bluesource

Privacy Policy (HR)

Last updated 11 April 2023

At bluesource, we are committed to protecting and respecting your privacy.

Your privacy is important to us and this privacy policy ("Policy") explains what personally identifiable information ("PII") we collect about you, why we need it, how we use it, the conditions under which we may disclose it to others and how we keep it secure.

We may change this Policy from time to time, so please occasionally check this Policy, available from the HR Policy section the Company's Intranet and also contained within the Employee Handbook, to ensure that you are up to date with any changes. By accepting employment with bluesource Information Limited, you are agreeing to be bound by this Privacy Policy and any revisions to it.

Any questions regarding this Policy and our privacy practices should be sent to privacy@bluesource.co.uk or by contacting the Head of Operations. Alternatively if it relates to an HR matter, please contact human.resources@bluesource.co.uk.

Who are we?

bluesource Information Limited (the "Company"), is private limited company registered in England, under number 4064193, with our registered office at: 122 Tooley Street, London, SE1 2TU. The Company comprises of Bluesource Information Limited and its trading subsidiaries.

We act as a Data Controller for HR related PII under certificate number ZA155583 with the ICO.

Legal basis for processing PII

To keep and maintain records relating to your employment/contract with the Company, it will be necessary to record, keep and process reasonable personal data relating to you on computer and in hard copy form. To the extent that it is reasonably necessary in connection with your employment and the Company's responsibilities as an employer, this data may be disclosed to others, including other employees of the Company or any Group Company, the Company's professional advisers, payroll provider, the Inland Revenue, the police and any regulatory and other authorities. As an employee, you consent to the Company recording, processing, using and disclosing personal data relating to yourself, as set out above, including the transmission of such data overseas whether outside the EU or otherwise. This consent does not affect your rights under the Data Protection Act 2018 or as superseded by the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

How do we collect information from you?

Information you give us

If you are under contract to work for bluesource as an employee or contractor, etc., you will be asked to supply certain PII which is reasonably required for the purpose of contracting and maintaining our relationship with you and to be able to provide employment, and fulfill any legal or legislative requirement, such as for identity verification, taxation, modern slavery. PII may be collected directly or via a contract, form, email or other such document.

We also obtain information about you throughout your employment with the Company, take on certain responsibilities and job roles, and subscribe to employee benefits.

Additionally as with external contacts, information may be gathered when you visit our website, subscribe to one of our news feeds (via the website, follow us via LinkedIn or Twitter, etc.).

We may also be passed your information from certain bluesource partners, such as recruitment agencies and previous employers in relation to your employment with us and assume that any necessary consents have been received from the relevant data controller.

We may combine information about you that we have with information we obtain from different services we provide to you.

Certain types of more sensitive information such as your credit history may be required for a specific purpose and where such information is required, your explicit consent will be sort before gathering this information for a specified purpose.

Information we get from the use of our services

In addition to the above, PII may also be contained within documentation/correspondence produced or received in the course of employment, such as a named individual in a project brief, proposal, quotation, contract, or other such document you have been involved with (collectively "Documents").

When you use our services we may automatically collect and store certain information in server or application logs, which may include:

- Details of when you accessed the service;
- Telephony log information, such as your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls. your access from a security perspective;
- IP address used to access the service; and
- Cookies that may uniquely identify your browser, search engine or preferences. (Please refer to Bluesource's Cookie Policy for further information, available at www.bluesource.co.uk).

What type of information do we collect about you?

The PII we collect from you will be appropriate, specific and minimalized for the purpose of providing employment to you and HR related services. The following PII is typically collected and for the following reasons:

Name	to verify identity and identify you as an individual
Date of birth	to verify identity, pension and medical protection provision
Personal contact details	to verify identity and perform pre-employment screening, to communicate with you and establish HR services and benefits
Address History	to verify identity and perform pre-employment screening, update records and change log
Passport	Certified copy of original document to verify identity and perform pre-employment screening, proof of right to work in UK, travel on work business oversees
Visa	Certified copy of original document to verify identity and perform pre-employment screening, proof of right to work in UK, travel on work business oversees
Driving License	Certified copy of original document to verify identity, proof of address, perform pre-employment screening, drive on work business
Proof of current address	Certified copy of document/s proving address to verify identity and perform pre-employment screening. This may be in the form of a recent utility bill, bank statement or valid driving license, etc.
Bank Details	to set up payroll to pay you and if applicable validate current address as part of pre-employment screening
Card details	Certified copy of original document to verify identity
National insurance number	to identify you and for payroll purposes

DBS check	part of pre-employment screening and requirement for our Information Security Management System under ISO27001 and requirement of customer contractual obligation. Certificate numbers, date of check and outcome of check stored. Certificates not kept on file and if received, passed back to data subject as their property.
Credit reference check	only obtained with explicit consent of data subject for a specified purpose. Required to be able to provide services to specific customers where regulation, such as FSA, require workers to be credit checked to prevent fraud and possible financial crime, etc. Certified copy retained on HR file.
Security clearance	details of any security clearance that has been obtained for the individual and reasonably required to be able to deliver services where there is a contractual requirement for a worker to be security cleared.
CV	received as part of the employment application process
References	received as part of the employment application process and employment screening
Certificates	where certain qualifications are required for a role or to support training that has been taken, certificates may be held on file as proof of attendance and where applicable holding the relevant qualification.
Next of kin PII	held by HR in case of an emergency and we need to get hold of next of kin. Name and contact details held and may be passed to relevant third party for the purpose of death in service insurance, pension provision or other staff benefits, where beneficiary information is required.
Beneficiary PII	held by HR in case of an emergency and we need to get hold of a beneficiary. Name and contact details held and may be passed to relevant third party for the purpose of death in service insurance, pension provision or other staff benefits, where beneficiary information is required.
Partner PII	may be held by HR and passed to relevant third parties for the provision of certain staff benefits that can be extended to family members, such as medial insurance and gifts. Name, contact details, relationship with employee and date of birth may be processed.
Dependents PII	may be held by HR and passed to relevant third parties for the provision of certain staff benefits that can be extended to family members, such as medial insurance and gifts. Name, contact details, relationship with employee and date of birth may be processed. Where PII relates to persons below 16 years of age and is freely given by the employee, it is assumed that their consent is given or authorized by the holder of parental responsivity over the person.
Special Category – sickness	during your employment you may be unwell and need to take sick leave which will be tracked by the Company in its HR tools and associated records. Upon return to work you will be required to complete a return to work form, or similar, to ensure you are fit for work and to record the sickness absence. If you are off sick for a certain amount of consecutive time, a sick note/fit for work form may be required from your GP and a copy of this saved on your HR file for reference. The company tracks and processes certain leave details, such as frequency and duration, and applies statistical formulas to obtain Bradford Factor scoring to measure and report on absenteeism across the Company. The Company does not solely make any decisions based on such profiling or automated processing of PII, except where necessary for entering into, or performance of, a contract between the data subject and data controller
Special Category – Medical history	in some circumstances there may be a requirement to obtain medical records from you and where this is required for specific purpose, explicit consent will be obtained from you.
IP Address	The IP address of a device used to access or approve services, such as signing documents on behalf of the company, may be logged for information security and compliance purposes

Cookies	Cookies may track access to certain Company websites. Please refer to the Company's Cookie Policy for more details

Work specific:

Employee/Payroll ID	Unique number generated by the Company to identify you for payroll purposes
Login Names	used to authenticate and track access to Company systems, applications and services for information security purposes and provide individual accountability to such access. Passwords handled in accordance with the Company's information security management system under ISO27001. Required to uniquely identify an individual
Role	used to specify the role within the company that you perform and to apply relevant responsibilities, benefits and controls, as well as to communicate to individuals at a role level
Department	used to specify the department you work in and to apply relevant responsibilities, benefits and controls, as well as to communicate to individuals at a departmental level
Work contact details	Work address, work email, work telephone number, work mobile number are processed in day to day in communications to and from you and may be used, together with your name in documentation produced during the relationship between us and you.

We will only ask for sensitive information (date of birth and health information) which is absolutely necessary for a specific reason or we are required to monitor equality, or comply with the Modern Slavery Act, or similar legislation, etc. We do not currently process the following special categories of PII (as defined under GDPR):

- Racial or Ethnic Origin (unless required to track equality in the workplace)
- Political Opinions
- Religious or philosophical beliefs
- Trade Union Membership
- Genetic Data
- Biometric data
- Data concerning sex life or sexual orientation

Appendix 1 to this document below, provides further details on what PII is potentially collected and processed whilst working for the Company and Appendix 2, demonstrates the associated data flows.

How we use the information about you?

We process this data for the purposes described in this Policy, namely:

- To be able to contract with you to provide work/employment and pay you for your services and provide a Company pension.
- To be able to provide benefits and services to you.
- For Information Security requirements in line with our Information Security Management System and that of our customers, to whom, we provide services.
- As a Company contact or reference named in a Document produced in the course of a relationship between yourself with bluesource;
- Improve security by protecting against fraud and abuse;
- Identify an individual requesting access to information or services;

- Resolve disputes, troubleshoot problems and inforce our policies;
- Communicate with you;
- Provide you with information updates that you have signed up to receive;
- Customise your experience;
- Conduct analytics and measurement to understand how our services are used;
- Improve the quality of our services and develop new ones;
- Advise you of products and services which may be of interest based upon searches and current subscribed services, or previous consented interest;
- When you contact bluesource, we may keep a record of your communication to help solve any issues you might be facing, such as on our call logging software. We may also use your email address to inform you about our services, such as letting you know about upcoming events, changes or improvements; and
- To gather feedback about our products and services.
- Sickness records may be processed statistically by HR to access sickness levels and trends.
- Compliance with the Company's legal and legislative requirements

Our servers and MS Azure instances are located within the UK. If you choose to provide us with personal information, you are consenting to the transfer and storage of that information in such locations and elsewhere we have facilities. We will endeavor to use facilities and services based in the UK and EU, wherever possible.

We will ask for your consent before using information for a purpose other than those set out in this Privacy Policy.

We retain your PII as long as it is reasonably necessary and relevant for our operations or to comply with relevant laws. In addition, we may need to retain PII after termination of our relationship with you to comply with laws or legislation, prevent fraud, collect any fees owed, resolve disputes, troubleshoot problems, assist with any investigation, enforce our policies and agreements and take other actions permitted or required by applicable laws.

Transparency

People have different privacy concerns and our goal is to be clear about what information we collect and why we need it, so that you can make a meaningful informed choice on providing it to us.

We will not request, capture or store PII which is considered unnecessary for the consented purpose.

Your rights under GDPR

Under GDPR you have certain rights to the PII held about you, namely:

- **The right to information** as to whether your PII is being processed by the Company, as a controller, or a third-party processor, to access a copy of that data, to find out the purposes of processing your data, how long it will be stored by the controller, and to be provided with supplemental information about the processing. This Privacy Policy is intended to provide key information to you about HR related data processing.
- **The right of subject access** to a copy of your PII, the purpose of processing your data, the categories of the information being processed and the third parties or categories of third parties that will receive the data..
- **The right to rectification** of any inaccuracies in your PII that is held.
- **The right to erasure (the "right to be forgotten")** of PII that:
    - Is no longer necessary in the relation to the purposes of which they were collected or otherwise processed;
    - Your consent for processing has been withdrawn and there is no other legal grounds for processing;
    - You object to processing and there are no overriding legitimate grounds for the processing;
    - Has been unlawfully processed without your consent or other legal basis;
    - Has to be erased for compliance with an EU legal obligation.

- **The right to restrict processing** of stored personal data until your consent to lift the restriction is given, or is necessary for the establishment of legal claims, to protect the right of another person, or in the interests of the wider public.
- **The obligation to notify relevant third parties** of any rectification, erasure or processing restriction on your personal information.
- **The right to data portability.** You have the right to receive the personal data concerning your "access request" in a structured, commonly used format which can, where necessary, be transferred to another controller.
- **The right to object** to your personal information being processed.
- **The right to not be evaluated solely on the basis of automated processing**

For further details on your rights, please refer to General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

Accessing and updating your personal information

If the information we hold about you is wrong, needs to be updated or deleted, please email the details to privacy@bluesource.co.uk so we can update the necessary information - unless we have to keep that information for legitimate business, compliance or legal purposes. When updating your personal information, we may ask you to verify your identity before we can act on your request.

We may reject requests that are unreasonably repetitive, require disproportionate technical effort (for example, developing a new system or fundamentally changing an existing practice), risk the privacy of others, or would be extremely impractical (for instance, requests concerning information residing on backup systems or references to an individual within historical support tickets, historical accounting information or within individual historical Documents, that are still required for retention for legitimate business reasons).

Where we can provide information access and correction, we will do so free of charge, except where it would require a disproportionate effort. We aim to maintain our services in a manner that protects information from accidental or malicious destruction, which is further described below under Information Security.

Information that we share

bluesource does not rent, sell, or share PII with other people or nonaffiliated companies except to provide products or services you've requested, when we have your permission (explicit, freely given individual consent), or under the following circumstances:

- **For Contractual consent** (rather than explicit, freely given individual consent) necessary to be able to provide the service. For example, to be able to provide a contract to you for employment or provide certain staff benefits, such as a Company Pension. Without this consent at a contractual level, we would be unable to reasonably provide services and offer employment as "explicit and freely given" consent is inappropriate as we have a level of authority over you, which could negate it being "freely" given.

- **For external processing:**
    - Where we need to provide certain information to trusted partners and subcontractors, working on behalf of, or with bluesource, under contractual and confidentiality agreements, to deliver part or all of the service. Such information shall be the minimum required for that purpose. For example, if we have to escalate a support issue to Microsoft, for their assistance in resolving it, we may need to provide certain PII related to yourself, such as contact details. These companies do not have any independent right to share this information;
    - To assist bluesource communicate with you about offers from bluesource and our partners, where any necessary consents have been freely given. These companies do not have any independent right to share this information.

- **For Legal reasons**

  We will share PII with companies, organisations or individuals outside of bluesource if we believe in good faith that access, use, preservation or disclosure of the information is reasonably necessary to:

- Respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims;
- Meet any applicable law, regulation, legal process or enforceable government request;
- Enforce applicable terms of service and to investigate potential violations;
- Detect, prevent and address fraud, security and technical issues;
- Protect against harm to the rights, property or safety of bluesource, our workers, our customers, our suppliers, or the public, as required or permitted by law;
- Meet our obligations under DPA and GDPR to report breaches to the data controller and where we are acting as the controller, to the relevant supervisory authority (which is the Information Commissioners Office for the UK).

We limit access to PII to those employees, partners and subcontractors we believe reasonably need to come into contact with that information to provide services to you, or your company, in order to do their jobs. We have a "who needs to know, minimum rights" policy to such access.

If we are involved in a merger, acquisition or asset sale, we will continue to ensure the confidentiality of any personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

Whenever we share personal data, we take all reasonable steps to ensure that it is treated securely and in accordance with this privacy policy.

PII for HR purposes may be shared, obtained or processed by external parties under contractual arrangements with bluesource to provide specific services to bluesource and their employees. These included and are not limited to:

Category of third party	Third Party	Purpose
Recruitment agencies	various	Applications and feedback on employment with relevant recruiter
Pre-employment screening	Due Diligence Checking	Criminal record check from Disclosure Scotland which is an employment requirement for being able to offer employment
HR consultancy	SME ADVISOR	External HR consultancy as an extension to in-house HR
HR consultancy	HR First	External HR consultancy as an extension to in-house HR
Financial	Harwood Hutton	Payroll and company auditors
Financial	HMRC	Taxes, etc.
HR related software as a service	E-days	Cloud based processing of employee leave, including holiday, sick leave and leave profiling
HR related software as a service	Concur	Employee expenses
Employee benefits	Tenet Employee Solutions	Pension intermediary and other employee benefit provider
Employee benefits	MetLife	Death in Service insurance
Employee benefits	AXA PPP	Private Medical Insurance
Employee benefits	AVIVA	Company pension provision

Information Security

We work hard to protect bluesource and the information we are entrusted to look after from unauthorised access, unauthorized alteration, unauthorized disclosure or unauthorised destruction. We ensure your PII's integrity, availability and confidentiality are suitably protected.

We have implemented an information security management system ("ISMS") which is certified annually to the ISO27001 standard.

Unfortunately, no data transmission over the Internet or any other network can be guaranteed as 100% secure. As a result, while we strive to protect your personal data, we cannot ensure and do not warrant the security of any information you transmit to us, and this information is transmitted at your own risk.

If you have been given log-in details to provide you with access to certain services (for example software as a service type services), you are responsible for keeping those details confidential. This is also a requirement of the Company's Information Security policies and failure to abide by these is likely to result in a disciplinary matter.

When this Privacy Policy applies

This Policy applies to all the services offered by bluesource Information Limited and its affiliates, including bluesource Inc., except for services that have separate privacy policies that do not incorporate this Policy.

It does not apply to the practices of companies that bluesource does not own or control, or to people that bluesource does not employ or manage.

Where partners or subcontractors are engaged to perform parts or all of a service, as the data controller, bluesource is responsible for ensuring that the same data protection obligations, shall be imposed on that other processor by way of a contract, or other legal act, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing meet the requirements of the DPA/GDPR as appropriate.

Our Policy does not cover the information practices of other companies and organisations that advertise our services.

Compliance and cooperation with regulatory authorities

We regularly review our compliance with our Privacy Policy as part of our ISMS and with the requirements of the DPA and GDPR.

Should I have a complaint, how do I report it?

To make it easy for our customers to raise a complaint, in the unlikely event they need to, we have a single email address that can be used complaints@bluesource.co.uk. We will determine whether the complaint is service, compliance or HR related and engage the necessary individuals to deal with the complaint for you.

Changes

bluesource may update this Policy. We will notify you about significant changes in the way we treat PII by sending a notice to the primary contact's email address specified in your company's account with us, or by placing a prominent notice on our website site.

Questions and Suggestions

If you have questions or suggestions, please complete a feedback form or you can contact us at: privacy@bluesource.co.uk.

APPENDIX 1 – PII ACCESS

TYPE OF PII	BLUESOURCE ACCESS								EMAILS & DOCUMENTS				AUTHENTICATION			WEB		APPLICATIONS								
	HR	Finance	Line Manager	Admins	Operations	SMC	Sales	Consulting	EMAILS	HR DOCS	COMPANY DOCS	OFFICE365	AD	CISCO FIREWALL/VPN	GUEST WIFI	INTRANET	WEBSITE	CONNECTWISE Manage	CONNECTWISE Sell	N-Able	FILEMAKER HR	FILEMAKER Orders	E-days	Office365 Apps	SAGE	ConCur
WORKER - employee/contractor																										
Name																										
Date of Birth																										
Personal Address - current																										
Address History																										
Private phone numbers																										
Private email address																										
Visa / Right to work in UK																										
Passport																										
Driving Licence																										
Proof of address																										
Bank Details																										
Card Details for ID verification																										
National Insurance Number																										
DBS Certificate / Number																										
Credit Reference check																										
Qualification certs																										
CV																										
References																										
SPEC. CAT. Health - sick leave																										
SPEC. CAT. Health - other																										
SPEC. CAT. - Other																										
Next of Kin PII																										
Partner's PII																										
Dependant's PII																										
IP Address														?	?		?									
COOKIE																										
Payroll ID																										
AD Login Name																		link to email	link to email							
Software Login																										
Role / Job title																										
Department																										
Work Address																										
Work number																										
Work mobile																										
Work email address																										
NON WORKER - customer, contact, supplier,partner, etc.																										
Name																										
Company																										
Role / Job title																										
Department																										
Work Address																										
Work number																										
Work mobile																										
Work email address																										
Software Login																										
IP Address														?	?		?	?	?							
COOKIE																		?	?							

KEY
- Access to this information
- Needs to know, minimum rights for specific reasons
- Not processed

APPENDIX 2 – HR data mapping