Data Processing Addendum

The data processing addendum incorporated by reference into Actionable Science, Inc. service agreements.

Version 3.0 · Effective 10 November 2026

Actionable Science Inc (ASC) Data Processing Addendum

This Data Processing Addendum ("DPA" or "Addendum") is incorporated by reference into any services agreement between you and Actionable Science Inc ("ASC") for the provision of cloud services (the "Agreement") pursuant to which ASC processes Personal Data on your behalf.

For the purposes of this DPA, "Controller" means the entity entering into the Agreement that determines the purposes and means of Processing Personal Data, including both the individual using the services and any legal entity on whose behalf such individual acts.

This DPA sets out the terms that apply when ASC, acting as a Processor, processes Personal Data on behalf of the Controller in connection with the services provided under the Agreement. This DPA ensures compliance with applicable Data Protection Laws, including the UK GDPR, EU GDPR, and other relevant legislation.

ASC and the Controller are each referred to herein as a "Party" and collectively as the "Parties".

1. SCHEDULES

This DPA is supplemented by the following Schedules, which are incorporated by reference and attached as applicable:

1.1. Schedule 1 (EU Standard Contractual Clauses) contains the standard contractual clauses adopted pursuant to Commission Implementing Decision (EU) 2021/914 for transfers of Personal Data to third countries. The Annexes to Schedule 1 set out the details of Processing (including the Parties, categories of Personal Data and Data Subjects, purposes of Processing, security measures, and Sub-processors). Schedule 1 applies where Clause 12.2, 12.3 or 12.3A of this DPA applies.

1.2. Schedule 2 (UK International Data Transfer Addendum) contains the International Data Transfer Addendum issued by the UK Information Commissioner under Section 119A(1) of the UK Data Protection Act 2018. Schedule 2 modifies Schedule 1 for transfers subject to UK Data Protection Laws. Schedule 2 applies where Clause 12.3 of this DPA applies.

1.3. The current published versions of the instruments incorporated in Schedule 1 and Schedule 2 are available at the following locations, or at such other URLs as ASC may provide from time to time:

Schedule	**Instrument**	**URL**
Schedule 1	EU Standard Contractual Clauses	Click here to view EUSCC

Schedule	Instrument	URL
Schedule 2	UK International Data Transfer Addendum	Click here to view UKIDT

2. DEFINITIONS

2.1. In this DPA, unless the context requires otherwise:

2.1.1. "Affiliate" means an entity that owns or controls, is owned or controlled by, or is under common control or ownership with either ASC or Controller (as applicable), where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract, or otherwise.

2.1.2. "Controller", "Data Subject", "Personal Data", "Personal Data Breach", "Process" (and its derivatives), "Processor", and "Special Categories of Personal Data" have the meanings given to them in the applicable Data Protection Laws.

2.1.3. "Data Protection Laws" means all applicable laws and regulations relating to the processing of Personal Data and privacy, including: (a) the UK GDPR and the UK Data Protection Act 2018; (b) Regulation (EU) 2016/679 (the EU General Data Protection Regulation); (c) the Indian Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, and (d) the Digital Personal Data Protection Act, 2023 and rules framed thereunder (together, the "DPDP Act"), as and when notified; and (e) any other applicable national implementing laws, regulations, and secondary legislation, in each case as amended, replaced, or superseded from time to time.

2.1.4. "Data Subject Request" means a request from a Data Subject to exercise any right under applicable Data Protection Laws.

2.1.5. "EEA" means the European Economic Area.

2.1.6. "EU GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

2.1.7. "EU SCCs" means the standard contractual clauses pursuant to Commission Implementing Decision (EU) 2021/914, as set out in Schedule 1.

2.1.8. "Restricted Transfer" means: (a) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to a country outside the United Kingdom not subject to adequacy regulations pursuant to Section 17A of the Data Protection Act 2018; or (b) where the EU GDPR applies, a transfer of Personal Data from the EEA to a country outside the EEA not subject to an adequacy decision pursuant to Article 45 of the EU GDPR; or (c) where the DPDP Act applies, a transfer of Personal Data from India to a country or territory outside India that the Central Government has restricted by notification under Section 16 of the DPDP Act.

2.1.9. "Sub-processor" means any third party engaged by ASC to Process Personal Data on behalf of the Controller.

2.1.10. "Supervisory Authority" means: (a) in relation to the UK GDPR, the Information Commissioner's Office; (b) in relation to the EU GDPR, the independent public authority established by an EU Member State pursuant to Article 51; and (c) in relation to the DPDP Act, the Data Protection Board of India.

2.1.11. "UK GDPR" means the EU GDPR as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of Section 3 of the European Union (Withdrawal) Act 2018, as amended.

2.1.12. "UK IDTA" means the International Data Transfer Addendum issued by the Information Commissioner under Section 119A(1) of the UK Data Protection Act 2018, as set out in Schedule 2.

2.2. The terms "include", "includes", and "including" are deemed to be followed by "without limitation".

2.3. References to clauses, paragraphs, and schedules are to the clauses, paragraphs, and schedules of this DPA unless otherwise specified

3. SCOPE AND ROLES

3.1. This DPA applies to the Processing of Personal Data by ASC on behalf of the Controller in connection with the services provided under the Agreement.

3.2. The Parties acknowledge that for the purposes of Data Protection Laws, the Controller is the controller and ASC is the processor in respect of the Personal Data Processed under this DPA.

3.3. The details of the Processing, including the categories of Personal Data, categories of Data Subjects, nature and purpose of Processing, and duration of Processing, are set out in the Annexes to Schedule 1 (which describe the Rezolve.ai platform) and, for Rapport, Annex R, which supplements Annex I to Schedule 1 where the Controller has subscribed to Rapport.

3.4. Each Party shall comply with its respective obligations under applicable Data Protection Law

4. CONTROLLER OBLIGATIONS

4.1. The Controller warrants, represents, and undertakes that:

4.1.1. it has complied and shall continue to comply with all applicable Data Protection Laws in respect of the collection, use, and transfer of Personal Data to ASC.

4.1.2. it has provided and shall continue to provide all necessary notices to, and has obtained and shall continue to obtain all necessary consents or authorisations from, Data Subjects to permit ASC to Process Personal Data for the purposes described in the Agreement and Schedule 1;

4.1.3. all Personal Data provided to ASC is accurate, complete, and lawfully obtained;

4.1.4. it shall not disclose any Special Categories of Personal Data to ASC unless expressly agreed in writing. For Services that access Controller devices (such as Rapport), the Parties

acknowledge that Special Categories of Personal Data may be processed incidentally where they are present in files, command output or other content that the Controller's authorised users choose to access through the Service. The Controller is responsible for configuring and using those features in line with Data Protection Laws;

4.1.5. it is responsible for the security of Personal Data in transmission from the Controller to ASC; and

4.1.6. the Processing instructions given to ASC are lawful and do not infringe any applicable Data Protection Laws.

4.2. The Controller shall indemnify, defend, and hold harmless ASC and its Affiliates, and their respective officers, directors, employees, and agents, from and against any claims, damages, losses, liabilities, costs, and expenses (including reasonable legal fees) arising out of or in connection with:

4.2.1. any breach by the Controller of its obligations, warranties, or representations under this DPA;

4.2.2. any Processing of Personal Data by ASC in accordance with the Controller's documented instructions where such instructions or the underlying Processing is subsequently found to infringe applicable Data Protection Laws through no fault of ASC; or

4.2.3. any claim by a Data Subject, Supervisory Authority, or third party arising from the Controller's failure to comply with its obligations under applicable Data Protection Laws, including failure to provide required notices or obtain required consents.

5. PROCESSING INSTRUCTIONS

5.1. ASC shall Process Personal Data only on documented instructions from the Controller, including with respect to transfers of Personal Data to a third country or international organization, unless required to do so by applicable law, in which case ASC shall inform the Controller of that legal requirement before Processing unless prohibited by law.

5.2. ASC shall immediately inform the Controller if, in ASC's opinion, an instruction from the Controller infringes applicable Data Protection Laws.

5.3. ASC shall Process Personal Data only for the purposes set out in the Agreement and Schedule 1, and in accordance with this DPA.

5.4. ASC shall not Process Personal Data for longer than is necessary to carry out the purposes set out in the Agreement and Schedule 1, except where required by applicable law.

5.5. ASC's Processing of Personal Data shall be conducted in accordance with ASC's internal data protection policies and procedures, which establish governance frameworks for the lawful processing of Personal Data, the handling of Data Subject Requests, and the retention and secure deletion of Personal Data. ASC shall maintain and regularly review such policies to ensure continued alignment with applicable Data Protection Laws.

6. CONFIDENTIALITY

6.1. ASC shall ensure that persons authorized to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.2. ASC shall ensure that access to Personal Data is limited to those personnel who need access to fulfill ASC's obligations under this DPA and the Agreement.

7. SECURITY OF PROCESSING

7.1. ASC shall implement and maintain technical and organizational measures that ASC reasonably determines to be appropriate to protect Personal Data against unauthorized or unlawful Processing and against accidental loss, destruction, damage, theft, alteration, or disclosure. These measures shall be appropriate to the harm that might result from any unauthorized or unlawful Processing, accidental loss, destruction, or damage, having regard to the state of the art, the costs of implementation, and the nature of the Personal Data.

7.2. The security measures implemented by ASC are described in Annex II to Schedule 1 and include encryption of Personal Data in transit and at rest, access controls, data loss prevention tools, backup and recovery procedures, and incident response capabilities.

7.3. ASC's security measures include:

7.3.1. encryption of Personal Data in transit using TLS 1.2 or higher and at rest using AES-256 or equivalent industry-standard encryption;

7.3.2. secure encryption key management procedures, including key generation, storage, rotation, and revocation controls;

7.3.3. data loss prevention controls designed to detect and prevent unauthorized transmission or exfiltration of Personal Data;

7.3.4. access controls based on the principle of least privilege, ensuring that personnel access only the Personal Data necessary for their role; and

7.3.5. logging and monitoring of access to systems containing Personal Data.

7.4. ASC shall periodically reassess the appropriateness of the security measures implemented, taking into account changes in the state of the art, evolving threats, and changes to the nature, scope, context, and purposes of Processing.

7.5. ASC shall regularly test, assess, and evaluate the effectiveness of the technical and organizational measures implemented to ensure the security of Processing.

7.6. ASC may update or replace the security measures described in this Clause 7 from time to time, provided that any such update or replacement does not materially diminish the overall level of protection afforded to Personal Data.

8. SUB-PROCESSORS

8.1. ASC may engage Sub-processors to Process Personal Data on behalf of the Controller, subject to the requirements of this Clause 8.

8.2. The Sub-processors authorized as at the date of this DPA are listed in the Sub-processor List at https://www.rezolve.ai/legal/subprocessors, which forms Annex III to Schedule 1 and shows the Services for which each Sub-processor is used.

8.3. ASC shall inform the Controller in writing by email to the Controller's notice contact, of any intended changes concerning the addition or replacement of Sub-processors at least thirty (30) days in advance, giving the Controller sufficient opportunity to object prior to engagement. ASC shall provide the Controller with such information as the Controller may reasonably require to exercise its right to object

8.4. If the Controller objects to a new Sub-processor on reasonable grounds relating to data protection, the Parties shall discuss and seek to resolve the matter in good faith. If unable to reach a resolution within thirty (30) days of the Controller's initial objection, the Controller may, as its sole and exclusive remedy, terminate the affected services under the Agreement by providing written notice to ASC. Such termination shall not entitle the Controller to any refund of prepaid fees, and the Controller shall remain liable for all fees accrued through the effective date of termination.

8.5. ASC shall conduct due diligence prior to engaging any Sub-processor to ensure the Sub-processor can provide the level of protection for Personal Data required by this DPA. Such due diligence shall include:

8.5.1. assessment of the Sub-processor's technical and organizational security measures;

8.5.2. evaluation of the Sub-processor's data protection policies and practices;

8.5.3. verification that the Sub-processor can meet the requirements of applicable Data Protection Laws; and

8.5.4. where applicable, review of relevant certifications, audit reports, or attestations held by the Sub-processor.

8.6. ASC shall ensure that any Sub-processor engagement is governed by a written contract that:

8.6.1. imposes data protection obligations no less protective than those imposed on ASC under this DPA;

8.6.2. requires the Sub-processor to Process Personal Data only on documented instructions from ASC;

8.6.3. requires the Sub-processor to ensure that persons authorized to Process Personal Data are subject to confidentiality obligations;

8.6.4. requires the Sub-processor to implement appropriate technical and organizational security measures;

8.6.5. requires the Sub-processor to assist ASC in responding to Data Subject Requests and Personal Data Breaches; and

8.6.6. requires the Sub-processor to delete or return all Personal Data upon termination of the sub-processing arrangement.

8.7. ASC shall remain liable to the Controller for the performance of each Sub-processor's obligations to the extent ASC would be liable for its own performance of such obligations under this DPA and the Agreement.

9. DATA SUBJECT RIGHTS

9.1. Taking into account the nature of the Processing, ASC shall assist the Controller by appropriate technical and organizational measures for the fulfilment of the Controller's obligations to respond to Data Subject Requests, subject to provisions of this Clause 9.

9.2. If ASC receives a request directly from a Data Subject seeking to exercise rights under applicable Data Protection Laws, ASC shall forward the request to the Controller without undue delay. ASC shall not respond directly to any such request except on the documented instructions of the Controller or as required by applicable law.

9.3. For the avoidance of doubt:

9.3.1. ASC's obligation under Clause 9.2 is limited to forwarding the request to the Controller and does not extend to assessing the validity, merit, or legal basis of the request;

9.3.2. the Controller is solely responsible for verifying the identity of the Data Subject and determining the appropriate response to each Data Subject Request;

9.3.3. ASC's assistance with Data Subject Requests is limited to measures that are technically feasible through the platform's existing functionality, and ASC shall not be required to develop new features, modify the platform, or undertake manual processing that is not supported by the platform's standard administrative functions;

9.3.4. ASC shall not be liable for any delay, failure, or deficiency in responding to a Data Subject Request to the extent caused by the Controller's failure to provide timely instructions, the Controller's decision regarding the response, or the Controller's failure to use the platform's available functionality; and

9.3.5. the Controller shall indemnify ASC against any claims, damages, or regulatory penalties arising from ASC's compliance with the Controller's documented instructions regarding a Data Subject Request, except to the extent such claims arise from ASC's failure to comply with those instructions.

9.4. ASC maintains a Data Subject Request register that records, for each request:

9.4.1. the date of receipt and the nature of the request;

9.4.2. the identity of the Data Subject (to the extent known);

9.4.3. the actions taken in response to the request; and

9.4.4. the date of completion or closure of the request.

9.4.5.The Controller may access, export, and manage Personal Data through the platform's administrative interface, including functionality to respond to access, rectification, erasure, and portability requests without requiring ASC's direct involvement.

9.5. Subject to Clauses 9.3 and 9.6, ASC shall provide such assistance as the Controller reasonably requests in relation to Data Subject Requests, limited to providing information and documentation within ASC's possession or control that is necessary for the Controller to respond within required timeframes.

9.6. ASC may charge reasonable fees for assistance with Data Subject Requests to the extent such assistance requires resources beyond ASC's standard platform functionality or exceeds five (5) Data Subject Requests in any calendar month.

10. PERSONAL DATA BREACHES

10.1. ASC shall notify the Controller without undue delay after becoming aware of a Personal Data Breach affecting Personal Data Processed under this DPA. ASC will notify the Controller without undue delay and in any event within 48 (forty-eight) hours of becoming aware, and will provide further information in phases as it becomes available.

10.2. ASC has established a dedicated incident response team responsible for managing Personal Data Breach incidents. The incident response team includes senior personnel from relevant functions, including executive leadership, information security, information technology, and data protection. The incident response team is responsible for:

10.2.1. assessing the nature and scope of any suspected or confirmed Personal Data Breach;

10.2.2. coordinating containment and remediation measures;

10.2.3. preparing notifications to Controllers and, where required, to Supervisory Authorities and Data Subjects; and

10.2.4. conducting post-incident review to identify and implement measures to prevent recurrence.

10.3. The notification to the Controller shall include, to the extent then known:

10.3.1. a description of the nature of the Personal Data Breach, including where possible the categories and approximate number of Data Subjects and Personal Data records concerned;

10.3.2. the name and contact details of a contact point where more information can be obtained;

10.3.3. a description of the likely consequences of the Personal Data Breach; and

10.3.4. a description of the measures taken or proposed to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

10.4. Where it is not possible to provide all information at the same time, ASC shall provide the information in phases without undue further delay.

10.5. ASC shall cooperate with the Controller and provide reasonable assistance in relation to any notifications to Supervisory Authorities or Data Subjects required following a Personal Data Breach. ASC may charge reasonable fees for assistance provided under this Clause 10.5 to the extent such assistance requires more than thirty (30) hours of ASC personnel time, except where the Personal Data Breach was caused solely by ASC's breach of its obligations under this DPA.

10.6. ASC maintains a breach register documenting all Personal Data Breaches, regardless of whether notification to Supervisory Authorities is required. The breach register records:

10.6.1. the date and time of discovery of the Personal Data Breach;

10.6.2. a description of the nature of the breach, including the categories and approximate number of Data Subjects and Personal Data records affected;

10.6.3. the likely consequences of the breach;

10.6.4. the measures taken to address the breach and mitigate its effects; and

10.6.5. the details of any notifications made to Controllers, Supervisory Authorities, or Data Subjects.

10.7. ASC shall make relevant extracts from the breach register available to the Controller upon reasonable request in connection with any Personal Data Breach affecting the Controller's Personal Data.

10.8. Any notification made by ASC under this Clause 10 shall not be construed as an acknowledgement of fault or liability by ASC with respect to the Personal Data Breach.

11. AUDIT RIGHTS

11.1. ASC shall make available to the Controller all information necessary to demonstrate compliance with the obligations set out in this DPA and applicable Data Protection Laws.

11.2. ASC shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller, subject to the following conditions:

11.2.1. the Controller shall provide ASC with at least thirty (30) days' advance written notice of any proposed audit, except where such audit is required due to a Personal Data Breach or a request or investigation by a Supervisory Authority, in which case reasonable notice shall be provided;

11.2.2. the scope of any audit shall be agreed in advance between the Parties and shall be limited to matters reasonably necessary to verify ASC's compliance with this DPA;

11.2.3. audits shall be conducted during normal business hours and in a manner that minimizes disruption to ASC's business operations;

11.2.4. the Controller and any auditor mandated by the Controller shall be bound by confidentiality obligations no less protective than those contained in the Agreement;

11.2.5. the Controller shall bear its own costs of any audit, and ASC may charge reasonable fees for time spent by ASC personnel in connection with an audit that thirty (30) business day per calendar year.

11.2.6. ASC may satisfy audit requests by providing the Controller with copies of relevant third-party audit reports, certifications, or attestations (such as ISO 27001 certification or SOC 2 Type II reports), subject to confidentiality obligations. If ASC provides such reports and they are no more than twelve (12) months old, the Controller's audit rights under this Clause 11 shall be deemed satisfied for the period covered by such reports, unless the Controller demonstrates in

writing that specific, material concerns exist which are not addressed by such reports and which require on-site verification.

11.3. The Controller shall be entitled to conduct no more than one (1) audit per calendar year under this Clause 11, unless a Personal Data Breach affecting Personal Data Processed under this DPA has occurred or a Supervisory Authority has requested or commenced an investigation concerning ASC's Processing of Personal Data under this DPA.

11.4. Any third-party auditor mandated by the Controller shall not be a direct competitor of ASC or an Affiliate of a direct competitor of ASC, and shall execute a confidentiality agreement with ASC prior to commencing any audit.

11.5. If an audit reveals material non-compliance by ASC with this DPA, ASC shall promptly take steps to remedy such non-compliance at ASC's expense.

11.6. The audit rights granted under this Clause 11 do not extend to the facilities or systems of ASC's Sub-processors. Where the Controller requires assurance regarding a Sub-processor's compliance, ASC shall use reasonable efforts to obtain and provide relevant certifications, audit reports, or attestations from the Sub-processor, subject to any confidentiality restrictions imposed by the Sub-processor.

12. INTERNATIONAL DATA TRANSFERS

12.1. ASC shall not transfer Personal Data to a country outside the EEA or the United Kingdom (as applicable) unless appropriate safeguards are in place in accordance with applicable Data Protection Laws.

12.2. EEA-Established Controllers: Where the Controller is established in the EEA and a Restricted Transfer occurs, the EU SCCs set out in Schedule 1 shall apply. For the purposes of the EU SCCs: (a) Module 2 (Controller to Processor) applies; (b) the Controller is the "data exporter" and ASC is the "data importer"; and (c) the Annexes shall be completed in accordance with Schedule 1.

12.3. UK-Established Controllers: Where the Controller is established in the United Kingdom and a Restricted Transfer occurs: (a) the EU SCCs set out in Schedule 1 shall apply, as modified by the UK IDTA set out in Schedule 2; and (b) the UK IDTA shall be completed in accordance with Schedule 2. The UK IDTA takes precedence over the EU SCCs to the extent of any conflict, except where the EU SCCs provide greater protection for Data Subjects.

12.3A. Swiss-Established Controllers: Where the Swiss Federal Act on Data Protection ("FADP") applies to a Restricted Transfer, the EU SCCs in Schedule 1 apply with the following adaptations: (a) references to the GDPR are read as references to the FADP; (b) the Swiss Federal Data Protection and Information Commissioner is the competent supervisory authority; (c) the term "Member State" includes Switzerland, so that data subjects in Switzerland may enforce their rights there; and (d) the governing law and forum under Clauses 17 and 18 of the EU SCCs remain as selected in Schedule 1.

12.4. Controllers in Non-Restricted Jurisdictions: Where the Controller is established in the United States or in a country benefiting from an adequacy decision under applicable Data

Protection Laws, Schedule 1 and Schedule 2 shall not apply to the extent that no Restricted Transfer occurs.

12.5. ASC's standard data hosting and processing locations, and the circumstances in which authorized personnel may remotely access Personal Data for the purposes of support, maintenance, and service delivery, are set out in Annex I to Schedule 1. To the extent such arrangements involve the transfer of Personal Data to a country outside the EEA or the United Kingdom (as applicable), such transfers constitute Restricted Transfers subject to the safeguards set out in this Clause 12.

12.6. Where Schedule 1 and/or Schedule 2 apply, the liability provisions in Clause 12 of the EU SCCs (and, where applicable, as modified by the UK IDTA) govern liability for breaches of those instruments, as further addressed in Clause 14 of this DPA.

13. DATA RETENTION AND DELETION

13.1. ASC shall Process Personal Data only for so long as necessary to fulfill the purposes set out in the Agreement and Schedule 1, and in accordance with the Controller's documented instructions.

13.2. Upon termination or expiry of the Agreement, the Controller shall notify ASC in writing within thirty (30) days whether it elects return of Personal Data under this Clause 13. If the Controller fails to make such election within this period, the Controller shall be deemed to have elected deletion under Clause 13.3.2.

13.3. Following the Controller's election (or deemed election), ASC shall:

13.3.1. where the Controller elects return, return all Personal Data to the Controller in a commonly used, machine-readable format within (90) days of such election, or within such other period as specified in the Agreement; or

13.3.2. where the Controller elects deletion or is deemed to have elected deletion, delete all Personal Data upon expiry of the retention period set out in Clause 13.4 and thereafter certify to the Controller in writing that deletion has been completed.

13.4. If the Agreement does not specify a post-termination retention period, ASC shall retain Personal Data for a period of one (1) year following termination or expiry of the Agreement to enable the Controller to retrieve its data and to address any post-termination queries or disputes. Upon expiry of the retention period, ASC shall securely delete all Personal Data using industry-standard deletion methods that render the data unrecoverable, unless a shorter retention period is agreed in writing between the Parties.

13.5. The Parties' respective responsibilities for Personal Data deletion are as follows:

13.5.1. During the term of the Agreement, the Controller is responsible for managing and deleting Personal Data of departed employees, former users, and other individuals whose data is no longer required, using the platform's administrative functions. ASC shall ensure that such administrative functions enable the Controller to delete Personal Data in a timely manner.

13.5.2. Upon termination or expiry of the Agreement, ASC is responsible for bulk deletion or return of all remaining Personal Data in accordance with the Controller's election under Clause 13.2 and Clause 13.3.

13.5.3. Where the Controller elects deletion, ASC shall provide written confirmation of deletion upon completion.

13.6. Notwithstanding the foregoing, ASC may retain Personal Data to the extent required by applicable law, provided that ASC ensures confidentiality and Processes it only as necessary for the purpose specified by law.

13.7. This Clause 13 shall survive termination or expiry of this DPA.

13.8. Rapport: Notwithstanding Clauses 13.2 to 13.4, for Personal Data processed in connection with Rapport ("Rapport Data"), during the term and subject to applicable law, the Controller sets retention periods for each category of Rapport Data in the Service, and Rapport deletes data automatically when those periods end. On termination, ASC will, at the Controller's written request made within 30 days, export the Controller's Rapport Data in a commonly used format and then delete it, completing the export and deletion within 30 (thirty) days of the request. If no request is made, ASC will delete the Controller's Rapport Data within 90 (ninety) days after termination. In each case, deletion is subject to applicable law requiring retention, and data held in backups is deleted in the ordinary backup cycle, subject to applicable law.

14. LIABILITY

14.1. Each Party's liability under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement, except as otherwise provided in this Clause 14.

14.2. Nothing in this DPA or the Agreement shall limit or exclude either Party's liability for:

14.2.1. fraud or fraudulent misrepresentation;

14.2.2. death or personal injury caused by negligence;

14.2.3. any other liability that cannot be limited or excluded by applicable law or the applicable transfer mechanism.

14.3. Neither Party shall be liable to the other for any indirect, incidental, special, consequential, punitive, or exemplary damages, including loss of profits, loss of revenue, loss of business, loss of data, or reputational harm, arising out of or in connection with this DPA, regardless of whether such damages were foreseeable or whether a Party was advised of the possibility of such damages.

14.4. Subject to Clauses 14.2 and 14.3, ASC's total aggregate liability under this DPA shall not exceed, and shall count towards, the maximum aggregate liability of ASC under Section 12.1(ii) of the Master Terms. This limitation shall apply regardless of the form of action, whether in contract, tort (including negligence), strict liability, or otherwise.

15. ASSISTANCE WITH COMPLIANCE

15.1. ASC shall assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the UK GDPR or EU GDPR (as applicable), taking into account the nature of Processing and the information available to ASC. This includes:

15.1.1. implementing appropriate security measures (Article 32);

15.1.2. notifying Personal Data Breaches to Supervisory Authorities and Data Subjects (Articles 33 and 34);

15.1.3. conducting data protection impact assessments where required (Article 35); and

15.1.4. prior consultation with Supervisory Authorities where required (Article 36).

15.2. ASC may charge reasonable fees for assistance provided under this Clause 15 to the extent such assistance requires more than thirty (30) hours of ASC personnel time per request.

15.3. ASC's assistance under Clause 15.1 shall be limited to providing information about ASC's Processing activities, security measures, and Sub-processors that is reasonably necessary for the Controller to conduct a data protection impact assessment or engage in prior consultation. ASC shall not be required to conduct data protection impact assessments on behalf of the Controller or to provide legal advice regarding the Controller's compliance obligations.

16. GENERAL PROVISIONS

16.1. This DPA comes into effect on the date on which the Agreement becomes effective and continues until the later of: (a) termination or expiry of the Agreement; or (b) ASC ceasing to Process Personal Data on behalf of the Controller.

16.2. In the event of conflict between this DPA and the Agreement, this DPA shall prevail to the extent of such conflict.

16.3. In the event of conflict between this DPA and the EU SCCs (Schedule 1) or the UK IDTA (Schedule 2), the EU SCCs or UK IDTA shall prevail.

16.4. Without prejudice to Clause 17 of the EU SCCs or corresponding provisions of the UK IDTA, the Parties submit to the jurisdiction stipulated in the Agreement for any disputes arising under this DPA.

16.5. This DPA is governed by the laws stipulated in the Agreement, without prejudice to Clause 17 of the EU SCCs or corresponding provisions of the UK IDTA.

16.6. Notices under this DPA shall be in writing and delivered in accordance with the Agreement.

16.7. If any provision of this DPA is held invalid, the remaining provisions shall not be affected.

16.8. No amendment of this DPA shall be valid unless in writing and signed by both Parties, except that ASC may update this DPA in accordance with Section 15.9of the Master Terms, provided updates do not reduce the protection of Personal Data except as required by law.

16.9. Nothing in this DPA confers rights on any person other than the Parties, except that Data Subjects may enforce the EU SCCs and UK IDTA as third-party beneficiaries to the extent provided therein.

ANNEX R – RAPPORT DATA PROCESSING ANNEX (applies only where the Controller has subscribed to Rapport)

1. Data subjects: the Controller's employees, contractors and other users of enrolled devices; the Controller's staff who use the Rapport console; employees who receive Rapport experience surveys.

2. Categories of personal data: device identifiers and hostname; assigned-user identifier (optional); operating system, hardware and software inventory; performance, reliability and network-quality measurements; process names (no arguments or paths); application crash and hang summaries; workforce activity aggregates (if enabled); content that authorised users access through support tools or that AI features process (including in automated investigations), including files, command output and AI assistant conversations; survey responses; console users' business email, name, role, authentication and activity records.

3. Special categories: not intended; may be processed incidentally (Clause 4.1.4).

4. Nature and purpose: monitoring device health and digital experience; diagnosing and fixing device issues; patch and software deployment; AI-assisted investigation; reporting; providing and securing the Service.

5. Duration: the term of the Agreement plus the periods in Clause 13.8.

6. Default retention (the Controller can change these in the Service): telemetry samples, command jobs and script runs – 90 days; experience events, app-usage categories, AI assistant sessions and rule runs – 180 days; device history, alerts, score history, activity, issues, device records and audit log – 365 days (audit log minimum 365 days); daily and hourly rollups, inventory fingerprints and operation measurements – 400 days; support cases – 180 days; account-recovery records – 180 days; email delivery records – 180 days, except unsubscribe and bounce records, which are kept while the account exists.

7. Location: United States. Remote support access from India by Actionable Science Labs Private Limited, limited to a specific support case and logged; no copies of Rapport Data are stored in India.

8. Sub-processors: as listed in the Sub-processor List for Rapport.

9. Transfers: Transfers from the EEA and Switzerland are covered by Schedule 1 (with Clause 12.3A), transfers from the UK by Schedule 2, and transfers from India are made in accordance with applicable Indian law.