DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") forms an integral part of, and is subject to the AnalyticsVerse Services Terms of Service (the "**Services Agreement**") entered into by and between you, the customer (the "**Controller**") and AnalyticsVerse Solutions Pvt. Ltd. (the "**Processor**"). Capitalized terms not otherwise defined herein shall have the meaning given to them in the Services Agreement.

1. Definitions.

In addition to capitalized terms defined elsewhere in this DPA, the following terms shall have the meanings set forth below:

- "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "**Control**" for purposes of this definition means direct or indirect ownership or control of more than 50% of the voting interest in the subject entity.

- "**Applicable Law**" means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) ("GDPR"), laws implementing or supplementing the GDPR.

- "**Controller Personal Data**" means any Personal Data Processed by Processor on behalf of Controller pursuant to or in connection with the Services Agreement.

- **"Data Protection Laws"** means the data protection or privacy laws, rules, and regulations of the European Union, the European Economic Area and their member states under this Agreement

- **"Standard Contractual Clauses"** means the standard contractual clauses for Processors approved pursuant to the European Commission's decision (EU) 2021/914 of 4 June 2021, for the transfer of personal data to third countries in the form set out in Annexure 3; as amended, superseded or replaced from time to time in accordance with this Agreement.

- **"Sub-processors"** means any person or entity appointed by or on behalf of AnalyticsVerse to process Customer Personal Data on behalf of the Customer.

- The terms, **“Commission”, “Controller”, “Data Subject”, “Member State”, “Personal Data”, “Personal Data Breach”, “Processing” and “Supervisory Authority”** shall have the same meaning as in the GDPR.

2. Processing of Controller Personal Data.

- Processor shall Process Controller Personal Data on Controller’s behalf and at Controller’s instructions as specified in the Services Agreement and in this DPA, including without limitation with regard to transfers of Controller Personal Data to a third country or international organization. For the avoidance of doubt, Processor may use aggregated and/or anonymized data (“**Aggregate Data**”) for purpose of providing benchmarks and for improving the Services, as defined below, including the algorithms and models used by the Services. Any other Processing shall be permitted only in the event that such Processing is required by any Data Protection Laws to which the Processor is subject. In such event, Processor shall, unless prohibited by such Data Protection Laws on important grounds of public interest, inform Controller of that requirement before engaging in such Processing.
  - Controller instructs Processor (and authorizes Processor to instruct each Sub Processor) (i) to Process Controller Personal Data for the provision of the services, as detailed in the Services Agreement (“**Services**”) and as otherwise set forth in the Services Agreement and in this DPA, and/or as otherwise directed by Controller; and (ii) to transfer Controller Personal Data to any country or territory as reasonably necessary for the provision of the Services and in accordance with Applicable Law.

- Controller sets forth the details of the Processing of Controller Personal Data, as required by Article 28(3) of the GDPR are set forth in **Annexure 1** (*Details of Processing of Controller Personal Data*), attached hereto.

- To the extent that the Processor Processes Controller Personal Data in countries outside of the European Economic Area that do not provide an adequate level of data protection, as determined by the European Commission or other adequate authority as determined by the EU, the Standard Contractual Clauses shall apply in the form set out in Annexure 3, which are incorporated into and form a part of this Agreement.

3. Controller.

Controller represents and warrants that it has and shall maintain throughout the term of the Services Agreement and this DPA, all necessary rights to provide the Controller Personal Data to Processor for the Processing to be performed in relation to the Services and in accordance with the Services Agreement and this DPA. To the extent required by Data Protection Laws, Controller is responsible for obtaining any necessary Data Subject consents to the Processing, and for ensuring that a record of such consents is maintained throughout the term of the Services Agreement and this DPA and/or as otherwise required under Data Protection Laws.

4. Processor Employees.

Processor shall take reasonable steps to ensure that access to the Controller Personal Data is limited on a need to know and/or access basis and that all Processor employees receiving such access are subject to confidentiality undertakings or professional or statutory obligations of confidentiality in connection with their access to and use of Controller Personal Data.

5. Security.

Processor shall implement appropriate technical and organizational measures to ensure an appropriate level of security of the Controller Personal Data as set forth in the Binding Security Document attached hereto as Annexure 2. In assessing the appropriate level of security, Processor shall take into account the risks that are presented by the nature of the Processing and the information available to the Processor.

6. Personal Data Breach.

- Processor shall notify Controller without undue delay and, where feasible, not later than within 48 (forty-eight) hours upon Processor becoming aware of a Personal Data Breach affecting Controller Personal Data. In such an event, Processor shall provide Controller with reasonable and available information to assist Controller in meeting any obligations to inform Data Subjects or Supervisory Authorities of the Personal Data Breach as required under Applicable Law.

- At the written request of the Controller, Processor shall reasonably cooperate with Controller and take such commercially reasonable steps as are agreed by the parties or required under Applicable Law to assist in the investigation, mitigation and remediation of any Personal Data Breach.

7. Sub-Processors.

- Controller authorizes Processor to appoint (and permits each Sub Processor appointed in accordance with this Section 7 to appoint) Sub Processors in accordance with this Section 7.

- Processor may continue to use those Sub Processors already engaged by Processor as identified to Controller as of the date of this DPA.

- Processor may appoint new Sub Processors and shall give notice of any such appointment to Controller on subscription. To receive such notifications, please subscribe by sending an email to privacy@analyticsverse.com of your request to receive notifications of any new Sub-processors used to Process Personal Data. If, within seven (7) days of such notification, Controller notifies Processor in writing of any reasonable objections to the proposed appointment, Processor shall not appoint the proposed Sub Processor for the Processing of Controller Personal Data until reasonable steps have been taken to address the objections raised by Controller and Controller has been provided with a reasonable written explanation of the steps taken. Where such steps are not sufficient to relieve Controller's reasonable objections, each of Controller or Processor may, by written notice to the other party and with immediate effect, terminate the Services Agreement to the extent that it relates to the Services requiring the use of the proposed Sub Processor. In such event, the terminating party shall not bear any liability for such termination.

- With respect to each new Sub Processor, Processor shall:
  - Prior to the Processing of Controller Personal Data by Sub Processor, take reasonable steps (for instance by way of reviewing privacy policies as appropriate) to ensure that Sub Processor is committed and able to provide the level of protection for Controller Personal Data required by this DPA; and

    - ensure that the arrangement between the Processor and the Sub Processor is governed by a written contract, including terms that offer a materially similar level of protection for Controller Personal Data as those set out in this DPA and meet the requirements of Applicable Law.

  - Processor shall remain fully liable to the Controller for the performance of any Sub Processor's obligations.

8. Data Subject Rights.

  - Controller shall be solely responsible for compliance with any statutory obligations concerning requests to exercise Data Subject rights under Data Protection Laws (e.g., for access, rectification, deletion of Controller Personal Data, etc.). Processor shall, at Controller's sole expense, use commercially reasonable efforts to assist Controller in fulfilling Controller's obligations with respect to such Data Subject requests, as required under Data Protection Laws.

  - Upon receipt of a request from a Data Subject under any Data Protection Laws in respect to Controller Personal Data, Processor shall promptly notify Controller of such request and shall not respond to such request except on the documented instructions of Controller or as required by Data Protection Laws to which the Processor is subject, in which case Processor shall, to the extent permitted by Data Protection Laws, inform Controller of such legal requirement prior to responding to the request.

9. Data Protection Impact Assessment and Prior Consultation.

At Controller's written request and expense, the Processor and each Sub Processor shall provide reasonable assistance to Controller with respect to any Controller Personal Data Processed by Processor and/or a Sub Processor, with any data protection impact assessments or prior consultations with Supervisory Authorities or other competent data privacy authorities, as required under any Data Protection Laws.

10. Deletion or Return of Controller Personal Data.

Processor shall promptly and in any event within 60 (sixty) days of the date of cessation of provision of the Services to Controller involving the Processing of Controller Personal Data, delete, return, or anonymize all copies of such Controller Personal Data, provided however that Processor may retain Controller Personal Data, as permitted by Applicable

Law and further provided that Processor will not be required to delete or return Aggregate Data.

11. Audit Rights.

11.1. Subject to Sections 11.2 and 11.3, Processor shall make available to an auditor mandated by Controller in coordination with Processor, upon prior written request, such information reasonably necessary to demonstrate compliance with this DPA and shall allow for audits, including inspections, by such reputable auditor mandated by the Controller in relation to the Processing of the Controller Personal Data by the Processor, provided that such third-party auditor shall be subject to confidentiality obligations.

11.2. Any audit or inspection shall be at Controller's sole expense, and subject to Processor's reasonable security policies and obligations to third parties, including with respect to confidentiality. The results of any audit or inspection shall be considered the confidential information of the Processor and subject to the confidentiality provisions under the Agreement.

11.3. Controller and any auditor on its behalf shall use best efforts to minimize or avoid causing any damage, injury or disruption to the Processors' premises, equipment, employees and business and shall not interfere with the Processor's day-to-day business. Controller and Processor shall mutually agree upon the scope, timing and duration of the audit or inspection and the reimbursement rate, for which Controller shall be responsible. Processor need not give access to its premises for the purposes of such an audit or inspection:

11.3.1. to any individual unless he or she produces reasonable evidence of identity and authority;

11.3.2. if Processor was not given a prior written notice of such audit or inspection;

11.3.3. outside of normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis; or

11.3.4. for the purposes of more than one (1) audit or inspection in any calendar year, except for any additional audits or inspections which:

11.3.4.1. Controller reasonably considers necessary because of genuine concern as to Processor's compliance with this DPA; or

11.3.4.2. Controller is required to carry out by Applicable Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Applicable Law in any country or territory, where

Controller has identified its concerns or the relevant requirement or request in its prior written notice to Processor of the audit or inspection.

11.3.5. Processor shall immediately inform Controller if, in its opinion, an instruction received under this DPA infringes the GDPR or other applicable Data Protection Laws.

12. International Data Transfer.

- Controller Personal Data that Processor processes on Controller's behalf will be transferred to, and stored and processed in, India. Controller hereby consents to the transfer of the Controller Personal Data to third countries and Controller consents to the storage and Processing of the Controller Personal Data in the India region by Processor in order for Processor to provide the Services.

- For transfers of European Personal Data to Processor for processing by the Processor in a jurisdiction other than a jurisdiction in the EU, The EEA, or the European Commission, Processor agrees that it will provide at least the same level of privacy protection for European Personal Data as required under the Applicable Data Protection Laws.

- When Processor processes Controller Personal Data under European Data Protection Law in a country that does not ensure an adequate level of protection (within the meaning of applicable European Data Protection Law), then in such cases Processor shall process Controller Personal Data in accordance with the Standard Contractual Clauses in the form set out in Annexure 3, which are incorporated into and form a part of this Agreement. The Parties agree that for the purposes of the descriptions in the Standard Contractual Clauses, AnalyticsVerse is the "data importer" and Controller is the "data exporter" notwithstanding that Controller may itself be located outside Europe.

- It is not the intention of either Party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, in the event of any conflict or inconsistency between the provisions of the Agreement and the Standard Contractual Clauses, the provisions of the Standard Contractual Clauses shall prevail to the extent of such conflict.

13. Indemnity.

Controller shall indemnify and hold Processor harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the Processor and arising directly or indirectly out of or in connection with a breach of this DPA and/or the Data Protection Laws by Controller.

14. Limitation of Liability

In no event, the aggregate liability of the Processor, its officers, directors, partners, employees and other representatives, arising out of this Agreement and the Services Agreement or otherwise in connection with this Agreement and the Services Agreement, shall exceed the total of the amount paid by Controller to Processor in twelve (12) months immediately preceding the date on which such liability arose. Processor shall not be liable for failure to carry out any of its obligations under this Agreement if such failures result from acts of any third-parties or of Controller.

15. General Terms.

- **Order of Precedence**.
  - Nothing in this DPA reduces Processor's obligations under the Services Agreement in relation to the protection of Controller Personal Data or permits Processor to Process (or permit the Processing of) Controller Personal Data in a manner that is prohibited by the Services Agreement.
  - This DPA is not intended to, and does not in any way limit or derogate from Controller's obligations and liabilities towards the Processor under the Services Agreement and/or pursuant to Data Protection Laws or any law applicable to Controller in connection with the collection, handling and use of Controller Personal Data by Controller or other processors or their sub processors, including with respect to the transfer or provision of Controller Personal Data to Processor and/or providing Processor with access thereto.
  - With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Services Agreement and including (except where explicitly agreed otherwise in writing, signed on

behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

- **Changes in Data Protection Laws.**
    - Controller may, by at least 45 (forty-five) calendar days' prior written notice to Processor, request in writing any variations to this DPA if they are required as a result of any change in, or decision of a competent authority under any Data Protection Laws in order to allow Controller Personal Data to be Processed (or continue to be Processed) without breach of that Data Protection Laws.
    - If Controller gives notice with respect to its request to modify this DPA, (i) Processor shall make commercially reasonable efforts to accommodate such modification request and (ii) Controller shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Processor to protect the Processor against additional risks, or to indemnify and compensate Processor for any further steps and costs associated with the variations made herein.

- **Severance.** Should any provision of this DPA be held invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall either be (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their duly authorized representatives to be effective as of the Effective Date.

Customer	**AnalyticsVerse**
Customer Name:	AnalyticsVerse Solutions Private Limited.
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date:

Annexure 1: Details of Processing of Controller Personal Data

This **Annexure 1** includes certain details of the Processing of Controller Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Controller Personal Data.
The subject matter and duration of the Processing of the Controller Personal Data are set out in the Services Agreement and this DPA.

The nature and purpose of the Processing of Controller Personal Data:
Rendering Services in the nature of the AnalyticsVerse solution that provides software development analytics, as detailed in the Services Agreement.

Customer Personal Data will be Processed by AnalyticsVerse for purposes which shall include but shall not be limited to;

- Providing the Services to the Customer;
- Performing the Services Agreement, this Agreement and/or other contracts executed by the Parties;
- Acting upon Customer's instructions, where such instructions are consistent with the terms of the Services Agreement;
- Providing support and technical maintenance, if agreed in the Services Agreement;
- Preventing, mitigating and investigating the risks of Personal Data Breach, fraud, error or any illegal or prohibited activity;
- Resolving disputes;
- Enforcing the Services Agreement, this Agreement and/or defending AnalyticsVerse rights;
- Complying with applicable laws and regulations.

The types of Controller Personal Data to be Processed are as follows:
Data regarding how the Controller's systems, project management tools and code are used, planned, accessed and developed by employees and service providers of Customer. Additionally, names, emails and git profiles, project management tool profiles may be processed.

The categories of Data Subject to whom the Controller Personal Data relates to are as follows:
Data Subjects who are Controller's employees or service providers who access the Controller's systems and code.

The obligations and rights of Controller.
The obligations and rights of Controller are set out in the Services Agreement and this DPA.

Annexure 2: Binding Security Document

Processor will maintain measures meant to identify, manage, mitigate and/or remediate vulnerabilities within the Processor computing environments.
Security measures include:

- Patch management
- Vulnerability scanning and periodic penetration testing (Internet facing systems) with remediation of identified vulnerabilities

Processor uses the most appropriate secure settings for its devices and software.
Supplementary details of security settings used: Before using any new software the Processor's team checks that the product meets the necessary security and compliance requirements in addition to applying latest updates. Processor's team adopted the OWASP top 10 vulnerability scanners as a starting point combined with various scans, Encryption Procedures and multiple monitoring systems.

Processor controls who has access to your data and services
Processor will maintain proper controls for governing user access to systems and applications containing Personal Data. All access requests will be approved based on individual role-based access and reviewed on a regular basis for continued business need. Processor will limit privileged access to individuals for a limited period. Supplementary details of how access to your system is controlled: Access is granted based on role hierarchy and least privilege access, along with audit logs covering all systems. The system is fully monitored with manual reviews of the Top Management.

Processor protects itself from viruses and other malware.
All anti-virus and anti-malware software are regularly updated and regular scans are run

Processor keeps its software and devices up-to-date.
Hardware and software needs regular updates to fix bugs and security vulnerabilities.

Processor regularly backs-up its data.
Regular backups of your most important data will ensure it can be quickly restored in the event of disaster or ransomware infection.

Security Incidents
Processor will maintain an incident response plan and follow documented incident response policies including data breach notification to Data Controller without undue delay where a breach is known or reasonably suspected to affect Controller Personal Data.

Risk Management
Processor will assess risks related to processing of Personal Data and create an action plan to mitigate identified risks.

Security Policies
Processor will maintain and follow IT security policies and practices that are integral to Processor’s business and mandatory for all Processor employees, including supplemental personnel. IT security policies will be reviewed periodically and amend such policies as Processor deems reasonable to maintain protection of services and Content processed therein.

Processor employees will complete security and privacy education annually. Additional policy and process training will be provided to persons granted administrative access to security components that is specific to their role within Processor’s operation and support of the service, and as required to maintain compliance and certifications.

System and Network Security
Processor will employ encrypted and authenticated remote connectivity to Processor computing environments.

Privacy by Design
Processor will incorporate Privacy by Design principles for systems and enhancements at the earliest stage of development as well as educate all employees on security and privacy annually.

Annexure 3: Standard Contractual Clauses

(Controller to Processor)

Module II

SECTION 1

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annexure 4.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annexure 4.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annexure 4.B.

(d) The Appendix to these Clauses containing the Annexures referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b)

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annexure 4.B.

Clause 7

Intentionally Left Blank

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annexure 4.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annexure 4.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annexure 2. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annexure 4.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union [2](in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 7 business days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annexure 2 the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annexure 4.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annexure 4.C shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annexure 4.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of The Republic of Ireland (*specify Member State*).]

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the state that the client is situated.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

IN WITNESS WHEREOF, the parties have caused these Standard Contractual Clauses to be executed by their authorized representative:

On behalf of the data exporter:

Sign: Name: Position: _

Address: _

On behalf of the data importer:

Sign: Name: Position: _

Address:

Annexure 4 to the Standard Contractual Clauses

A. List of Parties

Data exporter(s):

Name:

Address:

Contact person's name, position and contact details:

Signature and date: _

Role: Controller

Data importer(s):

Name: AnalyticsVerse Solutions Private Limited

Address:

Contact person's name, position and contact details:

Signature and date: _

Role: Processor

B. Description of Transfer

- Categories of data subjects whose personal data is transferred

Data Subjects who are Controller's employees or service providers who access the Controller's systems and code.

- Categories of personal data transferred

Data regarding how the Controller's systems, code and project management tools are used, planned, accessed and developed by employees and service providers of Controller. Additionally, names, emails, git management profiles(Github/Gitlab/Bitbucket), project management tool profiles may be processed.

- The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Transfer is on a continuous basis.

- Nature of the processing

Rendering Services in the nature of the AnalyticsVerse solution that provides software development productivity analytics, as detailed in the Services Agreement.

- Purpose(s) of the data transfer and further processing

Rendering Services in the nature of the AnalyticsVerse solution that provides software development productivity analytics, as detailed in the Services Agreement.

- The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the term of the Services Agreement .

- For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

AWS – data hosting, processing for the duration of the provision of services.
Amplitude - usage analytics, processing for the duration of the provision of services
Okta – access management, processing for the duration of the provision of services
Chargebee – subscription management, processing for the duration of the provision of services
Stripe – payment gateway, processing for the duration of the provision of services
Freshchat – chat platform, processing for the duration of the provision of services
Sendgrid – SMTP Provider, processing for the duration of the provision of services
Zerobounce – email verification, processing for the duration of the provision of services
Google - Fraud Prevention, Usage Analytics, Conversion Tracking, processing for the duration of the provision of services
Hubspot - chat platform, processing for the duration of the provision of services
SendinBlue - marketing emails , processing for the duration of the provision of services
Mailchimp - marketing emails , processing for the duration of the provision of services

C. Competent Supervisory Authority

Indentification of the competent supervisory authority/ies in accordance with Clause 13

- If the data exporter is established in an EU Member State: the supervisory authority with responsibility for ensuring compliance by the data exporter with GDPR as regards the data transfer will act as competent supervisory authority.

- If the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR (i.e., Article 3(2) GDPR) and has appointed a representative in the EU (i.e., Article 27(1) GDPR): the supervisory authority of the Member State in which the representative is established will act as competent supervisory authority.

- If the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR without however having to appoint a representative in the EU: the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under the Standard Contractual Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, will act as competent supervisory authority.

Annexure 5

In accordance with Clause 9(a), the controller has authorized the use of the following sub-processors:

- AWS:
  Subject Matter: Data Hosting
  Nature of Processing: Cloud infrastructure provider for AnalyticsVerse, where the SaaS application is hosted.
- Amplitude:
  Subject Matter: Usage Analytics
  Nature of Processing: For understanding user usage across the platform
- Okta:
  Subject Matter: Access Management
  Nature of Processing: For managing access and authentication to the platform
- Chargebee
  Subject Matter: Subscription Management
  Nature of Processing: For managing subscriptions to the platform. All billing related operations are carried out through Chargebee
- Stripe
  Subject Matter: Payment Gateway
  Nature of Processing: For processing payments, stripe will be used in conjunction with Chargebee
- Freshchat
  Subject Matter: Chat platform
  Nature of Processing: Chat platform enabling to answer end user queries
- Sendgrid
  Subject Matter: SMTP Provider
  Nature of Processing: SMTP for sending emails to end customers.
- Zerobounce
  Subject Matter: Email verification
  Nature of Processing: For verifying email validity on signup to avoid spam
- Google
  Subject Matter: Fraud Prevention, Usage Analytics, Conversion Tracking
  Nature of Processing: Recaptcha for fraud prevention. Firebase and Google analytics for usage analtyics. Conversion tracking in google ads
- Hubspot
  Subject Matter: Chat platform
  Nature of Processing: Chat platform enabling to answer end user queries

- Sendinblue
  Subject Matter: Marketing emails
  Nature of Processing: To send promotional emails
- Mailchimp
  Subject Matter: Marketing emails
  Nature of Processing: To send promotional emails