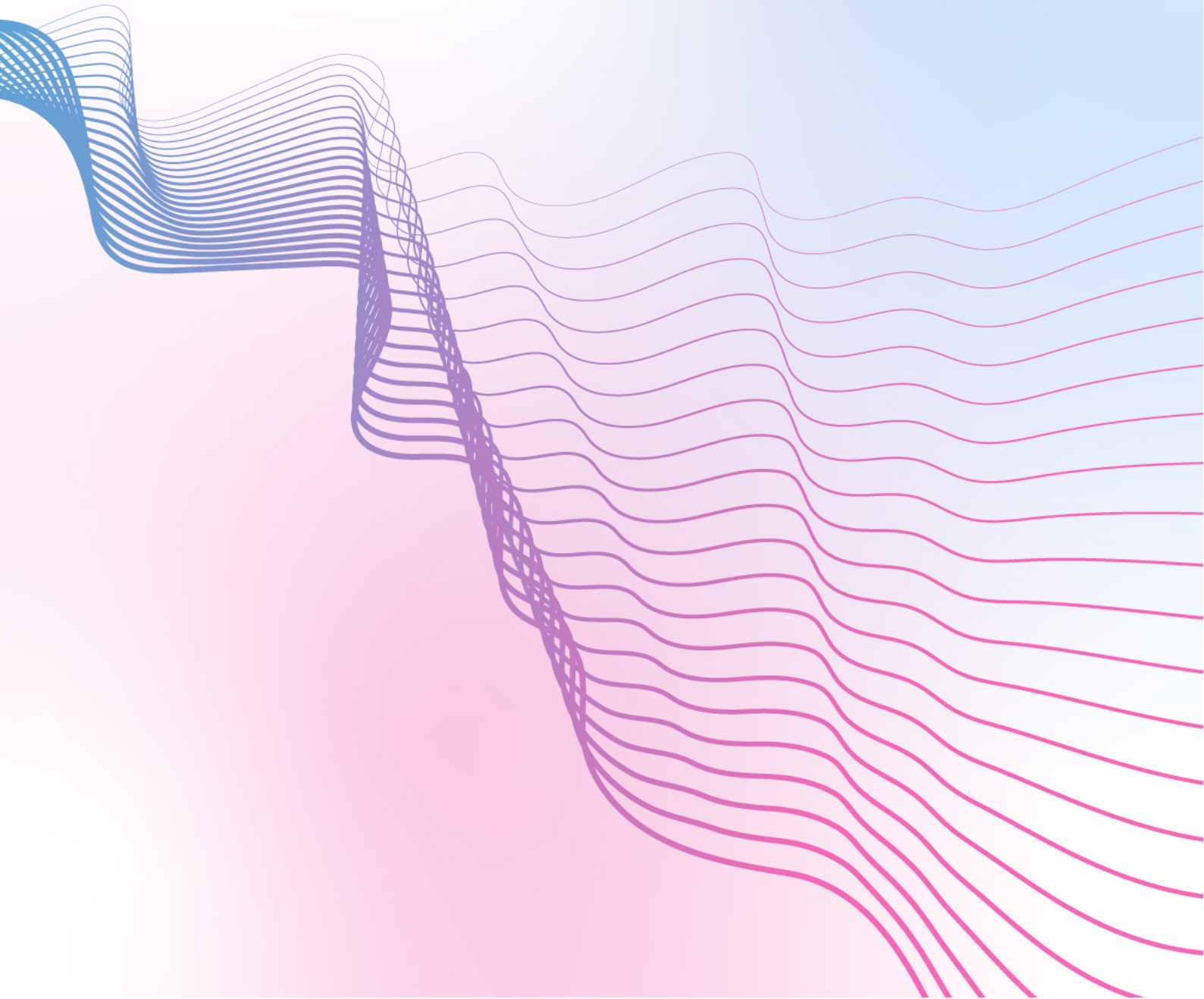
excelra

Data processing addendum

CONFIDENTIAL



This Data Processing Addendum ("**DPA**") is entered into on [date] (the "**DPA Effective Date**") between:

1. **[Excelra entity] along with its Affiliates,** as identified in Annex 3, Part A ("Excelra"); and
2. **[Counterparty legal name],** a [company] incorporated under the laws of [country], [registration number], having its registered office at [address] (the "**Counterparty**"),

(each a **"Party"** and together the **"Parties").**

Background

A. The Parties have entered into [name of agreement] dated [date] (the "**Agreement**"), under which one Party may process Personal Data on behalf of the other, and both Parties exchange business contact data during performance of services.

B. This DPA sets out the Parties' obligations under Data Protection Laws, including the EU GDPR, the UK GDPR, India's DPDPA and US State Privacy Laws.

C. This DPA forms part of the Agreement. If there is a conflict between this DPA and the Agreement on the processing of Personal Data, this DPA prevails. If there is a conflict between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses prevail.

1. Definitions

Terms used under one law include their equivalents under the others, as shown below. Other capitalised terms have the meaning given in the Agreement.

Term	Meaning	Equivalent terms
Affiliate	Any entity that controls, is controlled by or is under common control with a Party, "control" meaning ownership of more than 50% of the voting interests.	
Controller	The Party that determines the purposes and means of processing Personal Data.	Data Fiduciary (DPDPA); Business (CCPA)
Processor	The Party that processes Personal Data on behalf of the Controller.	Data Processor (DPDPA); Service Provider or Contractor (CCPA); Processor (other US State Privacy Laws)
Data Subject	The identified or identifiable natural person to whom Personal Data relates.	DataPrincipal (DPDPA); Consumer (US State Privacy Laws)
Personal Data	Any information relating to an identified or	Personal

	identifiable natural person that is processed under the Agreement.	Information (CCPA)
Sensitive Personal Data	Personal Data revealing racial or ethnic origin, political opinions, religious beliefs or trade union membership; genetic, biometric or health data; data on sex life or sexual orientation; precise geolocation; government identifiers; financial account data; and any other category designated as sensitive under Data Protection Laws.	Special Category Data (GDPR); Sensitive Personal Information (CCPA)
Processing	Any operation performed on Personal Data, whether or not automated, including collection, storage, use, disclosure, transfer, erasure and destruction.	—
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.	Personal Data Breach (DPDPA); Security Incident / Breach of Security (US State Privacy Laws)
Sub-processor	Any third party, engaged by the Processor to process Personal Data on behalf of the Controller.	—
Supervisory Authority	Any authority responsible for enforcing Data Protection Laws, including EU and UK data protection authorities, the Data Protection Board of India, the California Privacy Protection Agency and US State Attorneys General.	—
Data Protection Laws	All laws on privacy and the processing of Personal Data that apply to a Party.	—
EU GDPR	Regulation (EU) 2016/679.	—
UK GDPR	The EU GDPR as it forms part of UK law, with the UK Data Protection Act 2018.	—
DPDPA	India's Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025.	—
US State Privacy Laws	The California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 ("CCPA") and all other US state consumer privacy laws that apply to a Party.	—
HIPAA	The US Health Insurance Portability and Accountability Act of 1996 and its implementing regulations.	—

Standard Contractual Clauses (SCCs)	The clauses approved by the European Commission in Implementing Decision (EU) 2021/914.	—
UK Addendum	The International Data Transfer Addendum to the SCCs issued by the UK Information Commissioner.	—
Restricted Transfer	A transfer of Personal Data that would be prohibited under Data Protection Laws without an approved transfer mechanism.	—
Services	The services or products provided under the Agreement.	—

2. Scope and roles of the Parties

2.1 Module A – Business contact data (always applies). Each Party processes the other's business contact data (names, job titles, business email addresses and phone numbers of personnel) for communication, contract management, invoicing, compliance and relationship management **("Business Contact Data").** For this data, each Party is an independent Controller. Each Party shall:
(a) process it only for those purposes and in line with Data Protection Laws; (b) provide any privacy notice required to its own personnel; (c) protect it with appropriate security measures; (d) not sell it or use it for direct marketing to the other Party's personnel without a lawful basis; and (e) notify the other Party without undue delay of any Personal Data Breach affecting it. Clauses 3 to 11 do not apply to Business Contact Data.

2.2 Module B – Processing on behalf of the other Party (applies where selected in Annex 1). Where one Party (the "**Processor**") processes Personal Data on behalf of the other Party (the "**Controller**") to perform the Agreement, Clauses 3 to 12 apply. Annex 1 records which Party is the Controller and which is the Processor, and the details of the processing.

2.3 Excelra as Processor of customer data. Where Excelra receives Personal Data from a customer to perform Services, the customer is the Controller (or a Processor acting for its own Controller) and Excelra is the Processor (or Sub-processor). Excelra does not determine why that data is processed.

2.4 Counterparty as Processor of Excelra data. Where a vendor or service provider processes
Personal Data on Excelra's behalf, Excelra is the Controller and the vendor is the Processor.

2.5 Data minimisation. The Controller shall disclose to the Processor only the Personal Data needed for the Services. Unless agreed in Annex 1, the Controller shall not disclose Sensitive Personal Data or the Personal Data of children.

3. Obligations of the Processor

The Processor shall:

1. **Instructions:** process Personal Data only on the Controller's documented instructions, as set out in the Agreement, this DPA and Annex 1, including for international transfers, unless required otherwise by law, in which case it shall inform the Controller before processing unless the law prohibits this.
2. **Unlawful instructions:** promptly inform the Controller if, in its opinion, an instruction infringes Data Protection Laws.
3. **Purpose limitation:** not process Personal Data for its own purposes, and not sell, share for cross-context behavioural advertising, or otherwise commercially exploit it.
4. **No combining or de-identification:** not combine the Personal Data with data from other sources, or de-identify, aggregate or use it to train or improve products or AI models, unless the Controller agrees in writing or Data Protection Laws expressly permit it.
5. **Confidentiality:** ensure that personnel authorised to process Personal Data are bound by written confidentiality obligations, are trained in data protection, and access Personal Data only on a need-to-know basis.
6. **Security:** implement the measures in Clause 6 and Annex 2.
7. **Assistance:** taking into account the nature of the processing, assist the Controller with data subject requests (Clause 8), security, breach notification, data protection impact assessments and prior consultation with Supervisory Authorities.
8. **Records:** keep records of processing carried out on behalf of the Controller, as required by Article 30(2) GDPR and other Data Protection Laws.
9. **Inability to comply:** promptly notify the Controller if it can no longer meet its obligations under this DPA or Data Protection Laws. The Controller may then suspend the processing and, if the issue is not resolved within thirty (30) days, terminate the affected part of the Agreement.
10. **Authority requests:** unless prohibited by law, promptly notify the Controller of any request from a public authority to access Personal Data, challenge any request that is unlawful, and disclose only the minimum required.

4. Obligations of the Controller

The Controller shall:

3. **Lawful basis:** ensure it has a lawful basis under Data Protection Laws, including any consent required under the DPDPA or the GDPR, to collect the Personal Data and disclose it to the Processor.
4. **Notices:** provide all privacy notices required by Data Protection Laws to Data Subjects, including notice that Personal Data may be processed by service providers and transferred internationally.
5. **Lawful instructions:** ensure its instructions comply with Data Protection Laws.
6. **Accuracy and minimisation:** provide only Personal Data that is accurate and necessary for the Services, and inform the Processor in advance if it will disclose Sensitive Personal Data, Personal Data of children, or protected health information under HIPAA.
7. **Consent withdrawal:** inform the Processor promptly if a Data Subject withdraws consent or exercises a right that affects the processing.

5. Sub-processors

5.1 General authorisation. The Controller gives the Processor general written authorisation to engage the Sub-processors listed in Annex 3.

5.2 Changes. The Processor shall notify the Controller in writing at least thirty (30) days before adding or replacing a Sub-processor. The Controller may object on reasonable data protection grounds within that period. If the Parties cannot resolve the objection in good faith within a further thirty (30) days, either Party may terminate the affected part of the Services without penalty, and the Controller shall receive a pro-rata refund of any prepaid fees for that part.

5.3 Flow-down. Before a Sub-processor processes Personal Data, the Processor shall put in place a written agreement imposing data protection obligations no less protective than this DPA, including those required by Article 28(4) GDPR, Section 8 DPDPA and US State Privacy Laws.

5.4 Responsibility. The Processor remains fully responsible to the Controller for the performance of each Sub-processor's obligations.

5.5 Vendors of Excelra. Where Excelra is the Controller, the Counterparty shall not engage any Sub-processor other than those listed in Annex 3, Part B without Excelra's prior written approval.

6. Security of processing

6.1 Measures. The Processor shall implement and maintain appropriate technical and organizational measures to protect Personal Data against Personal Data Breaches, taking into account the state of the art, the cost of implementation, and the nature, scope, context and purposes of the processing and the risks to Data Subjects. These measures shall meet Article 32 GDPR, the reasonable security safeguards required by Section 8(5) DPDPA and the DPDP Rules, and the reasonable security requirements of US State Privacy Laws, and shall include at least those in Annex 2.

6.2 Standards. The Processor shall align its information security programme with a recognized standard such as ISO/IEC 27001, SOC 2 or the NIST Cybersecurity Framework, and review it at least annually.

6.3 Updates. The Processor may update its measures over time, provided the overall level of protection is not reduced.

7. Personal Data Breach

7.1 Notification. The Processor shall notify the Controller without undue delay, and in any event within forty-eight (48) hours, after becoming aware of a Personal Data Breach affecting the Controller's Personal Data. Notices to Excelra go to dpo@excelra.com and legaldesk@excelra.com; notices to the Counterparty go to the contact in Annex 1.

7.2 Content. The notice shall include, as far as then known, and shall be updated as more becomes known:

- The nature of the breach, including the categories and approximate number of Data Subjects and records concerned;
- The likely consequences;
- The measures taken or proposed to address the breach and reduce its effects; and a contact point for further information.

7.3 Response. The Processor shall promptly take reasonable steps to contain, investigate and remedy the breach, and shall cooperate with the Controller.

7.4 Regulatory notifications. The Controller is responsible for notifying Supervisory Authorities and Data Subjects, including within 72 hours under Article 33 GDPR, to the Data Protection Board of India and affected Data Principals under the DPDPA, and to individuals and regulators under US State Privacy Laws. The Processor shall not notify any third party about the breach without the Controller's prior written approval, unless the law requires it.

7.5 Other reporting. This Clause does not affect any separate legal duty of a Party to report incidents, such as reporting to CERT-In in India within six (6) hours.

7.6 No admission. A notification under this Clause is not an admission of fault or liability.

8. Data Subject rights

8.1 Forwarding. If the Processor receives a request from a Data Subject to exercise their rights, it shall forward it to the Controller within five (5) business days and shall not respond directly, except to confirm that the request has been passed on, unless the Controller authorises it.

8.2 Assistance. Taking into account the nature of the processing, the Processor shall assist the Controller, by appropriate technical and organisational measures, to respond to requests within the time limits set by Data Protection Laws, including requests to:

- Access or know (GDPR Article 15; DPDPA Section 11; CCPA);
- Correct, complete or update (GDPR Article 16; DPDPA Section 12; CCPA); erase or delete (GDPR Article 17; DPDPA Section 12; CCPA);
- Restrict or object to processing, or receive data in a portable format (GDPR Articles 18, 20 and 21);
- Withdraw consent or nominate another person to exercise rights (DPDPA Sections 6 and 14); and
- Opt out of sale, sharing, targeted advertising or profiling, or limit the use of sensitive data (CCPA and other US State Privacy Laws).

8.3 Grievances. Where the DPDPA applies, the Processor shall support the Controller's grievance redressal process by providing information within the time the Controller reasonably requests.

9. International data transfers

9.1 Locations. The Processor may process Personal Data in the countries listed in Annex 1 and Annex 3, including, where Excelra is the Processor, India, the United States, Belgium, the Netherlands and the United Kingdom. Any other location requires the Controller's prior written approval.

9.2 EU transfers. For any Restricted Transfer of Personal Data subject to the EU GDPR, the Parties enter into the SCCs, which are incorporated into this DPA by reference, with the module selected in Annex 4 and the information in Annexes 1 to 3 completing the SCC annexes.

9.3 UK transfers. For any Restricted Transfer subject to the UK GDPR, the SCCs apply as amended by the UK Addendum, and the tables of the UK Addendum are completed by Annexes 1 to 4.

9.4 Transfers from India. Transfers of Personal Data out of India shall comply with Section 16 DPDPA, any country restrictions notified by the Government of India, and any conditions in the DPDP Rules.

9.5 US restrictions. Neither Party shall give access to bulk US sensitive personal data, including genomic and health data, to a country of concern or covered person in breach of the US Department of Justice rule at 28 CFR Part 202.

9.6 Alternative mechanisms. If a transfer mechanism is invalidated or replaced, the Parties shall cooperate in good faith to put an alternative lawful mechanism in place promptly. The Processor shall carry out, or assist the Controller with, any transfer impact assessment required by Data Protection Laws.

10. Audits and information

10.1 Information. On request, the Processor shall make available the information reasonably needed to demonstrate compliance with this DPA, including current certifications (such as ISO/IEC 27001), audit reports, completed security questionnaires and policies.

10.2 Audits. If that information does not reasonably demonstrate compliance, or a Supervisory Authority requires it, the Controller (or an independent auditor bound by confidentiality, not a competitor of the Processor) may audit the Processor's compliance, subject to:

- At least thirty (30) days' written notice, unless following a Personal Data Breach;
- No more than once in any twelve (12) month period, unless following a Personal Data Breach or required by a Supervisory Authority;
- Audits during normal business hours, limited to the systems and records used to process the Controller's Personal Data, without access to other clients' data; and
- Each Party bearing its own costs, unless the audit reveals a material breach by the Processor.

10.3 Remediation. The Processor shall promptly remedy any material non-compliance identified.

11. Return and deletion

11.1 End of processing. Within thirty (30) days after the end of the Services, or earlier on the Controller's written request, the Processor shall, at the Controller's choice, return the Personal Data in a commonly used format or securely delete it, and shall confirm deletion in writing on request.

11.2 Purpose fulfilled. Where the DPDPA applies, the Processor shall also delete Personal Data when the Controller informs it that the purpose has been served or consent has been withdrawn.

11.3 Retention required by law. The Processor may keep Personal Data only to the extent required by law, and in routine back-ups until they are overwritten in the normal course. Retained data remains subject to this DPA and shall not be actively processed.

12. Jurisdiction-specific terms

12.1 EU GDPR and UK GDPR. Clauses 3 to 11 are intended to meet Article 28(3) GDPR. Where the GDPR applies, the Processor shall also cooperate with Supervisory Authorities on request, and shall appoint an EU or UK representative where Article 27 requires it.

12.2 India – DPDPA. Where the DPDPA applies:

- The Controller acts as the Data Fiduciary and remains responsible for compliance under Section 8(1), including for processing by the Processor;
- The Processor shall process Personal Data only under this valid contract, as required by Section 8(2);
- The Processor shall support the Controller in meeting its duties on notice, consent, accuracy, security, breach intimation, erasure and grievance redressal; and
- Where the Controller is a Significant Data Fiduciary, the Processor shall support any data protection impact assessment and audit required under Section 10.

12.3 United States – CCPA and other US State Privacy Laws. Where the Processor is a Service Provider, Contractor or Processor under US State Privacy Laws, it:

- Shall not sell or share Personal Data, or use it for targeted advertising;
- Shall not retain, use or disclose Personal Data outside the direct business relationship or for any purpose other than the business purposes in Annex 1;
- Shall not combine Personal Data with personal information from other sources, except as permitted by the CCPA regulations;
- Shall comply with US State Privacy Laws and provide the same level of privacy protection they require;
- Shall notify the Controller if it can no longer meet its obligations; and
- Grants the Controller the right to take reasonable steps to stop and remediate unauthorised use.

The Processor certifies that it understands and will comply with these restrictions. The Parties agree that no Personal Data is sold or shared between them for monetary or other valuable consideration.

12.4 HIPAA. If the Processor will create, receive, maintain or transmit protected health information on behalf of a covered entity or business associate, the Parties shall sign a separate Business Associate Agreement before that processing begins, and that agreement prevails for that information.

13. Liability, term and general

13.1 Liability. Each Party's liability under or in connection with this DPA is subject to the exclusions and limitations of liability in the Agreement, except to the extent such limitation is prohibited by Data Protection Laws or by the SCCs as between the Parties and Data Subjects. Each Party is responsible for administrative fines imposed on it for its own breach of Data Protection Laws.

13.2 Term. This DPA applies for as long as the Processor processes Personal Data on behalf of the Controller, and its confidentiality, security and deletion obligations survive until all Personal Data has been returned or deleted.

13.3 Changes in law. If a change in Data Protection Laws requires changes to this DPA, the Parties shall negotiate the necessary amendments in good faith.

13.4 Governing law. This DPA is governed by the governing law of the Agreement, and disputes are resolved under the Agreement's dispute resolution clause. However, the SCCs are governed by the law of the EU Member State in which the data exporter is established or, failing that, the laws of Belgium, with the courts of that Member State having jurisdiction; and the UK Addendum is governed by the laws of England and Wales.

13.5 Precedence. In case of conflict: (a) the SCCs and UK Addendum prevail; then (b) this DPA; then (c) the Agreement.

13.6 Severability and counterparts. If any provision is invalid, the rest remains in force. This DPA may be signed in counterparts and by electronic signature.

Signatures

	For [Excelra entity]	For [Counterparty]
Signature		
Name		
Title		
Date		

Annex 1 – Description of processing

Complete one Annex 1 per Agreement. Delete the options that do not apply.

Item	Details
Modules that apply	Module A (Business Contact Data) – always; Module B (processing on behalf) – [Yes / No]
Controller	[Counterparty / Excelra entity]
Processor	[Excelra entity / Counterparty]
Subject matter	Provision of the Services under the Agreement
Nature of processing	[Collection, storage, analysis, curation, transfer, deletion – as needed for the Services]
Purpose (business purpose)	Performing the Services described in the Agreement and statement(s) of work
Categories of Data Subjects	[Controller's employees and contractors; customers' or research study participants; vendors' personnel; other:
Categories of Personal Data	[Business contact details; professional details; user account and access-log data; pseudonymised research or clinical data; other:

Sensitive Personal Data	[None / Pseudonymised health or genetic data – specify safeguards in Annex 2]
Children's data	[None / specify, with verifiable parental consent where the DPDPA applies]
Frequency of transfer	[Continuous / one-off / as needed for each statement of work]
Duration	The term of the Agreement, plus the return and deletion period in Clause 11
Processing locations	[India, United States, Belgium, the Netherlands, United Kingdom, other:
Breach and privacy contacts	Excelra: dpo@excelra.com, legaldesk@excelra.com; Counterparty:

Annex 2 – Technical and organisational measures

The Processor maintains at least the following measures.

Area	Minimum measures
Governance	Written information security policy aligned with ISO/IEC 27001 or equivalent; named security and privacy owners; annual review
Access control	Unique user IDs; role-based, least-privilege access; multi-factor authentication for remote and privileged access; prompt removal of leavers' access
Encryption	Personal Data encrypted in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent)
Logging and monitoring	Logs of access to systems holding Personal Data, retained and reviewed for suspicious activity
Vulnerability management	Regular patching, vulnerability scanning and periodic penetration testing
Incident response	Documented incident response plan supporting the 48-hour notice in Clause 7
Backup and resilience	Encrypted backups with tested restoration; business continuity arrangements
Physical security	Controlled access to offices and data centres; reliance on certified cloud providers for hosting
Personnel	Confidentiality undertakings; background checks where lawful; annual data protection and security training
Sub-processors	Security due diligence before engagement and periodic review

Annex 3 – Excelra entities

Part A – Excelra group entities. Any of these entities may be the contracting Excelra entity, and each is an approved Sub-processor when another Excelra entity is the Processor.

Entity	Registered address	Country	Role in processing
Excelra Knowledge Solutions Private Limited	7th Floor, Wing B, NSL SEZ Arena, Plot No. 6, Survey No. 1, IDA Uppal, Hyderabad, Telangana 500039	India	Service delivery, data curation, analytics, support
Excelra Inc.	200 Middlesex Essex Turnpike, Suite 204, Iselin, New Jersey 08830	United States	Contracting, account management, service delivery
Excelra B.V.	Utrechtseweg 22B, 3544 NA Utrecht	Netherlands	Contracting, account management, service delivery
Excelra Belgium B.V. (including its UK operations)	Oktrooiplein 1, bus 201, 9000 Gent	Belgium (and United Kingdom)	Contracting, bioinformatics and data services, service delivery

Part B – Third-party Sub-processors.

Sub-processor	Location	Processing performed	Transfer mechanism
Cloud hosting and infrastructure providers	EU / US / India	Hosting, storage and backup	SCCs or adequacy decision, as applicable
Email, collaboration and productivity providers	EU / US	Communication and document sharing	SCCs or adequacy decision, as applicable
IT support and security service providers	EU / US / India	Technical support and security monitoring	SCCs or adequacy decision, as applicable

Annex 4 – Transfer mechanism details

Select the SCC module that matches the direction of the transfer.

Data flow	Exporter	Importer	SCC module
EU or UK customer (Controller) to Excelra India or Excelra Inc. (Processor)	Customer	Excelra entity	Module 2 (Controller to Processor)
EU or UK customer acting as Processor to Excelra India or Excelra Inc. (Sub-processor)	Customer	Excelra entity	Module 3 (Processor to Processor)
Excelra B.V. or Excelra Belgium B.V. (Processor) to Excelra India or Excelra Inc. (Sub-processor)	Excelra EU entity	Excelra entity	Module 3 (Processor to Processor)
Excelra EU entity (Controller) to a non-EEA vendor (Processor)	Excelra entity	Vendor	Module 2 (Controller to Processor)
Excelra EU entity (Processor) returning data to a non-EEA customer (Controller)	Excelra entity	Customer	Module 4 (Processor to Controller)

Options selected in the SCCs:

- Clause 7 (docking clause): applies.
- Clause 9 (sub-processors): Option 2, general written authorisation, with thirty (30) days' notice as in Clause 5.2.
- Clause 11 (redress): the optional independent dispute resolution wording does not apply.
- Clause 13 (supervision): the supervisory authority of the EU Member State in which the data exporter is established or, where Article 27 GDPR applies, of its EU representative.
- Clauses 17 and 18 (governing law and forum): the law and courts of the EU Member State in which the data exporter is established or, failing that, Belgium.
- **UK Addendum:** Table 1 is completed by the Parties' details in this DPA; Tables 2 and 3 by this Annex and Annexes 1 to 3; under Table 4, neither Party may end the UK Addendum when the ICO issues a revised version.

Where data means more

excelra

NEW JERSEY • BOSTON • LONDON • GHENT • UTRECHT • HYDERABAD

Connect with our experts: marketing@excelra.com

www.excelra.com

Disclaimer: This communication is intended solely for the recipient. The whole or any part of this communication should not be transmitted to any external entity or enterprise without the express written consent of Excelra. If you have received this communication by mistake, or if you are not the intended recipient, kindly delete it and immediately notify us in writing.