

# Data Processing Agreement

This Data Processing Agreement (“**DPA**”) is between

- (a) The company and its Affiliates (collectively the “**Customer**”) identified in the signature block, and
- (b) ToolsPlus Sdn. Bhd. (1275352-W) a company incorporated under the laws of Malaysia and its Affiliates (collectively “**ToolsPlus**”).

Together the “**Parties**” and each a “**Party**”.

This DPA supplements the terms of the End User License Agreement (“**EULA**”) (the “**Service Agreement**”), under which ToolsPlus provides certain services (“**Services**”).

This DPA will be effective as of the date ToolsPlus receives a complete and executed DPA from the Customer indicated in the signature block below in accordance with the instructions under Sections I and II below (the “**Effective Date**”). This DPA shall apply to personal data processed by ToolsPlus on behalf of the Customer in the course of providing the Services.

## I. Instructions

This DPA has been pre-signed on behalf of ToolsPlus. To enter into this DPA, you must:

- (a) be a customer of the Service(s);
- (b) complete the [signature block](#) below by signing and providing all items; and
- (c) submit the completed and signed DPA to ToolsPlus as instructed.

## II. Effectiveness

- (a) This DPA will only be effective (as of the Effective Date) if executed and submitted to ToolsPlus accurately and in full accordance with paragraph I above and this paragraph II. If you make any deletions or other revisions to this DPA, then this DPA will be null and void.
- (b) Customer signatory represents to ToolsPlus that he or she has the legal authority to bind the Customer and is lawfully able to enter into this DPA.
- (c) This DPA will terminate automatically upon termination of the Service or as earlier terminated pursuant to the terms of this DPA.

### III. Data Processing Terms

The Parties agree as follows:

#### 1. Definitions

Unless otherwise defined in this DPA or in the Service Agreement, all capitalized terms used in this DPA shall have the following meanings:

- 1.1. **“Affiliate”** means, with respect to a party, any person which directly or indirectly Controls, is Controlled by or is under common Control with such party.
- 1.2. **“Applicable Data Protection Law”** means US Data Protection Law and European Data Protection Law that are applicable to the processing of Customer Personal Data under this DPA.
- 1.3. **“Control”** shall mean the power to direct the management or policies of a person, whether through the ownership of more than 50% (fifty percent) of the voting power of such person or, through the power to appoint more than half of the members of the board of directors or similar governing body of such person, through contractual arrangements or otherwise.
- 1.4. **“controller”, “processor”, “data subject”, “personal data” and “processing”** (and **“process”**) shall have the meanings given in European Data Protection Law.
- 1.5. **“Customer Personal Data”** means any personal data provided by (or on behalf of) Customer to ToolsPlus in connection with the Services, all as more particularly described in this DPA.
- 1.6. **“EEA”** means the European Economic Area.
- 1.7. **“European Data Protection Law”** means: (i) Regulation 2016/679 of the European Parliament and of the Council 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) (the **“EU GDPR”**); (ii) in respect of the United Kingdom the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the **“UK GDPR”**); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) the Swiss Federal Data Protection Act (**“Swiss DPA”**).
- 1.8. **“Privacy Shield Principles”** means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended, superseded or replaced).
- 1.9. **“Restricted Transfer”** means: (i) where the EU GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country

which is not subject based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

- 1.10. **“Services”** means the services to be provided by ToolsPlus (directly or indirectly) to the Customer, in accordance with the Service Agreement.
- 1.11. **“Standard Contractual Clauses”** means: (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (**“EU SCCs”**); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR (**“UK SCCs”**); and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (the **“Swiss SCCs”**).
- 1.12. **“Sub-processor”** means any processor engaged by ToolsPlus to assist in fulfilling its obligations with respect to providing the Services pursuant to the Service Agreement or this DPA where such entity processes Customer Personal Data. Sub-processors may include ToolsPlus’ affiliates or other third parties.
- 1.13. **“U.S. Data Protection Law”** means all data protection or privacy laws and regulations applicable to the Customer Personal Data in question in force within the United States, including the California Consumer Privacy Act (as may be amended from time to time) (the **“CCPA”**), and any rules or regulations implementing the foregoing.

## 2. Roles of the Parties

Where Applicable Data Protection Law provides for the roles of “controller,” “processor,” and “subprocessor”:

- 2.1. Where Customer is a controller of the personal data covered by this DPA, ToolsPlus shall be a processor processing personal data on behalf of the Customer and this DPA shall apply accordingly;
- 2.2. Where Customer is a processor of the personal data covered by this DPA, ToolsPlus shall be a Sub-processor of the personal data and this DPA shall apply accordingly; and
- 2.3. Where and to the extent ToolsPlus processes personal data as a controller, ToolsPlus will process such personal data in compliance with Applicable Data Protection Laws and [Section 5](#) of this DPA, to the extent applicable.

### **3. Processing Instructions**

- 3.1. Subject to the other provisions of this DPA, the Customer
  - (a) instructs ToolsPlus to take such steps in the processing of Customer Personal Data on its behalf as are reasonably necessary to the provision of the Services or otherwise to the performance of ToolsPlus' obligations under the Service Agreement; and
  - (b) irrevocably authorizes ToolsPlus to provide equivalent instructions to Sub-processors on its behalf.
- 3.2. The description of the processing of personal data related to the Services is set out in [Exhibit 1](#).
- 3.3. The parties acknowledge and agree that the description of processing can be updated by ToolsPlus from time to time to reflect new products, features or functionality comprised within the Services. ToolsPlus will update relevant documentation to reflect such changes.

### **4. Compliance with Applicable Data Protection Law**

- 4.1. ToolsPlus shall comply and ensure that each of its Affiliates and Sub-processors comply with Applicable Data Protection Law in relation to its processing of personal data in connection with the Service Agreement.
- 4.2. The Customer shall ensure that, before any Customer Personal Data is disclosed by the Customer to the Processor, the Customer has taken any steps necessary to ensure that the disclosure does not breach any Applicable Data Protection Law. Without limiting the foregoing, the Customer shall be responsible:
  - (a) at all times for the integrity, quality and legality of the Customer Personal Data provided by the Customer to ToolsPlus. ToolsPlus is under no duty to investigate the completeness, accuracy or sufficiency of the Customer Personal Data provided to it by the Customer;
  - (b) for informing the data subject that their Customer Personal Data will be transferred to and processed by ToolsPlus, and to direct them to ToolsPlus' Privacy Policy available on the ToolsPlus website; and
  - (c) to the extent required by Applicable Data Protection Law, to obtain the consent of the data subjects for their Customer Personal Data to be transferred to and processed by the Processor, and where the data subject is below the applicable age of consent under Applicable Data Protection Law, to obtain the consent of the data subject's parents and/or guardians.

### **5. Restricted transfers**

The parties agree that when the transfer of Customer Personal Data from Customer (as "data exporter") to ToolsPlus (as "data importer") is a Restricted Transfer and Applicable

Data Protection Law requires that appropriate safeguards are put in place, it shall be subject to the appropriate Standard Contractual Clauses, which shall be deemed incorporated into and form a part of this DPA, as follows:

- 5.1. In relation to transfers of Customer Personal Data protected by the EU GDPR and processed in accordance with Sections [2.1](#) and [2.2](#) of this DPA, the EU SCCs shall apply, completed as follows:
  - (a) Module Two or Module Three will apply (as applicable);
  - (b) in Clause 7, the optional docking clause will apply;
  - (c) in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in [Section 8.4](#) of this DPA;
  - (d) in Clause 11, the optional language will not apply;
  - (e) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;
  - (f) in Clause 18(b), disputes shall be resolved before the courts of Ireland;
  - (g) Annex I of the EU SCCs shall be deemed completed with the information set out in [Exhibit 1](#) to this DPA, as applicable; and
  - (h) Subject to [Section 7](#) of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in [Exhibit 2](#) to this DPA;
- 5.2. In relation to transfers of Customer Personal Data protected by the EU GDPR and processed in accordance with [Section 2.3](#) of this DPA, the EU SCCs shall apply, completed as follows:
  - (a) Module One will apply;
  - (b) in Clause 7, the optional docking clause will apply;
  - (c) in Clause 11, the optional language will not apply;
  - (d) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;
  - (e) in Clause 18(b), disputes shall be resolved before the courts of Ireland;
  - (f) Annex I of the EU SCCs shall be deemed completed with the information set out in [Exhibit 1](#) to this DPA, as applicable; and
  - (g) Subject to [Section 7](#) of this DPA, Annex II of the EU SCCs shall be deemed completed with the information set out in [Exhibit 2](#) to this DPA;
- 5.3. In relation to transfers of Customer Personal Data protected by the UK GDPR, the EU SCCs will also apply in accordance with paragraphs (a) and (b) above, with the following modifications:
  - (a) any references in the EU SCCs to “Directive 95/46/EC” or “Regulation (EU) 2016/679” shall be interpreted as references to the UK GDPR; references to specific Articles of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK GDPR;

- (b) references to “EU”, “Union” and “Member State law” are all replaced with “UK”; Clause 13(a) and Part C of Annex I of the EU SCCs are not used; references to the “competent supervisory authority” and “competent courts” shall be interpreted as references to the Information Commissioner and the courts of England and Wales;
- (c) Clause 17 of the EU SCCs is replaced to state that “The Clauses are governed by the laws of England and Wales” and Clause 18 of the EU SCCs is replaced to state “Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceeding against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts”,

unless the EU SCCs, implemented as described above, cannot be used to lawfully transfer such Customer Personal Data in compliance with the UK GDPR in which case the UK SCCs shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes or Appendices of the UK SCCs shall be populated using the information contained in Exhibits [1](#) and [2](#) of this DPA (as applicable);

- 5.4. In relation to transfers of Customer Personal Data protected by the Swiss DPA, the EU SCCs will also apply in accordance with paragraphs (a) and (b) above, with the following modifications:

- (a) any references in the EU SCCs to “Directive 95/46/EC” or “Regulation (EU) 2016/679” shall be interpreted as references to the Swiss DPA;
- (b) references to “EU”, “Union”, “Member State” and “Member State law” shall be interpreted as references to Switzerland and Swiss law, as the case may be; and
- (c) references to the “competent supervisory authority” and “competent courts” shall be interpreted as references to the Swiss Federal Data Protection and Information Commissioner and competent courts in Switzerland,

unless the EU SCCs, implemented as described above, cannot be used to lawfully transfer such Customer Personal Data in compliance with the Swiss DPA in which case the Swiss SCCs shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes or Appendices of the Swiss SCCs shall be populated using the information contained in Exhibits [1](#) and [2](#) of this DPA (as applicable);

- 5.5. 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, if and to the extent the Standard Contractual Clauses conflict with any provision of the Service Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict;

- 5.6. Although ToolsPlus does not rely on the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks (“Privacy Shield”) as a legal basis for transfers of Customer Personal

Data in light of the judgment of the Court of Justice of the EU in Case C-311/18, for so long as ToolsPlus are self-certified to the Privacy Shield ToolsPlus shall continue to process Customer Data in accordance with the Privacy Shield Principles.

ToolsPlus will promptly notify Customer if it makes a determination that ToolsPlus can no longer meet its obligations under the Privacy Shield Principles; and

- 5.7. If ToolsPlus adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses or Privacy Shield adopted pursuant to Applicable Data Protection Laws) for the transfer of Customer Personal Data not described in this DPA (“**Alternative Transfer Mechanism**”), the Alternative Transfer Mechanism shall apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with European Data Protection Law and extends to the territories to which Customer Personal Data is transferred).

## 6. Confidentiality

Without prejudice to any existing contractual arrangements between the Parties, ToolsPlus shall treat all Customer Personal Data with confidentiality and shall inform all its employees, agents and/or approved Sub-processors engaged in processing the Customer Personal Data of its confidential nature. ToolsPlus shall ensure that all such persons or parties are under an appropriate obligation of confidentiality.

## 7. Security

ToolsPlus and, to the extent required under the Service Agreement, Customer shall implement appropriate technical and organizational measures to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data, in accordance with ToolsPlus’ security standards described in [Exhibit 2](#) (“**Security Measures**”). Customer acknowledges that the Security Measures are subject to technical progress and development and that ToolsPlus may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Services.

## 8. Subprocessing

- 8.1. Customer authorizes the engagement of Sub-processors.
- 8.2. Customer agrees that ToolsPlus may continue to use those Sub-processors already engaged by ToolsPlus as of the date of this DPA. Information about Sub-processors, including their functions and locations, is available at <https://toolspl.us/subprocessors>.
- 8.3. Requirements for subprocessor engagement with respect to each subprocessor, ToolsPlus shall:
  - (a) Before the Sub-processor first processes any Customer Personal Data, carry out adequate due diligence to ensure that the Sub-processor is capable of

providing the level of protection for Customer Personal Data required by the Service Agreement;

- (b) Ensure that the arrangement is governed by a written contract including terms that offer at least the same level of protection for Customer Personal Data as those set out in this DPA;
- (c) Remain fully liable for all obligations subcontracted to, and all acts and omissions of the Sub-processor.

8.4. Requirements for changes to Sub-processors, ToolsPlus shall:

- (a) Make available an up-to-date list of the Sub-processors it has appointed upon written request from Customer; and
- (b) notify Customer if it adds any new Sub-processors at least fourteen (14) days prior to allowing such Sub-processor to process Customer Personal Data. Customer must subscribe to receive notice of updates to the list of Sub-processors, using the link in [Section 8.2](#). Customer may object in writing to ToolsPlus' appointment of a new Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds relating to data protection. In such an event, the parties will discuss such concerns in good faith with a view to achieving resolution. If the parties are not able to achieve resolution, Customer, as its sole and exclusive remedy, may terminate the Service Agreement (including this DPA) for convenience.

## 9. Data Subject Rights

- 9.1. ToolsPlus shall use reasonable endeavours to assist the Customer in responding to their Data Subject requests. ToolsPlus shall have at least 20 days, from the time the Customer asks for assistance, to respond to the Customer's request. The performance and cost of such requests shall be in accordance with the EULA and ToolsPlus' standard applicable rate at any given time.
- 9.2. ToolsPlus must not disclose the Personal Data to any Data Subject or to a third party and responsibility for responding to requests from Data Subjects shall remain with the Customer.

## 10. Cooperation

- 10.1. If requested, ToolsPlus will provide reasonable assistance to the Customer to comply with its obligations under Applicable Data Protection Law, taking into account the nature of processing and the information available to ToolsPlus.
- 10.2. ToolsPlus shall make available to Customer upon request any reasonable information to demonstrate compliance with ToolsPlus' obligations under this DPA.
- 10.3. ToolsPlus shall reply to any requests for information under this Section within 60 days of receiving the request.
- 10.4. ToolsPlus permits and contributes to all reasonable audits, including inspections, conducted by the Customer (or auditors appointed by either of them), as reasonably

necessary to demonstrate ToolsPlus' compliance with this DPA, provided that the Customer shall:

- a. ensure that such audits take place during ToolsPlus' business hours and on reasonable notice;
  - b. ensure that appropriate confidentiality provisions, or other contractual, professional or statutory obligations of confidentiality, are agreed with any third party involved in audit or inspection; and
  - c. take (and ensure that auditors take) reasonable endeavours to avoid causing any damage, injury or disruption to ToolsPlus;
- 10.5. ToolsPlus may charge the Customer on a time and materials basis, at ToolsPlus' standard applicable rates at any given time, for time spent in providing assistance under this Section.

## **11. Incident Management**

- 11.1. ToolsPlus shall notify Customer without undue delay upon ToolsPlus (or any subprocessor) becoming aware of a personal data breach affecting Customer Personal Data, and provide the Customer with sufficient information to allow each to meet any obligations to report or inform data subjects of the personal data breach (a **"Security Incident"**).
- 11.2. ToolsPlus takes all reasonable steps to identify and correct the underlying cause of the Security Incident so as to eliminate or minimise the risk of its repetition and the occurrence of similar Security Incidents.
- 11.3. ToolsPlus shall cooperate with the Customer to assist in the investigation, mitigation and remediation of each such Security Incident.
- 11.4. Any notifications made to the Customer pursuant to this Section shall be addressed to the employee of the Customer whose contact details are provided in [signature block](#) of this Data Processing Agreement, and shall contain:
  - a. a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of Customer Personal Data records concerned;
  - b. the name and contact details of ToolsPlus' data protection officer or another contact point where more information can be obtained;
  - c. a description of the likely consequences of the incident; and
  - d. a description of the measures taken or proposed to be taken by ToolsPlus to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

## **12. Return or Destruction of Customer Personal Data**

- 12.1. Upon termination of this DPA, upon the Customer's written request, or upon fulfillment of all purposes agreed in the context of the Services whereby no further processing is required, ToolsPlus shall, at the discretion of Customer and within reasonable business efforts, either delete, or destroy the Customer's data.
- 12.2. Generally, ToolsPlus and its Sub-processors retain minimal Customer Personal Data to only the extent required by a legal obligation and for such period as required by the legal obligation.

## **13. Loss or Damage to Customer Personal Data**

ToolsPlus shall not be responsible for any loss, damages, destruction, alteration or disclosure of Customer Personal Data caused by any third party.

## **14. Termination**

This DPA and the Standard Contractual Clauses will remain in effect until the later of:

- (a) the termination or expiry of the Service Agreement, and
- (b) ToolsPlus ceasing to process the Customer Personal Data.

## Signatures

### Signed for and on behalf of the Customer

**Signature** (required)

---

**Name** (required)

---

**Title** (optional)

---

**Date** (required)

---

**EU representative**  
(required only where  
applicable)

---

Email contact

---

**Data Protection  
Officer**  
(required only where  
applicable)


---

Email contact

---

### ToolsPlus

**Signature**



---

**Name**

Tobias Binna

**Title**

Director

**Date**

October 11, 2021

Contact information for the Data Protection Officer/compliance officer of ToolsPlus:  
[legal@toolsplus.io](mailto:legal@toolsplus.io)

## Exhibit 1

### Annex 1(A): List of Parties

	Data Exporter	Data Importer
<b>Name</b>	Customer	ToolsPlus
<b>Address / Email address</b>	As provided for in the DPA	As provided for in the DPA
<b>Contact person's name, position, and contact details</b>	As provided for in the DPA	As provided for in the DPA
<b>Activities relevant to the transfer</b>	See Annex 1(B) below	See Annex 1(B) below
<b>Role</b>	See Annex 1(B) below	See Annex 1(B) below

### Annex 1(B): Description of Processing/Transfer

The parties acknowledge that ToolsPlus' processing of personal data will include all personal data submitted or uploaded to the Services by Customer from time to time, for the purpose of, or otherwise in connection with, ToolsPlus providing the Services to Customer. Set out below are descriptions of the processing/transfers of personal data as contemplated as of the date of this DPA. Such descriptions are subject to change or maybe supplemented pursuant to [Section 3.3](#) of the DPA.

Intercom for Jira and Jira for Intercom

<b>Categories of data subjects</b>	Customers, customers' employees, and customers' collaborators
<b>Categories of personal data transferred</b>	<p>User account information, including:</p> <ul style="list-style-type: none"> <li>• User ID</li> <li>• Avatar image</li> <li>• Avatar URL</li> <li>• Full name</li> <li>• Email address</li> <li>• Time zone</li> </ul> <p>Personal data in user-generated content</p>

<b>Controller/Processor roles</b>	Controller (Customer) to Processor (ToolsPlus)
<b>Sensitive data transferred?</b>	None
<b>Frequency of the transfer</b>	Continuous
<b>Nature of the processing</b>	<p>Providing the products and services, including:</p> <ul style="list-style-type: none"> <li>• Display user profiles</li> <li>• Create and update issues from Intercom</li> <li>• Display of user-generated content (chats, comments) on different platforms (Intercom and Jira)</li> </ul>
<b>Purpose of the data transfer</b>	<p>Providing the products and services, including:</p> <ul style="list-style-type: none"> <li>• User/team communication</li> <li>• Third-party integration</li> <li>• Support/Feedback</li> </ul>
<b>Duration of the processing</b>	No processed personal data is stored. Processing of personal data will cease automatically when the customer terminates and uninstalls the Service.

#### Travis for Jira

<b>Categories of data subjects</b>	Customers, customers' employees, and customers' collaborators
<b>Categories of personal data transferred</b>	<p>User account information, including:</p> <ul style="list-style-type: none"> <li>• User ID</li> <li>• Full name</li> <li>• Email address</li> </ul> <p>Personal data in user-generated content</p>
<b>Controller/Processor roles</b>	Controller (Customer) to Processor (ToolsPlus)
<b>Sensitive data transferred?</b>	None
<b>Frequency of the transfer</b>	Continuous

<b>Nature of the processing</b>	<p>Providing the products and services, including:</p> <ul style="list-style-type: none"> <li>Forwarding source code build information from Travis CI to Jira</li> </ul>
<b>Purpose of the data transfer</b>	<p>Providing the products and services, including:</p> <ul style="list-style-type: none"> <li>User/team communication</li> <li>Third-party integration</li> <li>Support/Feedback</li> </ul>
<b>Duration of the processing</b>	<p>Processed personal data is stored on the Customer's Jira instance and can be removed at the Customer's discretion with whatever means Atlassian provides to remove such data.</p>
ToolsPlus business operations, including support	
<b>Categories of data subjects</b>	<p>Customers, customers' employees, and customers' collaborators</p>
<b>Categories of personal data transferred</b>	<p>User account information, including:</p> <ul style="list-style-type: none"> <li>Full name</li> <li>Email address</li> </ul> <p>Employment information, including:</p> <ul style="list-style-type: none"> <li>Company/organization</li> </ul> <p>Browser information</p> <p>Metadata, including:</p> <ul style="list-style-type: none"> <li>Event name and timestamp</li> <li>Page URL</li> <li>Referring URL</li> </ul>
<b>Controller/Processor roles</b>	<p>Controller (Customer) to Processor (ToolsPlus)</p> <p>Controller (Customer) to Controller (ToolsPlus)</p>
<b>Sensitive data transferred?</b>	<p>None</p>
<b>Frequency of the transfer</b>	<p>Continuous</p>
<b>Nature of the processing</b>	<p>Providing the products and services, including:</p> <ul style="list-style-type: none"> <li>Engage and respond to customer support questions</li> </ul>

	<ul style="list-style-type: none"><li>• Marketing activities</li><li>• Sales activities</li><li>• Collect/manage sales and licenses</li><li>• Analyze business metadata</li></ul>
<b>Purpose of the data transfer</b>	Providing the products and services, including: <ul style="list-style-type: none"><li>• Support/Feedback</li><li>• Marketing/Engagement</li></ul>
<b>Duration of the processing</b>	Customer data is retained permanently but can be removed from systems upon request from Customer.

### **Annex 1(C): Competent supervisory authority**

The competent supervisory authority, in accordance with Clause 13 of the EU SCCs, must be (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located. With respect to the processing of personal data to which the UK GDPR applies, the competent supervisory authority is the Information Commissioners Office (the "ICO"). With respect to the processing of personal data to which the Swiss DPA applies, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

## **Exhibit 2**

### **Technical and Organisational Security Measures**

#### **1. Access control**

##### **(a) Preventing unauthorized physical access**

Our Service is hosted on outsourced cloud infrastructure providers. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

The outsourced infrastructure providers' physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

##### **(b) Preventing unauthorized access to systems**

We take reasonable measures to prevent unauthorized access to IT systems, including authentication via strong passwords according to industry standards, and when available two-factor authentication, restricted access to employees by role, and logging of access.

Security reviews of code stored in our source code repositories are performed using static code analysis, checking for coding best practices, and identifiable software flaws.

We implement a bug bounty program to discover vulnerabilities in applications and services and to improve the overall security posture.

##### **(c) Controlling access to data**

We take reasonable measures to ensure personal data is accessible and manageable only by authorized staff, that access rights are differentiated according to duties, and that personal data cannot be read, copied, modified, or removed without authorization in the course of processing.

#### **2. Transmission control**

Data in transit is protected by HTTPS encryption (SSL/TLS). Our HTTPS implementation uses industry-standard algorithms and certificates. When data is at rest we take measures and follow industry-standard practices for security, such as to ensure that stored data is encrypted at rest.

#### **3. Availability control**

##### **(a) Infrastructure availability**

Our infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime.

(b) Online replicas and backups

Production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry-standard methods.

(c) Service availability

Our Services are designed to ensure redundancy and seamless failover. The infrastructure that supports the Services is architected with a goal to prevent single points of failure. This design assists our operations in maintaining and updating the applications while limiting downtime.