7th, 2024



Abra Group – Human Talent Privacy Notice (UK/EEA)

Last updated: November 7th, 2024

CONTENT

- 1. Introduction**
- 2. Personal data we collect and Process**
- 3. How we use your personal data (our purposes) and our legal basis for Processing it**
- 4. Who we share your personal data with**
- 5. How we keep your personal data secure**
- 6. International data transfers**
- 7. Data retention**
- 8. Your data protection rights**
- 9. Updates to this Privacy Notice**
- 10. How to contact us**

We recommend that you read this Notice in full to ensure you are completely informed about how we collect, Process, share and protect your personal data. However, if you only want to access a particular section of this Notice, then you can click on the relevant link above to jump to that section.

This Employee Privacy Notice (this “Notice”) applies to all employees, candidates or applicants for employment, officers, collaborators, retirees, or related third parties who are located in the UK or European Economic Area (“EEA”) or whose data is received, collected, managed, used, transmitted, stored, preserved, transferred or otherwise processed in any form, whether oral, electronic or written (collectively, “Processed” or “Processing”) by us in connection with our UK and/or EEA establishments (collectively, “UK Human Talent”) of Abra Group Limited (the “Parent Company”), its nonoperational subsidiaries Abra Group Platform Services LLC and Abra Global Finance, and/or any future Parent Company affiliates or subsidiaries acquired, formed, incorporated or otherwise created hereafter as of the date this Notice was last updated (the “Effective Date”) which do not already have a separate respective governing privacy policy in place as of the date of acquisition or creation (collectively, “Abra”, “our”, “us”, “we”, or the “Companies”). This Notice does not cover or govern our operational companies with governing privacy policies already in place as of the Effective Date (the “Operational Companies”). For purposes of the Operational Companies and their personal data collection and use, their respective privacy policies shall govern and this Privacy Policy shall only be applicable and govern the personal data collection and use of Abra. As it relates to UK Human Talent, this Notice shall govern and supersede our Privacy Policy.

When we refer to “staff” or “staff members”, we mean persons who work for (or who have worked for) us, whether employees or not, whether on a part-time, temporary or full-time basis, and including current and former employees, contingent workers, contractors, interns, trainees and others working at or attached to us. When we refer to “applicants” we mean persons applying to become staff whether on a part-time, temporary, or full-time basis. All references to “employment” shall apply equally to engagement of non-employees, and to applications for employment or engagement. For the avoidance of doubt, (a) designation as a “staff member” under this Notice and/or for the purposes of any data protection laws is not, of itself, an indication of the existence of a contract of service or employment relationship for any other purpose or under any other law; and (b) nothing in this Notice shall be construed as forming part of the contractual relationship between us and you.

1. Introduction

We are committed to handling personal data responsibly and in accordance with applicable law. We have issued this Notice to describe how we handle personal data that we hold about our staff and applicants (collectively referred to as “you”). This Notice sets out the personal data that we collect and Process about you, the purposes of the Processing and the rights that you have in connection with it. If you are in any doubt regarding the applicable standards, or have any comments or questions about this Notice, then please contact us using the contact details under the “[How to contact us](#)” heading in Section 10, below.

2. Personal data we collect and Process

In the course of your relationship as UK Human Talent with us, we will Process personal data about you and your dependants, beneficiaries, and other individuals whose personal data has been provided to us.

2.1. Sources of personal data

We collect this personal data from the following different sources:

- **Information that you provide directly:** When your UK Human Talent relationship starts with us, the initial information about you that we Process is likely to come from you directly. For example, contact details, bank details and information on your immigration status and whether

you can lawfully work. We may also require references and information to carry out background checks.

In the course of your employment or engagement, you may be required to provide us with information for other purposes such as sick pay and family rights (e.g. maternity and paternity leave and pay). If you do not provide information that you are required by statute or contract to give us, you may lose benefits or we may decide not to employ/engage you or to end your contract. If you have concerns about this in a particular context, you should speak to the applicable human resources management department.

- **Information from third parties:** In the course of your employment with us, we may receive personal data relating to you from others, including from recruitment agencies, academic institutions, referees, background checking agencies and other third parties during your recruitment. [We may also receive personal data relating to you from external training and/or survey providers, your medical advisor, occupational health providers, security clearance providers, staff benefits providers, landlords of premises and premises security providers, local tax authorities, payroll agents and tax/financial advisers.
- **Information that we collect indirectly:** We collect your personal data indirectly, including through our IT systems and other devices.
- **Information that we collect from publicly available sources:** We may collect information about you from news sources and/or social media platforms, for example in connection with any investigation or formal procedure concerning the same (for instance, for the investigation of an allegation that a staff member has breached our rules on social media use or conduct generally).

2.2. Categories of personal data

The table below describes the categories of personal data we collect from and about you and your dependants, beneficiaries and other individuals as well as the source of that information.

Data Categories	Personal Data Description	Source
Identity Data	Name or alias, gender, passport number, driver's license number, social security number or other government-issued identification number, tax registration number and other details in and copies of identity documents.	• Directly from you
Contact Data	Home and business address, personal and work telephone number, personal and work email addresses, emergency contact details (including emergency contact person and their telephone number).	• Directly from you
Application Data	Notes made by interviewers or other staff in connection with your application; criminal records data (when permitted), results of reference checks and screening such as verification of education and employment history, screening checks such as against politically exposed persons registers, disbarment checks and other searches relevant to the role for which you are applying; and nationality and country of birth, citizenship and right to work information, government identification documents	• Directly from you • Third parties

	(including passports and residency permits) and, where relevant, visa information.	
Employment Data	Job title/position, staff reference number, photograph, office location, employment contract, employment start and leaving date, working times and days and records relating to performance, disciplinary processes, training history, grievance procedures, accidents, sickness/holiday, leave (including parental and adoption leave), family rights and working days and hours.	• Directly from you • Third parties
Background Data	Age, date of birth, marital status, gender, pronouns, academic/professional qualifications, education, CV/résumé, criminal records data and security clearance status.	• Directly from you • Third parties
Family Data	Including information relating to your next-of-kin, spouse, partner, dependants and other family members (in particular, their names and dates of birth and details of entitlements under relevant benefit schemes).	• Directly from you
Payroll Data	Banking details, tax information (such as tax registration number), withholdings, salary, benefits, expenses, loans, company allowances, stock and equity grants.	• Directly from you • Third parties
Audio/Visual Data	Photographs and other audio-visual information used for workplace initiatives and promotional materials.	• Directly from you • Third parties
Sensitive Personal Data	Information that reveals your racial or ethnic origin, religious, political or philosophical beliefs, genetic data, biometric data for the purposes of unique identification, trade union membership, information about your health (including mental health and vaccination status), disability, sexual orientation.	• Directly from you
Communication Data	Contact details and content of communications when you communicate with us, for example, to inquire about employee benefits.	• Directly from you • Automatic collection
IT Data	Information required to provide access to company IT systems and networks (and information collected by/through those systems) such as IP addresses, log files and login information. IT Data may also include inferred location based on your IP address or activities, device identifiers associated with your computer or device, mobile carrier and related information, activity logs, and other information about activities you engage in on Abra property, equipment, accounts, systems and networks. Abra will on occasion monitor and review your use of Abra equipment, accounts, information technology systems and networks, including its phone networks,	• Automatic collection

	computer networks, including those used to access the Internet, videoconferencing systems and other company-provided electronic communications tools. Abra may access and review electronic files, messages, and emails sent or stored on its information technology systems, including accounts, computers and devices provided to you.	
Security and Access Data	Closed-circuit television (CCTV) footage in public or common areas in our premises and near our premises (such as in car parking areas and in which case footage may include vehicle licence plates). It may also include other information obtained through electronic means such as security records (e.g. swipe card records, building entry/exit data to which Abra may from time to time have access) and if you are visiting a premises, physical or electronic guest book information containing name, photograph, vehicle licence plate and person(s) you are visiting).	• Automatic collection • Third parties (where used for CCTV, security and access systems)
Ethics Reporting Data	In addition to certain Identity Data and Contact Data such as name, telephone number and email, which office you work from and also employee reference number (unless you report anonymously), IP address and inferred location based on your IP address, device identifiers associated with your computer or device and activity logs. Information reported to us, which may include personal data about other individuals such as those that have engaged in alleged misconduct (including criminal activity). Information collected in connection with an investigation, such as description of the alleged misconduct, witness statements and evidence gathered to ascertain the facts and circumstances. Conclusions of the investigation.	• Automatic collection • Directly from you • Third parties
Survey Data	Answers to survey questions, date and time survey completed and IP address. Although this data will usually be aggregated, technically (even though we do not intend to look at this data), you may be identifiable from your IP address when completing a survey.	• Automatic collection • Directly from you

3. How we use your personal data (our purposes) and our lawful basis for Processing it

We Process the personal data that we collect from and about you for a variety of employment-related purposes described in this Notice or for purposes that we explain to you at the time we collect your information.

3.1. Purposes and lawful basis for Processing personal data: The following table provides more details on our purposes for Processing your personal data and the related legal bases. The legal basis under which your personal data is Processed will depend on the data concerned and the specific context in which we use it, as further described in the following table below.

Purpose/Activity	Type of personal data	Lawful
Administering your contract including entering it, performing it and changing it	Identity Data Contact Data Employment Data Communications Data Including information on your terms of employment or engagement, your payment and benefits, your participation in pension arrangements, life and medical insurance and any bonus or share scheme.	• Performance of a contract with you • Legitimate interests
Contacting you or others on your behalf	Identity Data Contact Data Communications Data Spouse and Dependant data	• Performance of a contract with you • Legitimate interests
Payroll administration	Identity Data Contact Data Payroll Data Including your bank account details, salary, pension contributions and details of other benefits, and information on tax and social security/national insurance, information on attendance, holiday and other leave and sickness absence.	• Performance of a contract with you • Legitimate interests
Supporting and managing your work and performance and any health concerns	Employment Data Sensitive Personal Data (specifically health data) IT Data Including information connected with your work, anything you do at work and your performance including records of documents and emails created by or relating to you and information on	• Performance of a contract with you • Legitimate interests

	your use of our systems including computers, laptops or other devices. Management information regarding you including notes of meetings and appraisal/performance records. Information relating to your compliance with our policies. Information concerning disciplinary allegations, investigations and relating to grievances in which you are or may be directly or indirectly involved. To the extent required or permitted by local law, information concerning your health, including self-certification forms, medical and occupational health reports.	
Changing or ending your working arrangements	Identity Data Contact Data Employment Data Including information connected with anything that may affect your continuing employment or the terms on which you work including any proposal to promote you, to change your pay or benefits, to change your working arrangements or to end your employment.	• Performance of a contract with you • Legitimate interests
Physical and system security	Security and Access Data IT Data Including CCTV images and records of use of swipe and similar entry cards/systems. To the extent required or permitted by local law, records of your use of our systems including computers, phones and other devices and passwords.	• Legitimate interests
Providing references in connection with you finding new employment	Employment Data Specifically, information on your working for us and on your performance.	• Legitimate interests
Providing information to third parties in connection with	Employment data	• Legitimate interests

transactions that we contemplate or carry out	Including information on your contract and other employment data that may be required by a party to a transaction such as a prospective purchaser, seller or provider of outsourced services.	
Monitoring of diversity and equal opportunities	Background Data Sensitive Personal Data Specifically, to the extent required or permitted by local law, information on your nationality, racial and ethnic origin, gender, sexual orientation, religion, philosophical beliefs, disability, age and other diversity markers.	• Legitimate interests • Legal obligations • Public interest
Monitoring and investigating compliance with law, regulations policies, codes of practice and rules both generally and specifically	Contact Data Employment Data Background Data Ethics Reporting Data IT Data Security and Access Data Payroll Data Communications Data Sensitive Personal Data We expect our staff to comply with our policies and rules and monitor our systems to check compliance. If we have specific concerns about compliance, we may check systems and other data to look into those concerns (e.g. log in records, records of usage and emails and documents, CCTV images). We may from time-to-time conduct investigations if we receive any report of non-compliance with the law and regulations or with our codes of practice, policies and rules.	• Legitimate interests • Legal obligation • Public interest • In relation to Sensitive Personal Data: Employment obligations, Legal Claims, or in limited cases Public interest
Disputes and legal proceedings	Contact Data Employment Data Payroll Data IT Data	• Legitimate interests • Legal obligation • In relation to Sensitive Personal Data: Legal Claims.

	Communications Data Sensitive Personal Data Any other information relevant or potentially relevant to a dispute or legal proceeding affecting us.	
Day to day business operations including marketing	Contact Data Employment Data Audio/Visual Data Specifically, information used on global or local internal or external directories to identify what you do and how you can be contacted (to enable collaboration with colleagues and others). Any other Information relating to the work you do for us, your role and contact details. This may include a picture of you for internal or external use.	• Legitimate interests
Carrying out staff surveys	Survey Data We will typically aggregate survey responses and do not require details of specific persons responding. However, if you are completing a survey electronically even if no direct identifying information is provided, you technically might be identifiable from your IP address. We are only interested in looking at the aggregated information and not any information linking individuals to survey responses.	• Legitimate interests
Maintaining appropriate business records during and after your employment or engagement	Employment Data Other information relating to your work, anything you do at work and your performance relevant to such records.	• Performance of a contract with you • Employment obligations • Legal claims • Legitimate interests
Emergency medical treatment	Family Data Health Data Any other information required to notify your close contact(s) of any incident at or in connection with work and to allow responsible people to administer emergency medical treatment.	• Vital interests

Acquisitions, divestitures and integrations; restructuring and relocation	Contact Data Employment Data Background Data Ethics Reporting Data IT Data Security and Access Data Payroll Data Communications Data Sensitive Personal Data Information will be Processed and potentially shared with a third party (such as a purchaser of the business) relating to your role - as relevant to the particular context.	• Legitimate interests • In relation to Sensitive Personal Data: Employment obligations, or in limited cases Consent.
Complying with anti-money laundering and other legal requirements	Identify Data Contact Data Any other data we are required to disclose to satisfy anti-money laundering or other legal requirements.	• Legitimate interests • Legal obligations (e.g., UK Companies Act 2006) • Public interest

3.2. Lawful basis for Processing descriptions: Depending on our purpose for collecting your information, we rely on one of the lawful bases described in the table below (i.e. legally permitted reasons under GDPR/UK GDPR).

Lawful Basis	Description
Performance of a contract with you	We require certain personal data to carry out our contractual duties and exercise our contractual rights as an employer.
Consent	In certain circumstances, we may ask for your consent (separately from any contract between us) before we collect, Process or disclose your personal data, in which case you can voluntarily choose to give or deny your consent without any negative consequences to you. In general, Processing of your data in connection with employment will not be conditional on your consent.
Legitimate interests	We may collect, Process or disclose your personal data for the legitimate interests of either Abra or a third party, but only when we are confident that your privacy rights will remain appropriately protected. If we rely on our (or a third party's) legitimate interests, these interests will normally be to: operate, manage, administer our respective businesses effectively and

	properly. Where we require your data to pursue our legitimate interests or the legitimate interests of a third party, it will be in a way which is reasonable for you to expect as part of the running of our business and which does not materially affect your rights and freedoms.
Legal obligation	There may be instances where we must Process and retain your personal data to comply with laws or to fulfil certain legal obligations. For example, providing a safe place of work and avoiding unlawful discrimination.
Public interest	There may be instances where Processing your data is necessary to perform a specific task in the public interest or for a substantial public interest which could include, for example, prevention and detection of unlawful acts such as fraud or other crime or assisting third parties prevent or detect unlawful acts or dishonesty, or for diversity and inclusiveness monitoring purposes.
Vital interests	Although unlikely, it may be necessary to Process your data (including Sensitive Personal Data such as health data) to protect someone's life. In general, we will not Process your data on this ground but there may be rare occasions when we need to do so, for example, if we need to Process personal data to save your life and administer emergency medical treatment.
Employment obligations	Processing of your data where necessary for the purposes of your or our legal obligations and rights in relation to employment such as avoiding unlawful discrimination, or to provide occupational health and to assess working capacity.
Legal claims	To establish, make or defend legal claims.

4. Who we share your personal data with

We take care to allow access to personal data to only those who require such access to perform their tasks and duties, and to third parties who have a legitimate purpose for accessing it. In such certain scenarios where we permit a third party to access personal data, we will implement appropriate measures to ensure the information is used in a manner consistent with this Notice and that the security and confidentiality of the information is maintained.

We share your personal data with the following categories of recipients:

- **Our group companies** operating in the UK, Europe, and around the world in order to administer human resources, staff member compensation, and benefits at an international level within our human resources department's platform or the human resources platform of any third party engaged by us to provide services related to human resources management (our "[HR Platform](#)"), as well as for other legitimate business purposes such as IT services/security, tax and accounting, and general business management;
- **Third party service providers and partners** on a "need to know basis" and in accordance with applicable data privacy law. We may disclose your data if it is necessary for our legitimate interests as an organisation or the interests of a third party. We may also disclose your personal data if you consent, where we are legally required to disclose, and in connection with criminal or regulatory investigations.

Specific examples of such third parties and the circumstances in which your personal data may be disclosed to them include the following:

- **Any competent law enforcement body, regulatory, government agency, court or other third party** (such as our professional advisers) where we believe disclosure is necessary (i) as a matter of applicable law or regulation (e.g. to provide certain salary information to tax authorities), (ii) to exercise, establish or defend our legal rights, or (iii) to protect your vital interests or those of any other person;
- **A successor** (and its agents and advisers) in connection with any actual or proposed purchase, merger or acquisition of any part of our business as permitted by law and/or contract, provided that we inform the successor it must use your personal data only for the purposes disclosed in this Notice;
- **Any other person with your consent** to the disclosure (obtained separately from any contract between us);
- **Our service providers.** Our key providers for the following services:

Services	Personal data
Benefit/reward plan service providers (including medical insurance providers)	Contact Data Identity Data Family Data Sensitive Personal Data (such as health data) Background Data (such as gender, age, and month and day of birth)
Payroll, tax and expense administration support services	Contact Data Identity Data Payroll Data
Providers of our HR Platform	Contact Data Identity Data Employment Data Background Data Family Data Payroll Data Sensitive Personal Data

Providers of IT and communications infrastructure (including for data storage purposes) and/or provide business continuity services	Contact Data Identity Data IT Data Employment Data Background Data Family Data Payroll Data Audio/Visual Data Sensitive Personal Data Communication Data
Relocation, travel and/or travel permit co-ordinators/services (in connection with work-related travel)	Contact Data Identity Data Family Data Sensitive Personal Data (such as allergies, disabilities and vaccination status)
Staff training and/or qualifications and staff survey services	Contact Data Employment Data (such as learning and performance records) IT Data Communication Data
Auditors, advisors, legal representatives and similar agents in connection with the advisory services they provide to us for legitimate business purposes	Contact Data Identity Data Employment Data Background Data Payroll Data Sensitive Personal Data Communication Data

Ethics reporting provider	Contact Data
	Identity Data
	Employment Data
	Background Data
	Ethics Reporting Data
	IT Data
	Security and Access Data
	Communications Data
	Sensitive Personal Data

5. How we keep your personal data secure

We use appropriate technical and organisational measures to protect the personal data that we collect and Process about you. These measures are designed to provide a level of security appropriate to the risk of Processing. We rely on a number of technological security tools and implement industry-recognized security practices, including but not limited to: information transmission and storage through secure mechanisms, such as use of secure protocols, securing technological components, encryption, restricting access to information only to authorized personnel, backup of information, secure software development practices, firewalls, antivirus, and IPS, among technological security tools.

6. International data transfers

As we operate internationally, in some cases, where your personal data is transferred to one of the other Companies or third party, it is Processed in countries other than the UK/EEA. These countries may have data protection laws that are different to the laws of the UK/EEA (and, in some cases, may not be as protective).

Specifically, Companies are based in the United Kingdom, and United States of America, Cayman Islands [and Brazil]. Our third party service providers and partners operate around the world. This means that when we collect your personal data we will Process it in any relevant country.

Where we transfer your personal data to countries and territories outside of the UK or EEA that have been formally recognized as providing an adequate level of protection for personal data, we rely on the relevant “adequacy decisions” from the European Commission and “adequacy regulations” (data bridges) from the Secretary of State in the UK.

Where the transfer is not subject to an adequacy decision or regulations, we have taken appropriate safeguards to ensure that your personal data will remain protected in accordance with this Privacy Notice and applicable laws.

7. Data retention

We retain the personal data we collect from you where we have an ongoing legitimate business need to do so (for example, to comply with applicable legal, tax or accounting requirements). Generally, this means your personal data will normally be retained for at least two (2) years following the end of your employment to allow a reasonable period of time to respond to employment or work-related inquiries or to deal with any legal matters (e.g. judicial or disciplinary actions), document the proper termination of your employment or work relationship (e.g. to tax authorities), or to provide you with ongoing pensions or other benefits.

If you are not successful as a candidate, we may still keep your application and associated data for up to one (1) year to allow us to consider you for other suitable openings within Abra in the future unless you request that we delete your application.

8. Your data protection rights

Individuals located in the UK and EEA have the following data protection rights. To exercise any of them see specific instructions below or contact us using the contact details provided under the “[How to contact us](#)” heading, in Section 10, below.

- You may **access, correct, update or request deletion** of your personal data.
- You can **object to Processing** of your personal data, ask us to **restrict Processing** of your personal data.
- If we have collected and/or Processed your personal data with your consent, then you can **withdraw your consent** at any time by using the contact details provided under the “[How to contact us](#)” heading, in Section 10, below. Withdrawing your consent will not affect the lawfulness of any Processing we conducted prior to your withdrawal, nor will it affect Processing of your personal data conducted in reliance on lawful Processing grounds other than consent.
- You have the **right to complain to a supervisory authority** about our collection and use of your personal data. For more information, please contact your local supervisory authority. Contact details for supervisory authorities in Europe are available [here](#) and for the UK [here](#). Certain supervisory authorities may require that you exhaust our own internal complaints procedures before looking into your complaint.

We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws.

9. Updates to this Privacy Notice

We may update this Notice from time to time in response to changing legal, regulatory, technical or business developments. We encourage you to check back at this website periodically in order to be aware of the most recent version of this Notice.

You can see when this Notice was last updated by checking the “last updated” date displayed at the top of this Notice.

10. How to contact us

If you have any questions or concerns about our use of your personal data, please contact us using the following details: compliance@abragroup.net.

If you are employed or engaged in (or applying for) a contract based in the EEA or UK, the controller of your personal data is Abra Group UK.