ICON Speed – Data Processing Addendum ("DPA")

Version 1.0 – August 2025

This Data Processing Addendum ("**Addendum**") forms part of, and is subject to, the ICON Speed Master Subscription Agreement or other written agreement (the "**Agreement**") between **Momensity LLC d/b/a ICON Speed** ("**ICON**", "**we**", "**us**") and the customer identified in the Order Form ("**Customer**", "**you**").

---

1 Definitions

Applicable Data Protection Law – all worldwide legislation and regulations applicable to the processing of Personal Data under the Agreement, including, where relevant, the EU/UK GDPR, HIPAA, CCPA/CPRA, and any state-level privacy statutes.
Personal Data – any data relating to an identified or identifiable natural person that is uploaded to, or generated by, the Services.
Services – ICON's hosted software platform marketed as "ICON Speed", including the KRAG analytics core, DFDM processing tier, and related professional services.
Other capitalised terms shall have the meaning set out in the Agreement or Applicable Data Protection Law.

---

2 Roles & Scope

- ICON acts as **Processor** (or "Business Associate" under HIPAA) with respect to Personal Data that Customer submits to the Services.
- Customer acts as **Controller** (or "Covered Entity") and determines the purposes and means of processing.
- The subject-matter, nature, and purpose of processing are: **secure storage, transformation, and analysis of business assessment data, marketing metrics, and related datasets in order to surface insights and automate business workflows**.
- Data subjects may include Customer's employees, contractors, clients, and end-customers.
- Categories of Personal Data typically processed: contact information, behavioural metrics, transaction details, and free-form assessment responses.
- **Sensitive Data** (e.g. health information subject to HIPAA): processed only where explicitly authorised by Customer and subject to Section 7 (HIPAA).

---

3 Processor Obligations

1. **Instructions** – ICON shall process Personal Data only on documented instructions from Customer, unless required by law.
2. **Confidentiality** – ICON ensures that personnel authorised to process Personal Data are bound by confidentiality obligations.

3. **Security** – ICON implements the technical and organisational measures summarised in *Annex 2 – Security Measures* (including ISO 27001 controls, AWS GovCloud isolation, encryption at rest & in transit, least-privilege IAM, continuous monitoring).
4. **Sub-processors** – ICON may engage the sub-processors listed in *Annex 3 – Authorised Sub-processors*. ICON shall impose data-protection terms that provide at least the same level of protection. Customer provides general authorisation to such sub-processing.
5. **Data Subject Rights** – ICON shall assist Customer, via appropriate technical and organisational measures, in fulfilling requests to exercise rights of access, rectification, erasure, restriction, portability, and objection.
6. **Data Breach Notification** – ICON will notify Customer without undue delay (and within 72 hours for GDPR-covered data, or without unreasonable delay for HIPAA) after becoming aware of a Personal Data Breach affecting Customer Data.
7. **Records & Audits** – ICON shall maintain records of processing and make them available to supervisory authorities. Upon 30 days' advance written notice, ICON will permit Customer (or independent auditor) to audit ICON's compliance no more than once per 12-month period.

---

4 International Data Transfers

ICON stores Customer Data in the region specified in the Order Form. For cross-border transfers from the EEA/UK to the United States, the parties agree that the EU/UK Standard Contractual Clauses (Module 2 – Controller → Processor) are incorporated by reference, with ICON Speed LLC as "data importer" and Customer as "data exporter".

---

5 HIPAA-Specific Terms

Where Customer is a Covered Entity or Business Associate under HIPAA and transmits Protected Health Information ("**PHI**") into the Services, the HIPAA Business Associate Agreement ("**BAA**") in *Annex 1* shall apply and is hereby incorporated. ICON's GovCloud deployment is designed for HIPAA, FIPS-140-3, and CJIS compliance.

---

6 Return & Deletion

Upon termination of the Agreement, ICON will (at Customer's choice) return all Personal Data or securely delete it from active systems within 30 days, save for any data required to be retained under law or for legitimate backup (deleted within 90 days by automated lifecycle policies).

---

7 Liability & Indemnities

Liability under this Addendum is subject to the limitations and exclusions set forth in the Agreement. Customer shall indemnify ICON against claims arising from Customer's unlawful instructions or misuse of the Services.

8 Order of Precedence

In the event of conflict, this Addendum (and its Annexes) shall prevail over the Agreement to the extent of the conflict, except where explicitly stated otherwise.

9 Signatures

By executing the Order Form that references the Agreement, the parties are deemed to have signed this Addendum.

Annex 1 – HIPAA Business Associate Agreement

(Text redacted for brevity – will be supplied upon request or automatically attached when Customer selects HIPAA option in Order Form.)

Annex 2 – Technical & Organisational Security Measures

Infrastructure – AWS GovCloud (us-gov-east-1) with multi-AZ VPC, private subnets, and AWS WAF/Shield.
Encryption – AES-256 at rest (S3 SSE-KMS, RDS KMS), TLS 1.2+ in transit, FIPS-validated libraries.
Access Control – SSO (SAML 2.0/OIDC), MFA enforced, least-privilege IAM roles, customer-scoped KMS keys.
Monitoring & Logging – AWS CloudTrail, GuardDuty, centralized SIEM, 90-day log retention.
Business Continuity – automated snapshots, cross-region backups, RTO < 1 hour, RPO < 15 minutes.
Pen-Testing & Certification – annual CREST penetration test, SOC 2 Type II, ISO 27001, HIPAA via Vanta.

Annex 3 – Authorised Sub-processors

Provider	Purpose	Location	Safeguards
Amazon Web Services (AWS)	IaaS hosting, storage, networking	USA – GovCloud	SOC 2, ISO 27001, HIPAA, FIPS 140-3
Vanta Inc.	Continuous compliance monitoring	USA	SOC 2
SendGrid (Twilio)	Transactional e-mail for notifications	USA	SOC 2, ISO 27001, TLS
None others at present			

(ICON will notify Customer at least 30 days before adding or replacing a sub-processor.)

End of Addendum