

APPENDIX 'A' — DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is entered into between:

The Data Controller:

Name: [_____]

Company registration no.: [_____]

Address: [_____]

Represented by: [_____]

Privacy Contact: [_____]

(hereinafter "**Data Controller**" or "**Controller**")

AND

The Data Processor:

The Inactiv.com Media Solutions Private Limited

Address: 22 Rustam Bagh Main Road, Bangalore – 560017, India

Represented by: Akshat Choudhary (Director)

Privacy Contact: privacy@blogvault.net

The Inactiv.com Media Solutions Private Limited provides website backup, security, performance, migration, and management services under the product names BlogVault, MalCare, WP Remote, Airlift, and Migrate Guru. In this DPA, "BlogVault" refers to the company (The Inactiv.com Media Solutions Private Limited) and its products collectively.

(hereinafter "**Data Processor**" or "**BlogVault**")

The Controller and the Processor are hereinafter jointly referred to as the "**Parties**" and individually as "**Data Processor**" and "**Data Controller**" respectively.

1. INTRODUCTION

1.1 This Data Processing Agreement sets out the terms under which the Data Processor processes personal data on behalf of the Data Controller in connection with the BlogVault engagement agreement (the "**Main Agreement**"), in which the Parties have agreed to the terms for the Data Processor's delivery of services to the Data Controller (the "**Main Services**"). This DPA shall be effective as from the Effective Date.

1.2 Definitions:

1.2.1 The terms "**Data Controller**", "**Data Subject**", "**Personal Data**", "**Process**", "**Processing**", "**Processor**", and "**Supervisory Authority**" shall have the meanings given to these terms in the Applicable Data Protection Law.

1.2.2 "**Services**" means the website backup, security scanning, malware detection and removal, performance monitoring and optimisation, website migration, uptime monitoring, staging, and related management services provided by BlogVault under the product names BlogVault, MalCare, WP Remote, Airlift, and Migrate Guru, and any related account management and support services.

1.2.3 "**Applicable Data Protection Law**" means:

- (a) the EU General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR") and any implementing national legislation;
- (b) the UK General Data Protection Regulation as retained in UK law by the European Union (Withdrawal) Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ("UK GDPR"), together with the UK Data Protection Act 2018;
- (c) any other applicable data protection or data privacy law or regulation of the European Union, European Economic Area, or the United Kingdom.

1.2.4 "**GDPR**" means the EU General Data Protection Regulation (Regulation (EU) 2016/679).

1.2.5 "**Personal Data Breach**" or "**Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Controller Controlled Data transmitted, stored, or otherwise processed by the Data Processor or its Sub-Processors.

1.2.6 "**Security Measures**" means the technical and organisational security measures set out in **Sub-Appendix B**.

1.2.7 "**Sub-Processor**" means any entity (other than the employees or agents of the Data Processor) engaged by the Data Processor or by any other Sub-Processor to process Controller Controlled Data on behalf of the Data Controller.

1.2.8 "**Controller Controlled Data**" means the personal data processed by BlogVault on behalf of and in accordance with the instructions of the Data Controller as part of the Services, but only to the extent that such processing is subject to Applicable Data Protection Law.

1.2.9 "**End Users**" means the users of the Data Controller's website, software products, applications, and related support services.

1.2.10 "**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses adopted by the European Commission in its Implementing Decision (EU) 2021/914 of 4 June 2021, as amended or replaced from time to time, and, where the UK GDPR applies, together with

the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under s.119A of the Data Protection Act 2018 (the "**UK Addendum**").

1.2.11 "Transfer Impact Assessment" or "TIA" means an assessment of the laws and practices of the destination country of a cross-border transfer, evaluating whether the personal data transferred would be afforded an adequate level of protection, and identifying any supplementary measures necessary.

1.2.12 "EU-US Data Privacy Framework" or "DPF" means the framework adopted by the US Department of Commerce and recognised as adequate by the European Commission under Implementing Decision (EU) 2023/1795 of 10 July 2023, as amended or replaced.

1.2.13 "Effective Date" means the date on which the Data Controller accepted or the Parties otherwise agreed to this DPA.

2. SCOPE AND APPLICABILITY

2.1 This DPA applies to the processing of Controller Controlled Data by the Data Processor on behalf of the Data Controller in connection with the Main Services.

2.2 This DPA shall ensure that the Data Processor complies with the Applicable Data Protection Law, including but not limited to:

- (a) Regulation (EU) 2016/679 (EU GDPR);
- (b) UK GDPR and the UK Data Protection Act 2018, where the Data Controller or End Users are located in the United Kingdom.

2.3 The Data Processor does not assume any responsibility or liability for the processing of personal data by the Data Controller that falls outside the scope of this DPA, including personal data processed through Third-Party Services or outside of the Main Services.

2.4 Independent Controller Processing: BlogVault may process certain account, billing, business contact, support, and service usage information as an independent data controller for its own legitimate business purposes, including account administration, billing, legal compliance, fraud prevention, service improvement, and security. Such processing is outside the scope of this DPA and is described in BlogVault's Privacy Policy.

3. PROCESSING OF PERSONAL DATA

3.1 The categories, types, and nature of Personal Data processed by the Data Processor on behalf of the Data Controller are set out in **Sub-Appendix A**.

3.2 The Data Processor shall only process Controller Controlled Data to the extent, and in such a manner, as is necessary to provide the Main Services in accordance with the documented instructions of the Data Controller, unless processing is required by Applicable Data Protection Law or other Union or Member State law to which the Data Processor is subject; in such case, the Data Processor shall inform the Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.3 The Data Processor shall ensure that any person authorised to process the Personal Data has committed himself or herself to confidentiality obligations or is under an appropriate statutory obligation of confidentiality.

3.4 Record of Processing Activities:

The Data Processor shall maintain records of its processing activities to the extent required by Applicable Data Protection Law (including **Article 30** of the GDPR) and shall provide the Data Controller with information reasonably necessary to demonstrate the Data Processor's compliance with this DPA.

3.5 Details of Data Processing:

Element	Description
Subject Matter	Processing of Controller Controlled Data as described in this DPA
Duration	As specified in the Main Agreement
Purpose	Provision of the Main Services as initiated by the Data Controller
Nature of Processing	The Main Services as described in the Main Agreement
Type of Personal Data	As set out in Sub-Appendix A
Categories of Data Subjects	The Data Controller, its End Users, and any other individuals whose personal data is included in the Controller Controlled Data processed as part of the Main Services

4. DATA CONTROLLER'S INSTRUCTIONS

4.1 The Data Processor shall process Personal Data only on documented instructions from the Data Controller (the "**Instructions**"). The Instructions at the time of entering into this DPA are that the Data Processor may only process Personal Data for the purpose of delivering the Main Services as described in the Main Agreement.

4.2 Additional instructions outside the scope of this DPA require prior written agreement between the Parties, including agreement on any additional fees payable by the Data Controller. The Data Processor shall promptly inform the Data Controller if, in the Data Processor's opinion, an instruction infringes Applicable Data Protection Law.

4.3 The Data Controller warrants that:

- (a) its Instructions comply with all applicable laws, regulations, and rules;
- (b) the Controller Controlled Data has been collected lawfully and in accordance with the Applicable Data Protection Law;
- (c) the processing in accordance with the Instructions will not cause the Data Processor to breach any applicable laws or regulations.

4.4 The Data Processor shall not access or use Controller Controlled Data except as provided in the Main Agreement, as necessary to maintain or provide the Main Services, or as necessary to comply with applicable law or a binding order of a governmental, law enforcement, or regulatory body.

5. DATA PROCESSOR'S OBLIGATIONS

5.1 Compliance with Instructions

The Data Processor shall process Controller Controlled Data only in accordance with the Instructions. The Data Processor shall promptly notify the Data Controller if, in the Data Processor's opinion, any Instruction infringes Applicable Data Protection Law, or if the Data Processor is unable to comply with any Instruction. Where Applicable Data Protection Law prevents the Data Processor from complying with an Instruction, the Data Processor shall notify the Data Controller without undue delay, unless such notification is prohibited by law on important grounds of public interest (e.g., a prohibition under law to preserve the confidentiality of a law enforcement investigation).

5.2 Confidentiality

The Data Processor shall treat all Personal Data as strictly confidential. Personal Data shall not be copied, transferred, or otherwise processed in conflict with the Instructions, unless the Data Controller has agreed in writing. All Data Processor personnel authorised to process Personal Data shall be subject to binding confidentiality obligations.

5.3 Security Measures

- 5.3.1** The Data Processor shall implement and maintain the technical and organisational security measures set out in **Sub-Appendix B**, in accordance with the requirements of **Article 32** of the GDPR, 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 risk of varying likelihood and severity for the rights and freedoms of natural persons.
- 5.3.2** The Data Processor may update its Security Measures from time to time, provided that such updates do not materially decrease the overall level of protection for Controller Controlled Data.
- 5.3.3** Access to Controller Controlled Data shall be restricted to Data Processor personnel who require such access to perform their duties in connection with the Main Services, and who are bound by appropriate confidentiality obligations.
- 5.3.4** The Data Processor shall provide documentation of its Security Measures to the Data Controller upon written request.

5.4 Personal Data Breach Notification

- 5.4.1** The Data Processor shall notify the Data Controller **without undue delay and in any event within seventy-two (72) hours** after becoming aware of a Personal Data Breach affecting Controller Controlled Data. "Awareness" shall mean the point at which the Data Processor has a reasonable degree of certainty that a security incident has occurred that has led or may lead to a Personal Data Breach.
- 5.4.2** The initial notification shall include at minimum:
- (a) a description of the nature of the Breach, including where possible the categories and approximate number of Data Subjects and Personal Data records concerned;
 - (b) the name and contact details of the Data Processor's privacy contact from whom more information can be obtained;
 - (c) a description of the likely consequences of the Breach;
 - (d) a description of the measures taken or proposed to be taken by the Data Processor to address the Breach, including, where appropriate, measures to mitigate its possible adverse effects.
- 5.4.3** Where it is not possible to provide all information within 72 hours, the Data Processor shall provide the information in phases without further undue delay as it becomes available.
- 5.4.4** The Data Processor shall cooperate with the Data Controller and provide reasonable assistance to enable the Data Controller to comply with its notification obligations under **Articles 33 and 34** of the GDPR.
- 5.4.5** The Data Processor shall document all Personal Data Breaches, including the facts relating to the Breach, its effects, and the remedial action taken, in accordance with **Article 33(5)** of the GDPR.
- 5.4.6** The Data Processor's obligation under this Section does not apply to incidents caused solely by the Data Controller's systems, credentials, instructions, or Third-Party Services outside the Data Processor's control.
- 5.4.7 Division of Breach Notification Responsibility:** The Parties acknowledge the following allocation of breach notification obligations under the GDPR:
- (a) The Data Processor is responsible for notifying the Data Controller of any Personal Data Breach affecting Controller Controlled Data, in accordance with Sections 5.4.1 to 5.4.5;
 - (b) The Data Controller is responsible for: (i) assessing whether the Breach is likely to result in a risk to the rights and freedoms of Data Subjects and, if so, notifying the relevant Supervisory Authority within seventy-two (72) hours of becoming aware, in accordance with GDPR Article 33; (ii) assessing whether the Breach is likely to result in a high risk to the rights and freedoms of Data Subjects and, if so, directly notifying the affected Data Subjects without undue delay, in accordance with GDPR Article 34.
 - (c) The Data Processor shall provide the Data Controller with all information reasonably necessary to enable the Data Controller to carry out its notification obligations under (b) above.

5.5 Data Protection Impact Assessment and Prior Consultation

- 5.5.1** Taking into account the nature of processing and the information available to the Data Processor, the Data Processor shall assist the Data Controller in:
- (a) preparing data protection impact assessments in accordance with Article 35 of the GDPR, where such assessments are required; and
 - (b) any prior consultations with the Supervisory Authority in accordance with Article 36 of the GDPR.
- 5.5.2** The Data Processor shall also provide reasonable assistance to the Data Controller in fulfilling its obligations to respond to requests by Data Subjects under **Chapter III** of the GDPR, taking into account the nature of the Main Services and the information available to the Data Processor.

5.6 Sub-Processors

5.6.1 The Data Controller gives general authorisation for the Data Processor to engage Sub-Processors to process Controller Controlled Data. A current list of Sub-Processors is set out in **Sub-Appendix C**.

5.6.2 The Data Processor shall give the Data Controller at least **fourteen (14) days' prior written notice** before appointing any new Sub-Processor or replacing an existing Sub-Processor. The notice shall include the name and processing activities of the proposed Sub-Processor.

5.6.3 The Data Controller may object to a proposed Sub-Processor by notifying the Data Processor in writing within the notice period, provided the objection is reasonable and relates to data protection concerns. If the Data Controller objects, the Data Processor shall not permit the objected-to Sub-Processor to process Controller Controlled Data. If BlogVault cannot reasonably accommodate the objection, either party may terminate only the affected Services in accordance with the Main Agreement.

5.6.4 The Data Processor shall impose contractual obligations on each Sub-Processor that provide at least the same level of data protection as set out in this DPA, including obligation to:

- (a) process Personal Data only on the Data Controller's documented instructions;
- (b) ensure that persons authorised to process Personal Data have committed to confidentiality;
- (c) implement appropriate technical and organisational security measures;
- (d) assist with breach notification, DPIAs, and Data Subject requests as applicable.

5.6.5 The Data Processor shall remain fully liable to the Data Controller for the performance of each Sub-Processor's data protection obligations as if the Data Processor had performed them directly, to the same extent the Data Processor would be liable under this DPA for its own acts or omissions.

5.6.6 Except as set forth in this Section 5.6, the Data Processor shall not permit any Sub-Processor to access Controller Controlled Data.

5.7 Audit Rights

5.7.1 The Data Processor shall make available to the Data Controller information reasonably necessary to demonstrate the Data Processor's compliance with this DPA, in the first instance through documentation such as security certifications, third-party audit reports, and compliance documentation, upon written request.

5.7.2 Where such documentation does not sufficiently address the Data Controller's reasonable and documented concerns, or where the Data Controller is legally required to conduct an audit, the Data Processor shall allow for and contribute to a reasonable audit by the Data Controller or a third-party auditor mandated by the Data Controller, subject to the conditions in this Section.

5.7.3 Any audit shall: (a) be conducted on no less than **thirty (30) days' prior written notice**, specifying scope and timing; (b) be limited in scope to matters relevant to this DPA; (c) be conducted once per twelve (12) month period unless triggered by a specific incident (such as a Personal Data Breach) or required by law or a regulator; (d) be carried out at the Data Controller's cost; (e) not unreasonably interfere with the Data Processor's normal operations; (f) be conducted by an auditor who is not a competitor of the Data Processor and who is bound by appropriate confidentiality obligations; and (g) not permit access to any other customer's data or to information not relevant to the Data Processor's compliance with this DPA.

5.7.4 The Data Processor may redact from any documentation or audit results any information that is confidential, relates to third parties, or is not relevant to the Data Processor's compliance with this DPA.

5.8 Data Subject Requests

5.8.1 The Data Processor shall promptly notify the Data Controller if the Data Processor receives a request directly from a Data Subject in relation to Controller Controlled Data. The Data Processor shall not respond directly to any such request unless authorised to do so by the Data Controller or required by Applicable Data Protection Law.

5.8.2 Taking into account the nature of the Main Services and the information available to the Data Processor, the Data Processor shall provide reasonable assistance to the Data Controller in responding to Data Subject requests under **Chapter III** of the GDPR, including access, rectification, erasure, restriction, data portability, and objection. Where the Data Controller can access, export, correct, or delete the relevant Controller Controlled Data through the Main Services, the Data Controller is responsible for doing so.

5.8.3 Where the Data Controller accesses or deletes data through its account, the Data Controller acknowledges that it is responsible for fulfilling the applicable Data Subject request and for notifying the Data Subject accordingly.

5.9 Deletion and Return of Data

5.9.1 The Data Controller may access and delete some Controller Controlled Data through the Data Controller's account. For any data not accessible through the account, the Data Processor shall, upon the Data Controller's written request and unless prohibited by applicable law:

- (a) return the Controller Controlled Data to the Data Controller; and/or

- (b) delete the Controller Controlled Data in accordance with the Data Processor's data retention policy (Sub-Appendix D) and applicable backup cycles, and request that Sub-Processors do the same.

5.9.1.1 Deletion Confirmation: The Data Processor shall complete deletion in accordance with its data retention policy and backup cycles and shall provide written confirmation of deletion to the Data Controller upon request where reasonably available.

5.9.2 A request for data return under Section 5.9.1(a) must be made within sixty (60) days after termination of the applicable Main Services.

5.9.3 Data stored in backup systems may be retained for up to **ninety (90) days** after termination, during which time it shall be securely isolated and protected from any further processing, except as required by applicable law. Thereafter, such backup data shall be deleted in accordance with the Data Processor's data retention policy.

5.9.4 For Controller Controlled Data processed by Sub-Processors, the Data Processor will instruct the relevant Sub-Processors to delete or return such data in accordance with this DPA and the applicable sub-processor agreement. Deletion by Sub-Processors may be subject to their own backup cycles and legal retention obligations.

5.10 Government and Legal Requests

The Data Processor shall notify the Data Controller, if permitted by applicable law, upon receiving:

- (a) an inquiry, complaint, or request from a Data Subject or other individual whose personal data is included in the Controller Controlled Data;
- (b) a binding demand (such as a court order or subpoena) from a government, law enforcement, regulatory, or other body;

in respect of Controller Controlled Data processed on the Data Controller's behalf.

6. INTERNATIONAL DATA TRANSFERS

6.1 The Data Controller acknowledges that the Data Processor may transfer Controller Controlled Data to countries other than the country in which the Data Controller is located, for the purpose of providing the Main Services.

6.2 Primary Data Storage:

The Data Processor stores Controller Controlled Data (including all backup archives and website content) primarily within the European Union, specifically:

- Hetzner data centers in Germany; and/or
- Amazon (AWS) EU regions (Ireland and/or Frankfurt).

Some operational and infrastructure processing may occur in the United States and India for service delivery, customer support, infrastructure management, and security monitoring. The Data Controller acknowledges that access to stored data by Data Processor personnel may occur from other locations (including India) for these purposes. Such access constitutes a cross-border transfer and is covered by the transfer mechanisms set out in Section 6.3.

6.3 Transfer Mechanisms:

Where transfers of Controller Controlled Data to a third country (i.e., outside the EEA, UK, or Switzerland) are required and no adequacy decision by the European Commission (or UK adequacy regulations) covers the transfer, the Data Processor shall ensure that such transfers are made subject to appropriate safeguards, including one or more of the following:

(a) Standard Contractual Clauses: The Parties agree that the **2021 SCCs (Module Two: Controller to Processor)** set out in the Annex to this DPA shall apply to such transfers. Where the UK GDPR applies, the UK Addendum shall apply alongside the SCCs.

(b) EU-US Data Privacy Framework: Where a recipient is certified under the EU-US Data Privacy Framework (DPF), transfers to such recipient shall be made in reliance on the DPF. Where the DPF does not apply or a recipient's DPF certification lapses, transfers shall be made subject to the SCCs or another appropriate transfer mechanism under this Section 6.3.

(c) Adequacy Decisions: Transfers to countries for which the European Commission has issued an adequacy decision (or which are subject to UK adequacy regulations) shall be made in reliance on such adequacy decision.

(d) Other Safeguards: Where no other mechanism applies, transfers may be made subject to binding corporate rules, approved codes of conduct, or approved certification mechanisms, as applicable.

6.4 Transfer Assessments and Supplementary Measures:

Where required by Applicable Data Protection Law, the Data Processor will assess restricted transfers and implement appropriate supplementary measures, taking into account the nature of the transfer, the Controller Controlled Data involved, and the safeguards available. The Data Processor may provide relevant transfer information upon reasonable request, subject to confidentiality, security, and legal limitations.

6.5 If the Data Processor reasonably requires the Data Controller to enter into SCCs or other appropriate safeguards in respect of international transfers, the Data Controller shall cooperate and do so promptly.

7. LIABILITY

7.1 The liability of each Party under this DPA shall be subject to the exclusions and limitations of liability set out in the Main Agreement, which shall apply equally to this DPA as if it were an integrated part thereof.

7.2 Each Party shall be liable to the other for damages caused by its breach of this DPA or the Applicable Data Protection Law, subject to the limitations in the Main Agreement.

8. PRIVACY CONTACT

The Data Processor's designated privacy contact is:

BlogVault Privacy Team

Email: privacy@blogvault.net

The Data Controller's designated privacy contact is:

[_____]

Email: [_____]

9. DURATION AND TERMINATION

9.1 This DPA shall remain in force for the duration of the Main Agreement.

9.2 Upon termination or expiry of the Main Agreement:

- (a) the Data Processor's authorisation to process Personal Data on behalf of the Data Controller shall cease;
- (b) the Data Processor shall, at the Data Controller's choice, return or delete all Controller Controlled Data in accordance with Section 5.9;
- (c) the Data Processor may retain Controller Controlled Data in backup systems for up to ninety (90) days after termination, subject to the protections described in Section 5.9.3.

9.3 Sections 5.3 (Security), 5.4 (Breach Notification), 5.6 (Sub-Processors — to the extent Sub-Processors retain data), 5.9 (Deletion and Return of Data — to the extent deletion is ongoing), 7 (Liability), 10 (Governing Law), and the SCCs/UK Addendum shall survive termination of this DPA.

10. GOVERNING LAW AND DISPUTE RESOLUTION

10.1 Governing Law:

This DPA shall be governed by and construed in accordance with the laws of India.

10.2 Hierarchy:

In the event of a conflict between this DPA and the SCCs or UK Addendum, the SCCs or UK Addendum shall prevail for the relevant restricted transfer. Nothing in this DPA shall limit any liability, Data Subject right, or other protection that cannot be limited under Applicable Data Protection Law, the SCCs, or the UK Addendum.

10.3 Dispute Resolution:

Any dispute arising out of or in connection with this DPA that cannot be resolved by the Parties through good faith negotiation within thirty (30) days shall be referred to the competent courts of Bangalore, India. Notwithstanding the foregoing, either Party may seek injunctive or other equitable relief in any court of competent jurisdiction to prevent irreparable harm.

10.4 Notwithstanding the above, nothing in this DPA shall limit the rights of a Data Subject under Applicable Data Protection Law, including the right to lodge a complaint with a Supervisory Authority or to seek judicial remedy.

11. AMENDMENTS

This DPA may only be amended or modified by a written instrument signed by both Parties. The Data Processor may update the Security Measures (Sub-Appendix B) and Sub-Processor list (Sub-Appendix C) in accordance with the procedures set out in Sections 5.3.2 and 5.6.2 respectively.

12. SEVERABILITY

If any provision of this DPA is held to be invalid, illegal, or unenforceable, the remaining provisions shall continue in full force and effect.

13. ENTIRE AGREEMENT

This DPA, together with the Main Agreement, the Sub-Appendices, and the SCCs (where applicable), constitute the entire agreement between the Parties with respect to the processing of Personal Data and supersede all prior agreements, understandings, and arrangements relating to such processing.

SIGNATURES

IN WITNESS WHEREOF, the Parties have executed this Data Processing Agreement as of the Effective Date.

For the Data Controller:

Name: _____

Title: _____

Date: _____

Signature: _____

For the Data Processor (BlogVault):

Name: Akshat Choudhary

Title: Director

Date: _____

Signature: _____

SUB-APPENDIX A — CATEGORIES OF PERSONAL DATA

The Data Processor processes the following categories of Personal Data in connection with its delivery of the Services:

Controller Controlled Data (processed as Data Processor on behalf of the Data Controller):

Category	Description
Website Content	The contents of the Data Controller's website(s) uploaded to or processed through the Services, which may include: WordPress database contents, posts, pages, comments, media files, user accounts, email addresses, form submissions, WooCommerce orders, metadata, plugin and theme data, configuration files, and logs
Backup Archives	Full and incremental backup copies of the Data Controller's website(s), including database dumps, file system archives, and migration copies
Security Scan Data	Results of security scans, malware signatures, file paths, suspicious code snippets, URLs flagged by scanning, and IP logs generated by the security services
Internet Protocol (IP) Address	IP addresses of End Users and administrators accessing the Data Controller's website(s)
Site Access Credentials	Access tokens, API keys, SFTP/SSH credentials, or database credentials provided by the Data Controller to enable the Services (stored in encrypted form)

Special Categories of Data

BlogVault does not intentionally collect special-category data (as defined in GDPR Article 9) as a distinct service category. However, Controller Controlled Data (particularly Website Content and Backup Archives) may contain special-category data if the Data Controller's website, database, or backups include such data. The Data Controller is responsible for ensuring lawful processing of any special-category data included in the content processed through the Services.

SUB-APPENDIX B — SECURITY MEASURES

The Data Processor implements and maintains the following technical and organisational security measures in accordance with **Article 32** of the GDPR, 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 risk of varying likelihood and severity for the rights and freedoms of natural persons:

- Data is encrypted in transit and, where supported by the relevant systems, at rest.
- Access controls are designed to restrict access to authorised personnel.
- MFA is required for personnel access to designated production systems.
- BlogVault maintains vulnerability management, access control, backup, restoration, and incident response processes.

The Data Processor may update these measures from time to time, provided that such updates do not materially decrease the overall level of protection for Controller Controlled Data. Further information is available to the Data Controller upon written request in accordance with Section 5.3.4.

SUB-APPENDIX C — LIST OF SUB-PROCESSORS

BlogVault uses the sub-processors listed below to provide, secure, support, bill, and improve the Main Services. Each sub-processor is permitted to process Controller Controlled Data only as necessary for the relevant function and is subject to written contractual obligations designed to provide a level of data protection materially equivalent to that provided by this DPA. The Controller gives the Data Processor general authorisation to use these sub-processors and any replacement or additional sub-processors notified in accordance with Section 5.6.

Sub-Processors

Sub-Processor	Function
Hetzner	Infrastructure
Amazon Web Services / Amazon	Infrastructure, cloud services, communications, AI services, and operational services
DigitalOcean	Infrastructure
Google / Google Cloud	Infrastructure, cloud services, AI services, analytics, communications, and operational services
Microsoft	Infrastructure
Cloudflare	Network, security, and traffic delivery
Stripe	Payments
PayPal	Payments
Freshdesk / Freshworks	Customer support and communications
Postmark	Transactional communications
Brevo	Communications
HubSpot	CRM and customer communications
OpenAI	AI services and automation
Anthropic	AI services and automation

Artificial Intelligence Service Providers

BlogVault may use third-party artificial intelligence and machine learning service providers (including those listed above) to support, automate, improve, or provide parts of the Main Services, including customer support assistance, diagnostics, security analysis, summarisation, classification, and operational automation. Such providers may process Controller Controlled Data only as necessary for the applicable function and subject to appropriate contractual, security, and transfer safeguards. BlogVault will use reasonable measures designed to limit the Controller Controlled Data submitted to such providers to what is necessary for the relevant function.

Updates to This List

BlogVault may update this list from time to time. Where required by Applicable Data Protection Law, the Data Processor will provide notice of additions or replacements and give the Controller an opportunity to object on reasonable data-protection grounds, in accordance with Section 5.6.

International Transfers

The Data Processor and its sub-processors may process Controller Controlled Data in countries other than the country in which the Controller or Data Subjects are located. Where such processing involves a restricted transfer under Applicable Data Protection Law, the Data Processor will ensure that an appropriate transfer mechanism is in place, such as an adequacy decision, the EU Standard Contractual Clauses, the UK Addendum, the EU-US Data Privacy Framework, or another lawful transfer mechanism.

SUB-APPENDIX D — DATA RETENTION POLICY

This Data Retention Policy sets out the periods for which BlogVault retains Personal Data processed under this DPA, in accordance with GDPR Article 5(1)(e) (storage limitation principle).

Retention Periods

Data Category	Retention Period	Reason
Website Content Backups (BlogVault servers in Germany)	Duration of Main Agreement	Core service — website backup and restoration
Backup Data	Up to 7 days after account deletion or termination	Backup recovery and operational safety
Security Scan Data	Duration of Main Agreement plus 7 days	Security monitoring and incident investigation
IP Address Logs (service-generated)	30 days	Security monitoring and incident investigation

Deletion Procedures

Upon expiration of the applicable retention period, or upon earlier receipt of a valid deletion request from the Data Controller:

1. Automated deletion: Data stored in systems with automated retention policies (analytics, IP logs, email logs) will be automatically purged.
2. Manual deletion: Data stored in manual systems will be deleted within thirty (30) days of the retention period expiry or deletion request.
3. Backup deletion: Data in backup systems will be securely isolated within three (3) days of the primary deletion and permanently purged at the next scheduled backup rotation (within 90 days).
4. Sub-Processor notification: The Data Processor will notify all relevant Sub-Processors to delete Controller Controlled Data in accordance with their own retention and deletion procedures.
5. Deletion confirmation: Upon request, the Data Processor will provide written confirmation of deletion where reasonably available.

Legal Holds

The above retention periods do not apply where Personal Data must be retained for longer periods to comply with applicable law, regulation, or legal proceedings (e.g., tax records, litigation holds, regulatory investigations). In such cases, data will be retained only for as long as legally required and will be processed solely for the purpose of the legal obligation.

ANNEX — STANDARD CONTRACTUAL CLAUSES (2021)

Incorporation of the Standard Contractual Clauses

For restricted transfers of Controller Controlled Data to countries that do not ensure an adequate level of data protection, the Parties hereby incorporate the **Standard Contractual Clauses** adopted by the European Commission in **Implementing Decision (EU) 2021/914 of 4 June 2021**, as amended or replaced from time to time.

The Parties agree that **Module Two (Controller to Processor)** of the SCCs shall apply to all transfers where the Data Controller is established in the EEA.

Option selections:

- Clause 7 (Docking Clause): Not selected
- Clause 11 (Redress): Not selected

The required Annexes to the SCCs are completed as set out below:

- Annex I (List of Parties, Description of Transfer, Competent Supervisory Authority) — see Annex I below
- Annex II (Technical and Organisational Security Measures) — see Sub-Appendix B of this DPA
- Annex III (List of Sub-Processors) — see Sub-Appendix C of this DPA

The complete official text of the 2021 Standard Contractual Clauses is available from the European Commission at:
https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

Competent Supervisory Authority

The competent supervisory authority for the purposes of the SCCs shall be determined in accordance with Article 56 of the GDPR, based on the Member State in which the Data Controller is established. Where the Data Controller is not established in the EEA, the supervisory authority shall be that of the Member State in which the Data Controller's representative is established, or as otherwise determined under the GDPR.

ANNEX I — SPECIFIC TERMS

I.A — List of Parties

Data Exporter (Data Controller):

Field	Details
Name	[_____]
Address	[_____]
Contact Person	[_____]
Activities	[Description of activities relevant to the transfer]
Role	Data Controller
Privacy Contact	[_____]

Data Importer (Data Processor):

Field	Details
Name	The Inactiv.com Media Solutions Private Limited
Address	22 Rustam Bagh Main Road, Bangalore – 560017, India
Contact Person	Akshat Choudhary
Activities	Website backup, security, performance, migration, and management services provided under the product names BlogVault, MalCare, WP Remote, Airlift, and Migrate Guru
Role	Data Processor
Privacy Contact	BlogVault Privacy Team, privacy@blogvault.net

I.B — Description of Transfer

Element	Description
Categories of Data Subjects	Data Controller, its End Users, and individuals whose personal data is included in website content processed through the Main Services
Categories of Personal Data	As described in Sub-Appendix A
Special Categories of Data	BlogVault does not intentionally collect special-category data; however, Controller Controlled Data may contain special-category data if included in the Data Controller's website content or backups. The Data Controller is responsible for ensuring lawful processing of any such data
Frequency of Transfer	Ongoing, as part of the Main Services
Retention Period	As specified in the Main Agreement and the Data Processor's data retention policy
Purpose of Transfer	Processing for the provision of the Main Services

I.C — Technical and Organisational Security Measures

As described in **Sub-Appendix B**.

[Supplementary measures for international transfers:]

Measure	Description
Encryption in Transit	Industry-standard encryption for all data transfers
Encryption at Rest	Strong encryption for stored data
Pseudonymisation	Not applicable
Split Processing	Not applicable

I.D — List of Sub-Processors

As described in **Sub-Appendix C**.

I.E — Contact Point for Data Subjects

For exercise of Data Subject rights under these Clauses:

BlogVault Privacy Team

Email: privacy@blogvault.net

[]

Email: []

UK INTERNATIONAL DATA TRANSFER ADDENDUM

Where the UK GDPR applies to a restricted transfer, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018 (the "**UK Addendum**"), is incorporated into this DPA and is completed using the information set out in Annex I, Sub-Appendix B, and Sub-Appendix C. The UK Addendum prevails over the SCCs to the extent of any conflict for UK restricted transfers.