**THIS DATA PROCESSING AGREEMENT IS A LEGAL AGREEMENT BETWEEN DEVOPS INTEGRATION AND ITS AFFILIATES, IF ANY (“DEVOPS”, “WE”, “OUR”, “US”) AND YOU (the “CUSTOMER”, “YOU”). THIS DPA SUPPLEMENTS OUR TERMS AND CONDITION WHICH YOU OPT INTO WHEN SIGNING UP FOR SERVICES PROVIDED BY US. THIS AGREEMENT TAKES EFFECT (OR BE DEEMED TO HAVE COME INTO EFFECT) BASED ON THE DAY YOU SIGNED UP FOR OUR SERVICES. YOU CAN OPT OUT ANYTIME BY CANCELLING YOUR ACCOUNT WITH US. NOW THEREFORE THIS DATA PROCESSING AGREEMENT WITNESSETH AS UNDER**

1. **DEFINITION**
2. **CONTROLLER:** The Controller means You – the Customer Data subject means the individual to whom Personal Data relates.
3. **DATA PROTECTION LAW:** Data Protection Laws means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of processing Personal Data in question under the Agreement, including without limitation European Data Protection Laws **(“GDPR”),** the California Consumer Privacy Act **(“CCPA”)** and the data protection and privacy laws of the United Kingdom, Australia and Singapore; in each case as amended, repealed, consolidated or replaced from time to time.
4. **DPA:** DPA means this data processing agreement.
5. **TERMS & CONDITIONS:** Terms & Condition means terms and condition placed on our website. The link to the same is given below;

<https://devopsintegration.io/terms>

1. **PERSONAL DATA:** Personal Data means any information relating to an identified or identifiable individual where such information is contained within Customer Data and is protected similarly as personal data or personally identifiable information under applicable Data Protection Law.
2. **PROCESSING:** The Processing means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data.
3. **PROCESSOR:** Processor means **“DEVOPS INTEGRATION”.**
4. **SERVICES:** Services means add on or Plug-in Services.
5. **STANDARD CONTRACTUAL CLAUSES:** Standard Contractual Clauses means the EU model clauses for Personal Data transfer from controllers to processors.
6. **SUBSIDIARY:** Subsidiary means any entity that directly or indirectly controls, is controlled by or is under common control of a party.

***“CONTROL,”*** *for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of a party.*

1. **SUB-PROCESSOR**. Sub-Processor means any person or entity engaged by Devops (including a Subsidiary) to process Personal Data in the provision of the Services to the Customer.
2. **SUBSCRIPTION TERM:** means the specific duration or period for which a subscription-based service is in effect.
3. **PURPOSE**

The Processor has agreed to provide the add Services to the Controller in accordance with the terms of this DPA and Terms & Conditions of Devops Integration. In providing the Services, the Processor shall process Customer Data on behalf of the Controller. Customer Data may include Personal Data. The Processor will process and protect such Personal Data in accordance with the terms of this DPA.

1. **RIGHTS AND OBLIGATIONS OF PROCESSOR**
2. ‍The Processor will process personal data only in accordance with the documented instructions provided by the Controller. The Processor should not process the data for any other purposes.
3. The Processor will assist the Controller in fulfilling its data protection obligations. This includes cooperating with the Controller in conducting Data Protection Impact Assessments (DPIAs) and notifying data breaches.
4. The Processor is obligated to implement appropriate technical and organizational measures to ensure the security and confidentiality of personal data. This includes encryption, access controls, and regular security assessments.
5. If the data processing is likely to result in a high risk to the rights and freedoms of Data Subjects, the Processor must assist the Controller in conducting DPIAs to assess and mitigate these risks.
6. The Processor is required to maintain records of its data processing activities and make these records available to supervisory authorities upon request.
7. If Personal Data is transferred to countries outside the European Economic Area (EEA) or other regions with specific data protection requirements, the Processor must ensure that adequate safeguards are in place.
8. The Processor may be required to cooperate with supervisory authorities and provide them with necessary information and documentation during investigations.
9. The Processor shall ensure that all employees, agents, officers, and contractors involved in the handling of Personal Data:
10. are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential;
11. have received appropriate training on their responsibilities as a data processor; and
12. are bound by the terms of this DPA.
13. The Processor shall implement appropriate technical and organizational procedures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.
14. The Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
15. the pseudonymisation and encryption of Personal Data;
16. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
17. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
18. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.
19. The security measures as mentioned in Section 5 shall be at all times adhered to as a minimum-security standard. The Controller accepts and agrees that the technical and organizational measures are subject to development and review and that the Processor may use alternative suitable measures to those detailed in the Section 5 to this DPA provided that such updates and modifications do not result in the degradation of the overall security of the Services.
20. **RIGHTS AND OBLIGATION OF CONTROLLER**
21. **‍**The Controller represents and warrants that it shall comply with the terms of the Terms & Conditions, this DPA and all applicable Data Protection Laws.
22. The Controller represents and warrants that it has obtained any and all necessary permissions and authorizations necessary to permit the Processor, its Subsidiaries, if any and Sub-Processors, to execute their rights or perform their obligations under this DPA.
23. All Subsidiaries of the Controller who use the Services shall comply with the obligations of the Controller set out in this DPA.
24. The Controller must have a lawful basis for processing personal data, such as consent, contract performance, legal obligation, legitimate interests, or protection of vital interests.
25. The Controller must provide clear, concise, and accessible information to Data Subjects about the data processing, including purposes, lawful basis, and data subject rights.
26. The controller should only collect and process data that is relevant and necessary for the stated purposes.
27. **SECURITY MEASURES**

The Processor will undertake the below mentioned security measures to protect the Personal Data;

1. The Processor shall implement and maintain appropriate technical and organizational security measures to safeguard the confidentiality, integrity, and availability of the Personal Data processed under this Agreement. These measures shall be designed to protect against unauthorized access, disclosure, alteration, and destruction of Personal Data, in accordance with applicable data protection laws.
2. The Processor shall establish access controls to ensure that Personal Data is accessible only to authorized personnel based on the principle of least privilege. Access to Personal Data shall be granted on a need-to-know basis, and access logs shall be maintained.
3. The Processor shall employ encryption mechanisms to protect Personal Data during transmission and storage. Data encryption in transit {e.g., Transport Layer Security (TLS)/Secure Sockets Layer (SSL)} and at rest (e.g., encryption of stored data) shall be utilized as appropriate.
4. Regular data backups shall be conducted to ensure data recovery in the event of data loss or a security incident. These backups shall be securely stored and regularly tested for integrity and recoverability.
5. The Processor shall maintain an incident response plan outlining procedures for detecting, reporting, and responding to data breaches and security incidents. Data breaches shall be reported to the Controller in accordance with the terms of this Agreement and applicable laws.
6. The Processor shall provide security training and awareness programs to its employees and contractors who have access to Personal Data to ensure they are knowledgeable about data protection and security best practices.
7. The Processor may engage third-party security assessments or audits to evaluate the effectiveness of its security measures. Any identified vulnerabilities or deficiencies shall be promptly remediated.
8. The Processor shall maintain a process for promptly applying security updates, patches, and fixes to software and systems to mitigate known vulnerabilities.
9. If applicable, the Processor shall implement physical security measures to protect data centers or facilities where Personal Data is processed or stored.
10. The Processor shall maintain documentation and records of its security measures, including policies, procedures, risk assessments, and security incident reports, as required by applicable data protection laws.
11. **SUB PROCESSOR**
12. The Controller acknowledges and agrees that:
13. Subsidiaries of the Processor may be used as Sub-processors; and
14. the Processor and its Subsidiaries respectively may engage Sub-processors in connection with the provision of the Services.
15. All Sub-processors who process Personal Data in the provision of the Services to the Controller shall comply with the obligations of the Processor similar to those set out in this DPA.
16. Where Sub-processors are located outside of the EEA, the Processor confirms that such Sub-processors:
17. are located in a third country or territory recognised by the EU Commission to have an adequate level of protection; or
18. have entered into Standard Contractual Clauses with the Processor; or
19. have other legally recognised appropriate safeguards in place.
20. The Processor shall make available to the Controller the current list of Sub-processors which shall include the identities of Sub-processors and their country of location. During the term of this DPA, the Processor shall provide the Controller with at least 10 days prior notification, via email (or in-application notice), of any changes to the list of Sub-Processor(s) who may process Personal Data before authorising any new or replacement Sub-processor(s) to process Personal Data in connection with the provision of the Services. The current list of Sub-processors is mentioned in Appendix 1.
21. The Processor will provide prior written notification (via email) to the Controller in the event of any proposed addition or removal of Sub Processors involved in the data processing. This notification will include relevant details such as the identity of the Sub Processor, their role in data processing, and the reasons for their addition or removal. In case if the Controller rejects the proposed modification, the Processor will promptly review the concerns and objections raised in relation to the proposed Sub Processor and explore potential alternatives or solutions that align with your data privacy and security preferences.
22. **LIABILITY**
23. **‍**The limitations on liability set out in the Terms & Conditions shall apply to all claims made pursuant to any breach of the terms of this DPA.
24. The parties agree that the Processor shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Sub-processors to the same extent the Processor would be liable if performing the services of each Sub-processor directly under the terms of the DPA, subject to any limitations on liability set out in the Terms & Conditions.
25. The parties agree that the Controller shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Subsidiaries as if such acts, omissions or negligence had been committed by the Controller itself. The Controller shall not be entitled to recover more than once in respect of the same claim.
26. **~~AUDIT~~**

**~~‍~~**~~The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with its processing obligations and allow for and contribute to audits and inspections. Any audit conducted under this DPA shall consist of an examination of the most recent reports, certificates and/or extracts prepared by an independent auditor, if any bound by confidentiality provisions similar to those set out in the Agreement. In the event that provision of the same is not deemed sufficient in the reasonable opinion of the Controller, the Controller may at its own expense conduct a more extensive audit which will be:~~

1. ~~limited in scope to matters specific to the Controller and agreed in advance with the Processor;~~
2. ~~carried out during Indian business hours and upon reasonable notice which shall be not less than 4 weeks unless an identifiable material issue has arisen; and~~
3. ~~conducted in a way which does not interfere with the Processor’s day-to-day business.~~

~~The Processor may charge a fee (based on its reasonable time and costs) for assisting with any audit. The Processor will provide the Controller with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. This clause shall not modify or limit the rights of audit of the Controller, instead it is intended to clarify the procedures in respect of any audit undertaken pursuant thereto.~~

1. **DATA DELETION**

Processor will delete or return all Customer Data, including Personal Data (including copies thereof) processed pursuant to this DPA, on termination or expiration of your Subscription Service in accordance with the procedures and timeframes set out in the Agreement, save that this requirement shall not apply to the extent Processor is required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which data Processor shall securely isolate and protect from any further Processing. The personal data includes Zendesk Ticket Id, DevOps Work item, Zendesk as well as DevOps API tokens. The personal data of the customers is retained for a period of 30 days. However, the Processor understand the importance of data privacy and customer requests. Therefore, if a customer requests the deletion of their personal data, we will ensure that the data is deleted within 48 hours of receiving the request. You may send your request via email to [support@devopsintegration.io](mailto:support@devopsintegration.io). Once the personal data is deleted, the customer will not be able to access the services until they revalidate their account through new API tokens for both Zendesk and Azure DevOps. This is necessary to establish a new connection between the customer's account and the respective platforms

1. **LOGS STORAGE AND DELETION**
2. The Service Provider shall maintain detailed logs of all activities and transactions related to the services provided to the Customer. Log data will be stored for a period of 30 days.
3. At the end of the specified retention period, the Service Provider shall promptly delete or anonymize the log data, unless required to retain such data by applicable laws or regulations.
4. Access to log data shall be limited to authorized personnel only. Any access to log data will be logged and subject to auditing.
5. **DATA BACKUP STORAGE, DELETION, AND AUTHORIZED ACCESS**
6. The Service Provider will maintain regular backups of Customer data to ensure data integrity and availability.
7. Backup data will be retained for a specified period of 30 days or as required by applicable laws and regulations.
8. Upon the expiration of the retention period, the Service Provider shall securely delete or anonymize backup data.
9. Access to backup data will be limited to authorized personnel only.
10. **NOTIFICATION OF DATA BREACH**
11. **‍**The Processor shall notify the Controller without undue delay after becoming aware of (and in any event within 72 hours of discovering) any accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access to any Personal Data (“**DATA BREACH**”).
12. The Processor will take all commercially reasonable measures to secure the Personal Data, to limit the effects of any Data Breach and to assist the Controller in meeting the Controller’s obligations under applicable law.
13. The Processor’s notification of, or response to, a Data Breach under this Section 10 will not be construed as an acknowledgment by the Processor of any fault or liability with respect to the Data Breach.
14. The Processor will not assess the content of the Controller’s data in order to identify information subject to any specific Controller data breach.
15. The Controller is solely responsible for complying with data breach notification laws applicable to the Controller and fulfilling any third-party notification obligations related to any Data Breach(es).
16. **COMPLIANCE, COOPERATION AND RESPONSE**
17. In the event that the Processor receives a request from a Data Subject in relation to Personal Data, the Processor will refer the Data Subject to the Controller unless otherwise prohibited by law.
18. The Controller shall reimburse the Processor for all costs incurred resulting from providing reasonable assistance in dealing with a Data Subject request or assisting the Controller in complying with its duties.
19. In the event that the Processor is legally required to respond to the Data Subject, the Controller will fully cooperate with the Processor as applicable.
20. The Processor will notify the Controller promptly of any request or complaint regarding the processing of Personal Data, which adversely impacts the Controller unless such notification is not permitted under applicable law or relevant court order.
21. The Processor may make copies of and/or retain Personal Data in order to comply with its legal or regulatory requirement including, but not limited to retention requirements.
22. The parties acknowledge that it is the duty of the Controller to notify the Processor within a reasonable time, of any changes to applicable data protection laws, codes or regulations which may affect the contractual duties of the Processor.
23. The Processor shall respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the technical and organizational measures to maintain compliance.
24. If the parties agree that amendments are required, but the Processor is unable to accommodate the necessary changes, the Controller may terminate the part or parts of the Services which give rise to the non-compliance. To the extent that other parts of the Services provided are not affected by such changes, the provision of those Services shall remain unaffected.
25. The Controller and the Processor and, where applicable, their representatives, shall cooperate, on request, with a supervisory data protection authority in the performance of their respective obligations under this DPA.
26. The parties agree that the Processor will be entitled to charge the Controller additional fees to reimburse the Processor for its staff time, costs and expenses in assisting the Controller, when the Controller requests the Processor to provide assistance pursuant to this DPA (data processing agreement). In such cases, the Processor will notify the Controller of its fees for providing assistance, in advance.
27. **TERM AND TERMINATION**
28. This DPA shall be effective from the date of execution and shall remain in force for the duration of the paid Subscription Term agreed between the Controller and the Processor, or until otherwise terminated in accordance with the provisions of this DPA.
29. This DPA shall be automatically extended for any extensions of the Subscription Term, unless either party provides written notice of termination at least 30 days before the end of the then-current Subscription Term.
30. **GENERAL**
31. This DPA sets out the entire understanding of the parties with regards to the subject matter herein. Should a provision of this DPA be invalid or become invalid then the legal effect of the other provisions shall be unaffected. A valid provision is deemed to have been agreed which comes closest to what the parties intended commercially and shall replace the invalid provision. The same shall apply to any omissions.
32. This DPA shall be governed by the laws of India. The courts of India shall have exclusive jurisdiction for the settlement of all disputes arising under this DPA.

**APPENDIX I**

**LIST OF SUB-PROCESSOR**

1. **Microsoft Azure Cloud Digital Ocean**