Bluesource

Data Processing Policy

Last updated 1st May 2026

1 Introduction

Bluesource Information Limited ("**Bluesource**", "**we**", "**us**" or "**our**") is committed to protecting Personal Data and respecting the privacy and rights of individuals in accordance with applicable data protection legislation, including the UK General Data Protection Regulation ("**UK GDPR**"), the EU General Data Protection Regulation ("**EU GDPR**"), and the Data Protection Act 2018 (together, "**Data Protection Law**").

This Data Processing Policy ("**Policy**") sets out the terms on which Bluesource processes Personal Data on behalf of its customers ("**Customer**") in connection with the provision of goods and services under an applicable agreement, order, statement of work or service schedule (the "**Agreement**"). For the purposes of Data Protection Law, the Customer acts as the **Controller** of Customer Personal Data, and Bluesource acts as a **Processor**, except where Bluesource independently determines the purposes and means of processing (such as for limited Support Data), in which case Bluesource acts as a **Controller**.

This Policy is incorporated into the Agreement and constitutes the data processing agreement ("**DPA**") between the parties for the purposes of Article 28 of the UK GDPR and EU GDPR. It describes the subject-matter, duration, nature and purposes of the processing, the types of Personal Data and categories of Data Subjects, the applicable technical and organisational measures, and the conditions governing the engagement of Sub-processors, as further detailed in the Schedules.

Bluesource may update this Policy from time to time to reflect changes in Data Protection Law, regulatory guidance, or processing activities. The current version will always be made available at https://www.bluesource.co.uk/privacy-and-governance. Where required by law, material changes will be notified to the Customer.

Any questions regarding this Policy or Bluesource's data protection practices should be directed to mailto:privacy@bluesource.co.uk or to the contact details set out in **Section 4.7** (Notifications) of this Policy.

2 Definitions

For this Policy, the following definitions shall apply, in addition to those in the Master Terms and Conditions:

"Agreement"	an agreement, usually in the form of an order, Work Order, accepted quote, means an agreement entered into between the Customer and Bluesource governing the provision of goods and/or services, including any order, Work Order, statement of work, service schedule, accepted quotation, or other document incorporated by reference.
"Controller"	the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data, as defined by Data Protection Law.
"Customer"	Bluesource's customer interested in or obtaining goods and/or services from Bluesource or their supply chain.
"Customer Personal Data"	Personal Data processed by Bluesource on behalf of the Customer in the course of providing the Services, for which the Customer acts as Controller.

"Data Breach"	breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed within the meaning of Data Protection Law.
"Data Subject"	an identified or identifiable natural person as defined by Data Protection Law.
"Data Protection Law"	all applicable data protection and privacy legislation, regulations and guidance, including the UK GDPR, the EU GDPR (where applicable), the Data Protection Act 2018, and the Privacy and Electronic Communications (EC Directive) Regulations 2003, in each case as amended, updated or replaced from time to time.
"Designated Contact"	an employee of the Customer nominated as a contact point for Bluesource.
"DPA"	this data processing agreement formed by this Policy as incorporated into the Agreement, for the purposes of Article 28 of the UK GDPR and EU GDPR.
"DPA2018"	the Data Protection Act 2018.
"EU GDPR"	Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data.
"EU Standard Contractual Clauses"	the standard contractual clauses, published by the European Commission, https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en or any subsequent final version thereof which shall automatically apply. To avoid doubt Modules 2 and 3 shall apply, as set out in **Section 6** (International Processing) below.
"General Terms & Conditions"	unless otherwise agreed with the Customer, Bluesource's standard General Terms and Conditions applicable to the Agreement. (a copy of which can be found at https://www.Bluesource.co.uk/privacy-and-governance).
"International Data Transfer Agreement" or "IDTA"	the international data transfer agreement issued by the Information Commissioner under section 119A of the Data Protection Act 2018, as amended or replaced from time to time.
"Party"	a party to this Agreement and "Parties" shall be construed accordingly.
"Personal Data" or **"PII"**	any information relating to an identified or identifiable natural person, as defined in Data Protection Law.
"Privacy Policy"	Bluesource's privacy policy published at: https://www.Bluesource.co.uk/privacy-and-governance/.
"Processing"	any operation or set of operations performed on Personal Data, whether or not by automated means, as defined in Data Protection Law.
"Processing Instructions"	the documented instructions issued by the Customer to Bluesource regarding the Processing of Customer Personal Data under the Agreement.
"Processor"	a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Controller, be it directly as processor of a Controller or indirectly as Sub-processor of a Processor which processes personal data on behalf of the Controller.
"Restricted Transfer"	a transfer of Personal Data to a Third Country or international organisation which, under the UK GDPR and/or EU GDPR, requires appropriate safeguards under Chapter V of the applicable Data Protection Law.

"Schedule"	the numbered Annex with respect to the EU Standard Contractual Clauses.
"Services"	the services to be provided by Bluesource to the Customer as described in a Service Schedule and/or Work Order, and subject to the terms this Policy and the General Terms and Conditions.
"Service Schedule"	the specific schedule relevant to the Services requested by the Customer. Service schedules for our standard services are available at: (available at https://www.Bluesource.co.uk/service-schedules/.
"SCC Relevant Transfer"	a transfer (or an onward transfer) to a Third Country of Personal Data that is either subject to GDPR or to applicable Data Protection Law and where any required adequacy means under GDPR, or applicable Data Protection Law can be met by entering into the EU Standard Contractual Clauses.
"Sub-processor Change Notification Period"	the period specified in this Policy or the Agreement during which the Customer may object to the appointment or replacement of a Sub-processor.
"Sub-processor" or **"sub-processor"**	Bluesource's affiliates, partners and third parties engaged by Bluesource in connection with the Services and which process Personal Data in accordance with this Data Processing Policy.
"Supervisory Authority"	an independent public authority established by a Member State or the United Kingdom pursuant to Data Protection Law, including the Information Commissioner's Office ("**ICO**")
"Support Data"	all data, including all text, sound, video, image files, or software, that are provided to Bluesource by or on behalf of Customer under an Agreement or produced during the relationship between the Parties, such as and not limited to support tickets, project documentation, statements of works, NDAs, contracts, purchase orders, invoices, and emails.
"Technical and Organisational Measures"	the technical and organizational measures implemented in accordance with Article 32 of the UK GDPR and EU GDPR, for the relevant Service, such as those detailed in **Clauses 4.5.5** (Obligation of Security of Processing) and **Section 5** (Security of Processing), or as detailed in the Agreement (such as in the applicable Service Schedule) and Bluesource's information security management system ("ISMS"), which is certified to ISO27001 for Information Security.
"Third Country"	any country, organization or territory not acknowledged by the European Union under Article 45 of GDPR as a safe country with an adequate level of data protection.
"UK Addendum"	the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner under section 119A(1) of the Data Protection Act 2018, as amended, updated or replaced from time to time, which forms part of the UK GDPR framework for international transfers of Personal Data and modifies the EU Standard Contractual Clauses for use in respect of transfers subject to the UK GDPR.
"UK GDPR"	the General Data Protection Regulation (EU) 2016/679 as retained in UK law pursuant to section 3 of the European Union (Withdrawal) Act 2018.
"Work Order"	the document detailing an order for good and/or services agreed in writing by the Parties, including but not limited to: the Customer accepting a Proposal; issuing a purchase order to Bluesource; placing an order via an order form, email, or other means; or receiving a document labelled 'work order' from Bluesource.
"Worker"	Bluesource employee, agent, authorised contractor, or sub-contractor, engaged in provisioning and delivering part or all a Service.

3 Privacy Notice and Transparency

3.1 Where Bluesource processes Personal Data as a Processor on behalf of a Customer, responsibility for providing privacy information to Data Subjects rests with the Customer as Controller. In such circumstances, Bluesource processes Personal Data solely in accordance with the Customer's documented instructions and this Policy.

3.2 Where Bluesource processes Personal Data as a Controller (for example, in relation to Support Data, business contacts, suppliers, marketing activities, or the administration of customer relationships), Bluesource provides transparency information to affected individuals through its Privacy Policy, which is published and kept up to date at: https://www.bluesource.co.uk/privacy-and-governance.

3.3 By way of summary, when acting as a Controller, Bluesource:

- processes Personal Data for purposes including the provision and administration of services, security and fraud prevention, communications, and compliance with legal obligations;
- only processes Personal Data where a lawful basis applies (such as contractual necessity, legal obligation, legitimate interests, or consent where required);
- implements appropriate technical and organisational measures, including through an ISO/IEC 27001-certified Information Security Management System, to protect Personal Data;
- limits access to Personal Data on a need-to-know and least-privilege basis; and
- respects the rights of individuals under applicable Data Protection Law, including rights of access, rectification, erasure, restriction, objection, and complaint to the Information Commissioner's Office.

3.4 Full details of how Bluesource collects, uses, shares, retains, and protects Personal Data when acting as a Controller, as well as how individuals may exercise their rights or raise complaints, are set out in the Privacy Policy, which shall prevail in the event of any inconsistency.

4 Personal Data and Data Processing

This section describes the Processing of Customer Personal Data by Bluesource as a Processor for the purposes of Article 28(3) of the UK GDPR and the EU GDPR. Where appropriate, terms used in this section shall have the meanings ascribed to them by Data Protection Law.

4.1 *Grounds and Legal basis for processing*

4.1.1 Bluesource provides a range of information technology services to its customers, including software and hardware procurement, consultancy, support services, managed services, cloud-based hosting (IaaS), and software-as-a-service (SaaS) solutions (the "Services"). Under an applicable Agreement, Bluesource processes Customer Personal Data solely to the extent necessary to provide the Services and to administer the contractual relationship between the Parties.

4.1.2 In connection with the performance of the Services, Bluesource processes a limited amount of Customer Personal Data strictly as a Processor (or sub-processor, as applicable) on behalf of the Customer, who acts as the Controller of such data. Bluesource acts as Controller only in relation to Support Data, as described in this Policy.

4.1.3 The Customer remains solely responsible for identifying and documenting the lawful basis for the Processing of Customer Personal Data under Data Protection Law. Bluesource does not determine the lawful basis for such Processing and processes Customer Personal Data only in accordance with the Customer's documented instructions and this Policy.

4.1.4 Where the Processing carried out by Bluesource on behalf of the Customer differs from or supplements the Processing described in this Policy, the relevant details of such Processing

shall be set out in the applicable Service Schedule or Work Order forming part of the Agreement.

4.2 ***Nature and location of processing***

This section describes the nature and location of Processing of Customer Personal Data by Bluesource as Processor for the purposes of Article 28(3)(a) and (c) of the UK GDPR and EU GDPR.
Where such Processing involves international transfers, the applicable safeguards under Chapter V of the UK GDPR and EU GDPR (including the EU Standard Contractual Clauses, the UK Addendum, and related transfer assessments) are set out in **Section 6** (International Processing).

4.2.1 Customer Personal Data provided by the Customer may be keyed or copied to Bluesource's systems and processed as Support Data solely for the purposes of providing and supporting the Services, and is stored, accessed, and reviewed in accordance with the Agreement and this Policy.

4.2.2 As a global organisation headquartered in the United Kingdom, Customer Personal Data and Support Data may be accessed by authorised Workers located in the United Kingdom and, where necessary to provide Services on a 24/7/365 basis, in other jurisdictions including Bulgaria, Norway, the Philippines, and the United States. Access is limited to authorised personnel on a need-to-know and least-privilege basis.

4.2.3 Where such access occurs, Processing is carried out on Bluesource's systems hosted within the United Kingdom and/or the European Economic Area ("EEA")

4.2.4 Where access to Customer Personal Data involves Workers located in a Third Country and employed by a Sub-processor, such access constitutes a restricted transfer under Data Protection Law. In such cases, Bluesource implements appropriate safeguards in accordance with Chapter V of the UK GDPR and EU GDPR, as further detailed in **Section 6** (International Processing), including the EU Standard Contractual Clauses (Modules 2 or 3, as applicable) and the UK Addendum where UK GDPR applies.

4.2.5 Where the UK GDPR applies, Bluesource has conducted, where applicable, a Transfer Risk Assessment ("TRA") to assess the risks associated with the international transfer and the effectiveness of the contractual and technical safeguards implemented

4.2.6 Where Customer Personal Data relates to individuals protected by the EU GDPR, Bluesource has also conducted, where required, a documented Transfer Impact Assessment ("TIA") to assess whether the laws and practices of the destination jurisdiction ensure a level of protection essentially equivalent to that guaranteed within the European Union. Where risks are identified, Bluesource implements appropriate supplementary technical, organisational, or contractual measures, or does not proceed with the transfer

4.2.7 In accordance with this Policy and Privacy Policy, Bluesource may outsource limited marketing activities and transfer only minimal Personal Data relating to business contacts to carefully selected Sub-processors. Such Processing is limited strictly to marketing Bluesource's goods and services and is not permitted for any other purpose.

4.2.8 Support Data, where applicable, is used for the following purposes:

- maintaining and administering the contractual relationship, including raising quotes, contracts, invoices, credits, notices, and producing documentation;
- communicating with the Customer via Designated Contacts;
- advising on relevant services and service improvements; and
- supporting security and fraud prevention activities.

4.2.9 Support Data may also be used to provide the Services, including:

- managing and resolving support tickets (incidents, problems, changes, and informational requests);
- delivering and managing projects;
- procuring and licensing goods and/or services on behalf of the Customer;

- escalating issues to relevant third parties (such as software vendors);
- advising on service performance, enhancements, and changes; and
- administering access controls where applicable

4.2.10 Limited Support Data may be processed within Bluesource's internal retrieval-augmented generation ("**RAG**") AI tool, Moses, solely to assist with resolving technical issues, trend analysis, problem management, proactive support, and productivity improvements. Such data is not used to train third-party models and remains subject to the same access, security, and retention controls applied to other Support Data under Bluesource's ISO/IEC 27001-certified Information Security Management System.

4.2.11 Certain Services, including email archiving, backup, data migrations, and email protection services, by their very nature, process Customer's data ("**Customer Data**"), provided by the Customer, which may contain any category of Personal Data relating to any category of Data Subject. Bluesource does not determine the content of such data and processes it strictly in accordance with the Customer's instructions and the applicable Service Schedule or Work Order.

4.3 *Categories of Personal Data*

In accordance with Article 28(3)(c) of the UK GDPR and the EU GDPR, Bluesource processes Customer Personal Data only to the extent necessary to provide the Services and in accordance with the Customer's documented instructions.

4.3.1 Subject to the nature and scope of the Services, Customer Personal Data typically processed by Bluesource may include:

- names;
- job titles, roles and professional responsibilities;
- departments;
- business addresses;
- business email addresses;
- business telephone numbers;
- correspondence and communications between the Parties, including emails, support tickets, project documentation, and service-related communications, where such correspondence contains Personal Data; and
- authentication and access-control data required to enable secure access to Services, systems, or portals, such as usernames, user identifiers, and access or authentication logs.
- business-related scheduling, availability, and meeting information;
- authorisation, approval, and change-tracking records associated with service delivery; and
- service-related activity and audit metadata linked to an identified individual, such as timestamps and action records.

4.3.2 Certain Services, and access to Bluesource systems, websites, or portals, may also involve the processing of limited technical or usage data necessary for authentication, security, and service operation, such as usernames, unique identifiers, IP addresses, and system logs. Further information on such processing, where Bluesource acts as Controller, is set out in the Privacy Policy.

4.3.3 Bluesource does not intentionally request or process Special Category Data (as defined in Article 9 of the UK GDPR and EU GDPR) unless such processing is expressly required for the provision of a specific Service and the Customer has provided documented instructions as Controller. Where such circumstances arise, the applicable Service Schedule or Work Order shall specify the nature of the data and any additional safeguards required.

4.3.4 Certain Services, including but not limited to email archiving, backup, data migration, and email protection services, by their nature process Customer Data provided by the Customer which may contain any category of Personal Data relating to any category of Data Subject. Bluesource does not determine the content of such data and processes it strictly as Processor, in accordance with the Customer's instructions and the applicable Agreement.

4.4 *Categories of Data Subjects*

4.4.1 In accordance with Article 28(3)(c) of the UK GDPR and the EU GDPR, Bluesource processes Customer Personal Data relating to the following categories of Data Subjects, as instructed by the Customer and to the extent necessary to provide the Services:

- Customer employees, workers, contractors, consultants, and other personnel;
- Customer designated contacts and authorised representatives;
- End customers or users of the Customer, where relevant to the Services; and
- Workers involved in the provision and delivery of the Services.

4.4.2 Certain Services, including but not limited to email archiving, backup, data migration, and email protection services, by their nature process Customer Data provided by the Customer which may contain Personal Data relating to additional categories of Data Subjects beyond those listed above. In such cases, Bluesource does not determine the categories of Data Subjects and processes the data solely as Processor, in accordance with the Customer's instructions and the applicable Agreement.

4.5 *Data Processing Obligations*

Where Bluesource processes Customer Personal Data as a Processor on behalf of the Customer, Bluesource shall comply with the following obligations in accordance with Article 28(3) of the UK GDPR and the EU GDPR:

4.5.1 Processing on instructions

Bluesource shall process Customer Personal Data only on documented instructions from the Customer, including with regard to any transfers of Personal Data to a Third Country or an international organisation, unless required to do so by applicable law, in which case Bluesource shall inform the Customer of that legal requirement unless prohibited by law.

4.5.2 Notification of unlawful or unsafe instructions

Prior to carrying out any instruction from the Customer, Bluesource shall notify the Customer if, in Bluesource's reasonable opinion, such instruction is likely to result in a Personal Data Breach or otherwise infringe Data Protection Law. In doing so, Bluesource does not provide legal advice and remains entitled to rely on the Customer, as Controller, to determine the lawfulness of the Processing and to provide documented instructions accordingly.

4.5.3 Records of Processing Activities

Bluesource shall maintain a record of its processing activities carried out on behalf of the Customer in accordance with Article 30(2) of the UK GDPR and the EU GDPR. Each party is responsible for its own compliance with applicable record-keeping and documentation requirements under Data Protection law.

Where required, each party shall reasonably assist the other by providing relevant information necessary to enable compliance with such obligations, in a manner reasonably requested.

4.5.4 Confidentiality

Bluesource shall ensure that persons authorised to process Customer Personal Data are subject to appropriate obligations of confidentiality and receive suitable training regarding their data protection responsibilities.

4.5.5 Security of Processing

Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing, as well as the risks to the rights and freedoms of natural persons, Bluesource shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including measures addressing:

- access control on a need-to-know and least-privilege basis;
- pseudonymisation and encryption of Personal Data where appropriate;
- the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- the ability to restore availability and access to Personal Data in a timely manner following an incident; and
- regular testing, assessment, and evaluation of the effectiveness of security measures.

Such measures are implemented through Bluesource's ISO/IEC 27001-certified Information Security Management System and applicable service-specific controls, together with compliance of its Cyber Essentials and Cyber Essentials Plus certifications.

4.5.6 Sub-processing

Bluesource may engage Sub-processors to process Customer Personal Data in connection with the provision of the Services, subject to the requirements of Article 28(2) and Article 28(4) of the UK GDPR and the EU GDPR.

Details of Sub-processors that are core to the delivery of specific Services are disclosed within the Agreement, including in one or more of the following: this Policy and in particular **Section 7** (Authorised Sub-processors); an applicable Service Schedule; or an applicable Work Order. Such disclosures are intended to provide transparency regarding the categories of Sub-processors engaged for particular Services.

Bluesource may update or replace Sub-processors where reasonably necessary to ensure continuity of Services, maintain operational resilience, address security or compliance requirements, or ensure consistent service delivery across its customer base. Bluesource shall not be required to constrain its Sub-processor arrangements on a per-customer basis where such constraint would adversely affect service delivery or operational efficiency.

Bluesource shall ensure that all Sub-processors are subject to written data protection obligations no less protective than those set out in this Policy and shall remain fully liable to the Customer for the performance of its Sub-processors in accordance with Article 28(4) of the UK GDPR and the EU GDPR.

Where a change in Sub-processors results in a material increase in risk to Customer Personal Data, Bluesource shall provide advance notice in accordance with the applicable Agreement to allow the Customer a reasonable opportunity to raise an objection on data protection grounds.

Unless otherwise specified in the Agreement or applicable Service Schedule, the Customer shall have a period of thirty (30) days from receipt of notice of a proposed Sub-processor appointment or replacement (the "**Sub-processor Change Notification Period**") to raise a reasoned objection on data protection grounds

4.5.7 Worker Obligations

Bluesource shall ensure that Workers authorised to process Customer Personal Data are bound by obligations of confidentiality, are made aware of Bluesource's obligations as Processor, and receive appropriate training to ensure compliance with Data Protection Law.

Bluesource shall remain liable to the Customer for any failure of its Workers to comply with such obligations.

4.5.8 Assistance to the Customer

Taking into account the nature of the Processing and the information available to Bluesource, Bluesource shall provide reasonable assistance to the Customer, insofar as this is relevant and technically feasible, in fulfilling the Customer's obligations under Data Protection Law, including with regard to:

- completing data protection impact assessments and, where applicable, prior consultations with relevant supervisory authorities, including the ICO;
- making available reasonable information necessary to demonstrate Bluesource's compliance with this Policy and Data Protection Law; and
- responding to requests from Data Subjects exercising their rights under Data Protection Law, to the extent Customer cannot fulfil such requests independently using the tools provided as part of the relevant Service and where Bluesource is technically able to assist.

Except where required by Data Protection Law or expressly included within the Services, such assistance may be subject to reasonable cost recovery as agreed between the Parties.

4.5.9 Audits and inspections

Bluesource shall allow for, and contribute to, audits or inspections conducted by the Customer or an auditor mandated by the Customer for the purpose of demonstrating compliance with this Policy, subject to reasonable confidentiality, scope, timing, and security requirement.

Except where required by Data Protection Law or expressly included within the Services, such assistance may be subject to reasonable cost recovery as agreed between the Parties.

4.5.10 Personal Data Breaches

Bluesource shall notify the Customer without undue delay, and in any event no later than 24 hours after confirmation, upon becoming aware of a Personal Data Breach affecting Customer Personal Data and shall reasonably assist the Customer in meeting any notification or communication obligations under Data Protection Law.

Such notification shall, to the extent information is available at the time, include a description of the nature of the Personal Data Breach, the categories and approximate volume of Personal Data and Data Subjects affected, the likely consequences of the breach, and the measures taken or proposed to address and mitigate its effects. Additional information shall be provided as it becomes available.

4.5.11 Deletion or return of Customer Data

Subject to **Clause 4.5.12** (Retention of Support Data for Legitimate Business Purposes) below, at the choice of the Customer, and subject to applicable legal retention requirements, Bluesource shall delete or return all Customer Personal Data upon termination or expiry of the relevant Services and delete existing copies, unless retention is required by law. Personal Data contained in backups will be securely deleted or overwritten in accordance with defined backup retention cycles.

4.5.12 Retention of Support Data for legitimate business purpose

Notwithstanding any obligation to delete or return Customer Personal Data at the end of the Services, Bluesource may retain limited Support Data where reasonably necessary for legitimate business purposes, including but not limited to ensuring the integrity, security, resilience, and availability of its systems and services, complying with applicable legal or regulatory obligations, exercising or defending legal claims, and meeting accounting, audit, and record-keeping requirements.

Personal Data contained within system backups is not selectively deleted where doing so would compromise backup integrity or system resilience. Such data will be securely deleted or irreversibly overwritten in accordance with defined backup retention cycles once the relevant backup data reaches end of retention.

Where a system restore is required, Bluesource will take reasonable steps to re-apply any valid deletion or restriction requests received after the date of the backup used for restoration, where technically feasible.

Any Support Data retained under this section shall continue to be subject to appropriate technical and organisational measures, access controls, and confidentiality obligations in accordance with this Policy and Bluesource's ISO/IEC 27001-certified Information Security Management System and shall not be used for any purpose incompatible with the original purpose of Processing.

4.5.13 Demonstrating compliance and audits

Bluesource shall make available to the Customer the information reasonably necessary to demonstrate compliance with this Policy and Data Protection Law and shall allow for, and contribute to, audits or inspections conducted by the Customer or an auditor mandated by the Customer, subject to reasonable confidentiality, scope, timing, and security requirements.

4.5.14 Notification

Bluesource shall notify the Customer without undue delay should it:

- receive notice of any investigation or adverse finding by a Data Protection Regulator in relation to its Processing of Personal Data which could pose a risk to Customer Personal Data.
- be under a legal obligation to Process Customer Personal Data, other than under the Customer's instructions (or Controller's, where this is not the Customer), in which case it shall inform the Customer/Controller of the legal obligation, except to the extent the law prohibits it from doing so.
- receive any request from or on behalf of a Data Subject exercising their rights under the Data Protection Law in respect of Customer Personal Data under the exclusive control of Bluesource.
- receive a request from or on behalf of a Data Subject relating to Customer Personal Data, Bluesource shall promptly notify the Customer and shall not respond to such request except on the Customer's documented instructions or where required to do so by applicable law.

4.6 *Duration of processing*

4.6.1 Bluesource shall process Customer Personal Data for the duration of the provision of the relevant Services under the Agreement, unless otherwise instructed in writing by the Customer or required by applicable law.

4.6.2 Subject to **Clause 4.5.11** above, Article 28(3)(g) of the UK GDPR and the EU GDPR, and at the choice of the Customer upon termination or expiry of the relevant Services, Bluesource shall delete or return all Customer Personal Data to the Customer and delete existing copies, unless retention of such data is required by applicable law.

4.6.3 Notwithstanding the foregoing, and as per **Clause 4.5.12** above:

4.6.3.1 Bluesource may retain limited Support Data where reasonably necessary for legitimate business purposes, including ensuring the integrity, security, resilience, and availability of its systems and services, complying with applicable legal or regulatory obligations (including accounting, tax, and audit requirements), exercising or defending legal claims, and maintaining appropriate operational records.

4.6.3.2 Personal Data contained within system backups is not selectively deleted where doing so would compromise backup integrity or system resilience. Such data will be securely deleted or irreversibly overwritten in accordance with defined backup retention cycles once the relevant backup data reaches end of retention.

4.6.3.3 Where a system restore is required, Bluesource will take reasonable steps to re-apply any valid deletion or restriction requests received after the date of the backup used for restoration, where technically feasible

4.6.3.4 Any Support Data retained in accordance with this section shall remain subject to appropriate technical and organisational measures, access controls, and confidentiality obligations under this Policy and Bluesource's ISO/IEC 27001-certified Information Security Management System and shall not be used for any purpose incompatible with the original purpose of Processing.

4.7 *Notifications*

4.7.1 All notifications to Bluesource regarding data protection, information security or privacy should be sent to:

- Nick Jaggers
  Head of Operations and acting DPO
  020 7940 6220
  nick.jaggers@Bluesource.co.uk; and
- Privacy@Bluesource.co.uk

4.7.2 All notifications to Customer regarding data protection, information security and privacy, unless otherwise agreed in writing, shall be addressed to the Designated Contact.

4.7.3 To make it easy 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.

5 Security of Processing

5.1 Bluesource has implemented and will apply appropriate Technical and Organisational Measures in accordance with Article 32 of the UK GDPR and EU GDPR, as per its obligation described in **Clause 4.5.5** (Security of Processing) above, to safeguard confidentiality, integrity, and availability against unauthorised access, alteration, disclosure, or destruction.

5.2 While no system can be guaranteed to be completely secure, Bluesource applies security controls proportionate to the risks identified and regularly reviews these measures to ensure they remain effective.

5.3 We operate an Information Security Management System ("ISMS") that is independently certified and maintained in accordance with recognised security standards, including ISO/IEC 27001, Cyber Essentials, and Cyber Essentials Plus.

5.4 In entering into the Agreement and ordering the relevant goods and/or services, the Customer acknowledges that it has had reasonable opportunity to review the nature of those measures (including where referenced in applicable Service Schedules and this Policy) and considers them appropriate, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the Processing of Customer Personal Data.

5.5 Bluesource applies the Technical and Organisational Measures relevant to a particular service offering consistently across its customer base using that service. Bluesource may update or replace such measures from time to time, without prior notice, provided that any such change does not materially diminish the overall level of security protecting Customer Personal Data.

5.6 Updated descriptions of service-specific Technical and Organisational Measures will be made available through the applicable Service Schedules published on Bluesource's website.

6 International Processing

6.1 References in this Policy to Third Countries and international transfers shall be interpreted in a manner consistent with both EU GDPR adequacy decisions and UK adequacy regulations, as applicable.

6.2 Where applicable for a specified Service, Bluesource may process Customer Personal Data, including by engaging Sub-processors, outside the country in which the Customer or Controller is located, solely in accordance with this Policy, **Clause 4.2** (Nature and location of Processing), applicable Data Protection Law, and the relevant Agreement, Work Order, or Service Schedule

6.3 Where Processing involves access to Customer Personal Data by Workers or Sub-processors located in a Third Country, such access constitutes a restricted transfer under Chapter V of the UK GDPR and/or EU GDPR. In such circumstances, Bluesource shall ensure that appropriate safeguards are implemented prior to the transfer and maintained for the duration of the Processing.

6.4 ***Applicability of EU Standard Contractual Clauses***

The following provisions apply solely in respect of transfers that constitute an SCC Relevant Transfer, as defined in this Policy:

6.4.1 Where Bluesource is not located in a Third Country and acts as a data exporter of Customer Personal Data as Processor, Bluesource has entered into the EU Standard Contractual Clauses with the relevant Sub-processor as the data importer. Module 3 (Processor-to-Processor) of the EU Standard Contractual Clauses shall apply to such transfers.

6.4.2 Where Bluesource is not located in a Third Country and acts as a data exporter of Personal Data for which it is the Controller, including Support Data, Bluesource has entered into the EU Standard Contractual Clauses with the relevant Sub-processor as the data importer. Module 2 (Controller-to-Processor) of the EU Standard Contractual Clauses shall apply to such transfers.

6.4.3 Where applicable, other Controllers or Processors authorised by the Customer to use the Services (including SaaS or IaaS hosted by Bluesource) may enter into the EU Standard Contractual Clauses with Bluesource on the same basis as the Customer. In such cases, the Customer enters into the EU Standard Contractual Clauses on behalf of such Controllers or Processors.

6.5 ***UK GDPR – International Data Transfer Addendum***

6.5.1 In respect of transfers subject to the UK GDPR, the EU Standard Contractual Clauses shall be read together with, and modified by, the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the Information Commissioner pursuant to section 119A of the Data Protection Act 2018 (the "UK Addendum").

6.5.2 For the purposes of the UK Addendum:

- Tables 1 to 3 shall be deemed completed using the relevant information from the EU Standard Contractual Clauses;
- The option "neither party" shall be deemed selected in Table 4; and
- The start date of the UK Addendum shall be the effective date of the applicable Agreement, unless otherwise specified.

6.5.3 As an alternative to the use of the EU Standard Contractual Clauses as modified by the UK Addendum, and where expressly agreed in writing between the parties, transfers of Personal Data subject to the UK GDPR may instead be governed by the International Data Transfer Agreement ("IDTA") issued by the Information Commissioner pursuant to section 119A of the Data Protection Act 2018.

For UK-only restricted transfers governed by the IDTA, the required information shall be completed by reference to the relevant provisions of this Policy, including **Section 4** (Data Processing Obligations) and **Section 5** (Security of Processing) and **Schedules 1–3**, unless otherwise agreed in writing.

Where the IDTA is used, it shall apply in place of, and not in addition to, the EU Standard Contractual Clauses and UK Addendum for the relevant transfer.

6.6 *Transfer Risk and Impact Assessments*

6.6.1 Where required by applicable Data Protection Law and consistent with **Clause 4.2** (Nature and Location of Processing) of this Policy:

- Bluesource has conducted a Transfer Risk Assessment ("TRA") for transfers subject to the UK GDPR; and
- Where Customer Personal Data relates to individuals protected by the EU GDPR, Bluesource has conducted a Transfer Impact Assessment ("TIA") to assess whether the laws and practices of the destination jurisdiction ensure a level of protection essentially equivalent to that guaranteed within the European Union.

6.6.2 Where risks are identified, Bluesource implements appropriate supplementary technical, organisational, or contractual measures, or does not proceed with the transfer.

6.7 *Relationship with the Agreement*

6.7.1 Nothing in the Agreement or this Policy shall be construed to prevail over any conflicting provision of the EU Standard Contractual Clauses or the UK Addendum. For the avoidance of doubt, where this Policy further specifies audit rights, security controls, or Sub-processor obligations, such specifications shall apply in addition to the EU Standard Contractual Clauses and the UK Addendum.

7 Authorised Sub-Processors

7.1 Subject to the service, the following sub-processors may be necessary to provide services to Customer, with minimal Support Data processed for the purposes outlined in this Policy and relevant Agreement:

- **Bluesource Inc** (Bluesource North America)

  Part of the Bluesource group of companies and located in Dallas, U.S.A.

  Purpose of processing: part of Bluesource's global service management centre, providing 24/7/365 support, monitoring, and managed services. Personal Data relating to contacts and support issues may be processed to provide the Services and raise service tickets. The systems processing the data are hosted within the UK and/or EEA.

  Processing location (address): Suite 225, 1900 Enchanted Way, Grapevine, Dallas, Texas, 76051, USA using Bluesource's systems hosted within the UK and/or EEA.

  To comply with the GDPR and Data Protection Law, following completion of appliable TRA and TIA, SCCs and a UK Addendum have been agreed between Bluesource and Bluesource Inc, as exporter and importer of Personal Data.

Cloud Bridge Recruitment Limited ("Cloud Bridge")

Provision of fulltime exclusive workers to facilitate 24x7s services, who are otherwise treated as a Bluesource employees.

Purpose of processing: part of Bluesource's global service management centre, providing 24/7/365 support, monitoring, and managed services. Personal Data relating to contacts and support issues may be processed to provide the services and raise service tickets. The systems processing the data are hosted within the UK and/or EEA.

Processing location (address): Manila, Philippines.

To comply with the GDPR and Data Protection Law, following completion of appliable TRA and TIA, SCCs and a UK Addendum have been agreed between Bluesource and Cloud Bridge Recruitment Limited, as exporter and importer of Personal Data.

Columbus

Services: Specialist support and consultancy related to MS Dynamics.

Processing location (address): UK, India

To comply with Data Protection Law, their workers in India are employees of the UK based company.

Distributers and Vendors (where relevant and specific to goods and/or services requested)

Services: procurement and licensing of goods/services procured for Customer. Minimal Support Data relating to a Designated Contact or Data Subject may need to be processed for licensing, shipping, or support escalation.

Processing location (address): specific to goods and/or services requested.

Harbor Solutions

Bluesource partner specialising in backup technologies.

Purpose of processing: providing 24/7/365 support, monitoring, and managed services related to backup technologies, including backup-as-a-service ("BaaS"). Personal Data relating to contacts and support issues may be processed to provide the services and raise service tickets and process Customer backup data.

Processing location (address): UK.

HubSpot UK Holdings Limited

Services: Marketing SaaS tool for Bluesource

Processing location (address): Europe in accordance with https://legal.hubspot.com/hubspot-regional-data-hosting-policy

Inforcer

Services: Inforcer is a Microsoft 365 multi-tenant management SaaS platform that enables Bluesource to standardise, secure and govern customer tenants at scale from a single pane of glass.

Processing location (address): Restricted to UK and EU

Microsoft

Services: MS Azure platform, hosting Bluesource's systems, and Office365. Also used for vendor escalation if applicable to a Service, such as the "Enhanced Support for MS" service.

Processing location (address): MS Azure within UK and/or EEA geography.

- **MS Azure OpenAI**

  Services: Microsoft Azure's OpenAI Large Language Model (LLM) used in connection with Bluesource's internal RAG AI tool, Moses, used to aid support services and knowledge learning, and where applicable to aid marketing and professionals services, within Bluesource's acceptable use policy for AI.

  Processing location (address): MS Azure within UK and/or EEA geography**.**

- **Mouton Global**

  Services: Specialist support and consultancy related to networking.

  Processing location (address): UK.

- **Nexus Open Systems**

  Services: Specialist support and consultancy related to voice technologies.

  Processing location (address): UK.

- **Onyx**

  Services: AI enabled SaaS licencing tool expert to review, optimise and plan licensing and assist with migration planning.

  Processing location (address): US.

- **Proventeq**

  Services: Specialist support and consultancy related to MS cloud technologies.

  Processing location (address): UK, and India.

  To comply with Data Protection Law, their workers in India are employees of the UK based company.

- **Sikuli**

  Services: Specialist support and consultancy related to MS cloud technologies.

  Processing location (address): Singapore.

  Whilst not strictly a sub-processor of Bluesource or Customer data, as they are passing qualified leads to Bluesource containing minimal contact data and liaising with us, SCCs and a UK Addendum have been agreed between Bluesource and Sikuli, as exporter and importer of Personal Data.

- **Vidette**

  Purpose of processing: part of Bluesource's global service management centre, providing 24/7/365 support, monitoring, and managed services. Personal Data relating to contacts and support issues may be processed to provide the services and raise service tickets. The systems processing the data are hosted within the UK and/or EEA.

  Processing location (address): UK (they also operate in other geographies but services to Bluesource are currently provided from UK)

  To comply with the GDPR and Data Protection Law, following completion of appliable TRA and TIA, SCCs and a UK Addendum have been agreed between Bluesource and Vidette, as exporter and importer of Personal Data.

7.2 Where a Service uses alternative and/or additional Sub-processors, **Clause 4.5.6** shall apply and as applicable, detailed in a Service Schedule and/or Work Order.

7.3 **Applicability of sub-processors to services** - The following table provides an overview of which sub-processors are likely to be involved in which services:

SERVICE	SUBPROCESSOR														
	Bluesource Inc.	Cloudbridge	Columbus	Distributors & Vendors	Harbor	HubSpot	Microsoft	Inforcer	Mouton Global	MS Azure OpenAI	Nexus	Onyx	Proventeq	Sikuli	Vidette
UK Business Hour Reactive Support										✓					
24/7 Reactive Support	O	✓				O				✓					✓
Enhanced Support for MS		✓					✓	O		✓		✓	O		✓
Advanced Support for MS		✓					✓	✓		✓		✓	O		✓
Managed Services		✓			O					✓			O		✓
Professional Services	O		O	O	O			O	O	✓	O		O		O
Backup Services		✓		O	✓					✓					✓
Bluesource's marketing activities				O		✓				✓				✓	
MS Dynamics Services			✓							✓					
Networking Services									✓	✓					
Procurement of goods/services				O	O		O					✓			
Voice Services										✓	✓				

KEY: O use depends on scope of the goods/services ordered

✓ applicable to the service

8 Governance and Review

This Policy is owned by Bluesource and is reviewed periodically to ensure it remains aligned with applicable Data Protection Law, regulatory guidance, and Bluesource's processing activities. The Policy may be updated from time to time in accordance with the change provisions set out in the Agreement.

9 Sign Off

For Bluesource	
Name	Nick Jaggers
Position	Head of Operations
Signature	
Date	01/05/2026

10 Revision History

Revision Date	Reviser	Description of Revision
30/08/2023	Nick Jaggers	Policy updated and republished
22/02/2024	Nick Jaggers	Reviewed and rebranded
18/04/2024	Nick Jaggers	Sub processors updated
09/04/2025	Nick Jaggers	Update
11/06/2025	Nick Jaggers	Applicability table added
31/07/2025	Nick Jaggers	Updated for the use of AI within Bluesource.
28/04/2026	Nick Jaggers	Annual review and update. Reference to EU and UK GDPR revised and inclusion of the addendums that were put in place. Key sub-processor list updated.

SCHEDULE 1 – DESCRIPTION OF PROCESSING

(EU Standard Contractual Clauses – Annex I.B)

This Schedule 1 describes the Processing of Personal Data for the purposes of Annex I.B of the EU Standard Contractual Clauses and applicable Data Protection Law.

The subject-matter, nature, purpose, categories of Personal Data, and categories of Data Subjects are as described in **Section 4** (Personal Data and Data Processing) of the main body of this Policy/DPA, including:

- the nature and purposes of the Processing (**Clause 4.1**);
- the nature and location of the Processing (**Clause 4.2**);
- the categories of Personal Data processed (**Clause 4.3**); and
- the categories of Data Subjects concerned (**Clause 4.4**).

The duration of the Processing shall correspond to the duration of the Services provided under the applicable Agreement, unless otherwise required by applicable law, as set out in **Clause 4.6** (Duration of Processing).

OPTIONAL CLAUSES OF THE EU STANDARD CONTRACTUAL CLAUSES

For the purposes of the EU Standard Contractual Clauses:

1. Except where applicable Data Protection Law requires otherwise, the governing law of the EU Standard Contractual Clauses shall be the laws of England and Wales, and the courts of England and Wales shall have jurisdiction.
2. Clause 7 (Docking Clause) of the EU Standard Contractual Clauses shall not apply.
3. Clause 11(a) (Redress) of the EU Standard Contractual Clauses shall not apply.
4. Where Bluesource acts as Controller, Option 1 (General Written Authorisation) of Clause 9 (Use of Sub-processors) shall apply, subject to the notification and objection periods set out in the applicable Agreement and **Section 7** (Authorised Sub-processors) of this Policy**.**

ANNEX I A – LIST OF PARTIES

For the purposes of the EU Standard Contractual Clauses:

- **Data Exporter**: As identified in the applicable Agreement (the Customer or Bluesource, as applicable).
- **Data Importer:** The relevant Sub-processor engaged by Bluesource in accordance with this Policy and the applicable Agreement.
- Where Bluesource is deemed the Controller, Module 2: Transfer Controller to Processor shall apply, such as for exporting Support Data to its Sub-processor, as the importer.
- Where Bluesource is deemed the Processor of Customer Data and exporting such data to its Sub-processor, as the importer, Module 3: Transfer Processor to Processor shall apply.

The identity and contact details of the Parties are set out in the applicable Agreement and, in respect of SCC-relevant transfers, in the relevant Sub-processor agreement entered into by Bluesource.

ANNEX I B – DESCRIPTION OF TRANSFER

The description of the transfer, including the categories of data, purposes of processing, frequency of transfer, and nature of processing operations, is set out in **Section 4** (Personal Data and Data Processing) and **Section 6** (International Processing) of the main body of this Policy/DPA.

ANNEX I C – COMPETENT SUPERVISORY AUTHORITY

For the purposes of Clause 13 of the EU Standard Contractual Clauses:

- Where the data exporter is established in the United Kingdom, the competent supervisory authority shall be the **Information Commissioner's Office (ICO).**
- Where the data exporter is established in the European Union, the competent supervisory authority shall be the authority of the Member State in which the exporter is established.

SCHEDULE 2 – Technical and Organisational Measures

(EU Standard Contractual Clauses – Annex II)

This Schedule 2 describes the Technical and Organisational Measures implemented for the purposes of Annex II of the EU Standard Contractual Clauses and Article 32 of the UK GDPR and EU GDPR.

Bluesource applies the Technical and Organisational Measures described in **Section 5** (Security of Processing) including the obligations set out in **Clause 4.5.5** (Security of Processing) of the main body of this Policy, including measures addressing:

- access control and least-privilege principles;
- encryption and pseudonymisation where appropriate;
- confidentiality, integrity, availability, and resilience of systems;
- incident response and business continuity; and
- regular testing and evaluation of security controls.

Where Customer Personal Data is transferred to a Sub-processor, Bluesource ensures that appropriate Technical and Organisational Measures are contractually imposed on the Sub-processor, commensurate with the risks of the Processing and consistent with the requirements of Article 32 GDPR and Annex II of the EU Standard Contractual Clauses.

Sub-processors are **not permitted to engage further sub-processors** except where expressly authorised in writing by Bluesource in accordance with **Clause 4.5.6** (Sub-processing) and **Section 7 (Authorised Sub-processors)** of this Policy.

SCHEDULE 3 – List of Subprocessors

(EU Standard Contractual Clauses – Annex III)

This Schedule 3 describes the permitted Sub-processors for the purposes of Annex III of the EU Standard Contractual Clauses and applicable Data Protection Law.

The authorised Sub-processors, together with details of:

- the nature of the services provided;
- the location of Processing; and
- applicable international transfer safeguards,

are set out in **Section 7** (Authorised Sub-processors) of the main body of this Policy/DPA.

No Sub-processor is permitted to appoint its own sub-processors except where expressly authorised in writing by Bluesource and subject to equivalent data protection obligations.