DATA PROCESSING AGREEMENT

This Data Processing Agreement (“DPA”) forms part of the Terms of Service or Master Services Agreement (“Principal Agreement”) between:

Customer (“Controller”)

and

IconicBIM (“Processor”)

1. DEFINITIONS

“Applicable Data Protection Law” means all laws applicable to the Processing of Personal Data under the Agreement, including the GDPR and CCPA/CPRA.

“Personal Data”, “Processing”, “Controller”, “Processor”, and “Data Subject” shall have the meanings given under Applicable Data Protection Law.

“Subprocessor” means any third party engaged by Processor to Process Personal Data.

“Standard Contractual Clauses” or “SCCs” means the European Commission’s approved standard contractual clauses.

2. SCOPE AND ROLES

2.1 Controller determines the purposes and means of Processing.

2.2 Processor shall Process Personal Data:

solely on documented instructions from Controller (including this DPA and the Principal Agreement), and

only for the purpose of providing the services.

2.3 Details of Processing are set out in Appendix A.

2.4 Processor shall immediately inform Controller if, in its opinion, an instruction infringes Applicable Data Protection Law.

3. CONFIDENTIALITY

3.1 Processor shall ensure that all personnel authorized to Process Personal Data:

are subject to binding confidentiality obligations, and

receive appropriate data protection training.

3.2 These obligations survive termination of employment or engagement.

4. PROCESSOR OBLIGATIONS

Processor shall:

4.1 Process Personal Data only as instructed by Controller.

4.2 Not:

sell Personal Data

share Personal Data for cross-context behavioral advertising

retain, use, or disclose Personal Data outside the business purpose

4.3 Not combine Personal Data with data from other customers except as permitted by law.

4.4 Provide reasonable assistance to Controller to ensure compliance with:

security obligations

breach notification obligations

regulatory consultations

5. SECURITY MEASURES

5.1 Processor shall implement appropriate technical and organizational measures, taking into account:

the state of the art

costs of implementation

nature, scope, context, and purposes of Processing

risk to Data Subjects

5.2 Measures include those described in Appendix B, including:

encryption in transit and at rest

access controls (RBAC)

multi-factor authentication

logging and monitoring

regular security testing

6. SUBPROCESSORS

6.1 Controller provides general authorization for Processor to engage Subprocessors listed in Appendix C.

6.2 Processor shall:

impose data protection obligations equivalent to this DPA

remain fully liable for Subprocessors

6.3 Processor shall:

provide at least 15 days prior notice of new Subprocessors

notify via email or public URL

6.4 If Controller objects:

parties will work in good faith to resolve concerns

if unresolved, Controller may terminate affected services

7. DATA SUBJECT RIGHTS

7.1 Processor shall assist Controller in responding to Data Subject requests, including:

access

rectification

erasure

restriction

7.2 Processor shall promptly notify Controller of any request received directly and shall not respond unless instructed.

8. PERSONAL DATA BREACH

8.1 Processor shall notify Controller without undue delay and no later than 72 hours after becoming aware of a Personal Data breach.

8.2 Notification shall include:

nature of the breach

categories and approximate number of Data Subjects

likely consequences

measures taken or proposed

8.3 Processor shall take reasonable steps to mitigate the breach.

9. INTERNATIONAL DATA TRANSFERS

9.1 Processor shall not transfer Personal Data outside its originating jurisdiction unless compliant with Applicable Data Protection Law.

9.2 Where required, transfers shall be governed by:

the Standard Contractual Clauses, incorporated by reference

9.3 Processor shall:

implement appropriate safeguards

assist with transfer impact assessments where required

10. AUDITS AND COMPLIANCE

10.1 Processor shall make available information necessary to demonstrate compliance.

10.2 Controller may:

conduct audits no more than once annually

conduct additional audits in case of breach or regulatory requirement

10.3 Processor may satisfy audit obligations through:

independent third-party certifications (e.g., SOC 2, ISO 27001) as they become available

10.4 Audits shall:

be subject to reasonable notice

not unreasonably disrupt operations

be subject to confidentiality obligations

11. DATA RETENTION AND DELETION

11.1 Upon termination, Controller may request:

return of Personal Data, or

deletion of Personal Data

11.2 Processor shall comply within 90 days, unless legally required to retain data.

11.3 Processor shall provide certification of deletion upon request.

12. LIABILITY

12.1 Liability shall be subject to the limitations set out in the Principal Agreement, except where prohibited by law.

13. GOVERNING LAW

This DPA shall be governed by the law specified in the Principal Agreement.

14. ORDER OF PRECEDENCE

In the event of conflict, this DPA shall prevail over the Principal Agreement with respect to data protection matters.

15. CONTACT INFORMATION

Processor privacy contact:

privacy@iconicbim.com

(or designated contact)

APPENDIX A – PROCESSING DETAILS

Subject Matter: SaaS platform services

Duration: Term of the Principal Agreement

Nature of Processing: Collection, storage, analysis, transmission

Purpose: Provision and improvement of services

Types of Personal Data: Names, email addresses, IP addresses, usage data, computer names, profile names

Categories of Data Subjects: Customers, employees, end users

Data Locations: United States and other regions where subprocessors operate

APPENDIX B – SECURITY MEASURES

Encryption in transit (TLS 1.2+) and at rest

Role-based access controls (RBAC)

Multi-factor authentication (MFA)

Logging, monitoring, and alerting

Vulnerability scanning and penetration testing

Incident response procedures

Backup and disaster recovery

APPENDIX C – SUBPROCESSORS

Microsoft Azure (hosting)

Backendless (backend services)

Microsoft Outlook (communications)

Processor shall maintain an up-to-date list at a public URL or upon request, including locations of processing.