

Data Processing Agreement for TEAM Cloud Services (“Data Processing Agreement”)

Version November 1, 2024

1. Scope and Applicability

This Data Processing Agreement applies to TEAM IM's Processing of Personal Information on Your behalf as a Processor for the provision of the Services specified in Your Services Agreement. Unless otherwise expressly stated in Your Services Agreement, this version of the Data Processing Agreement shall be effective and remain in force for the term of Your Services Agreement.

2. Responsibility for Processing of Personal Information and Description of Processing Activities

2.1 You are a Controller and TEAM IM is a Processor for the Processing of Personal Information as part of the provision of the Services. Each party is responsible for compliance with its respective obligations under Applicable Data Protection Law.

2.2 TEAM IM will Process Personal Information during the term of the Services Agreement solely for the purpose of providing the Services in accordance with the Services Agreement and this Data Processing Agreement.

2.3 In particular and depending on the Services, TEAM IM may Process Personal Information for hosting and storage; backup and disaster recovery; service change management; issue resolution; applying new product or system versions, patches, updates and upgrades; monitoring and testing system use and performance; IT security purposes including incident management; maintenance and performance of technical support systems and IT infrastructure; and migration, implementation, configuration and performance testing.

2.4 As part of the provision of the Services and depending on the Services, TEAM IM may Process Personal Information about Your Individuals, including Your end users, employees, job applicants, contractors, collaborators, partners, suppliers, customers and clients.

2.5 Personal Information about Your Individuals may include, but is not limited to, personal contact information such as name, home address, home telephone or mobile number, fax number, email address, and passwords; information concerning family, lifestyle and social circumstances including age, date of birth, marital status, number of children and name(s) of spouse and/or children; employment details including employer name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, and business contact details; financial details; goods and services provided; unique IDs collected from mobile devices, network carriers or data providers; geolocation data; IP addresses and online behavior and interest data.

2.6 Unless otherwise specified in the Services Agreement, You may not provide TEAM IM with any data that imposes specific data security or data protection obligations on TEAM IM in addition to or different from those specified in the Data Processing Agreement or Services Agreement (e.g. certain regulated health or payment card information). If available for the Services, You may purchase additional services

from TEAM IM designed to address specific data security or data protection requirements applicable to sensitive or special data You seek to include in Your Content. You remain responsible for compliance with Your specific regulatory, legal or industry data security obligations which may apply to such data.

2.7 Additional or more specific descriptions of Processing activities may be included in the Services Agreement.

2.8 TEAM IM is a Service Provider in respect to Personal Information processed in performance of the Services. TEAM IM will not: (a) Sell or Share any Personal Information; (b) retain, use, or disclose any Personal Information (i) for any purpose other than for the Business Purposes specified in the Services Agreement, including for any Commercial Purpose, or (ii) outside of the direct business relationship between TEAM IM and You; or (c) combine Personal Information received from or on behalf of You with Personal Information received from or on behalf of any third party, or collected from TEAM IM's own interaction with Individuals, except to perform a Business Purpose that is permitted by Services Agreement. TEAM IM will notify You of its use of Subprocessors in accordance with Section 5 of this Data Protection Agreement; and ensure Subprocessors are subject to applicable written agreements per Section 5 of this Data Protection Agreement. The parties acknowledge that the Personal Information You disclose to TEAM IM is provided only for the limited and specified Business Purposes set forth in the Services Agreement. You may take such reasonable steps as may be necessary (a) to remediate TEAM IM's unauthorised use of Personal Information, and (b) to ensure that Personal Information is used in accordance with the terms of this Data Processing Agreement by exercising Your rights under Section 8 of this Data Processing Agreement.

3. Your Instructions

3.1 In addition to Your instructions incorporated into the Services Agreement, You may provide additional instructions in writing to TEAM IM with regard to Processing of Personal Information in accordance with Applicable Data Protection Law. TEAM IM will promptly comply with all such instructions to the extent necessary for TEAM IM to (i) comply with its Processor obligations under Applicable Data Protection Law; or (ii) assist You to comply with Your Controller obligations under Applicable Data Protection Law relevant to Your use of the Services.

3.2 TEAM IM will follow Your instructions at no additional cost to You and within the timeframes reasonably necessary for You to comply with your obligations under Applicable Data Protection Law. TEAM IM will immediately inform You if, in its opinion, Your instruction infringes Applicable Data Protection Law. TEAM IM is not responsible for providing legal advice to You.

3.3 To the extent TEAM IM expects to incur additional charges or fees not covered by the fees for Services payable under the Services Agreement, such as additional license or third-party contractor fees, it will promptly inform You thereof upon receiving Your instructions. Without prejudice to TEAM IM's obligation to comply with Your instructions, the parties will then negotiate in good faith with respect to any such charges or fees.

4. Privacy Inquiries and Requests from Individuals

4.1 If You receive a request or inquiry from an Individual related to Personal Information Processed by TEAM IM under the Services Agreement, including Individual requests to access, delete or erase, restrict, rectify, receive and transmit (data portability), block access to or object to Processing of specific Personal Information, You can securely access Your Services environment that holds Personal Information to address the request. Additional information on how to access the Services to address privacy requests or inquiries from Individuals is available in the applicable TEAM IM Product or Service Feature Guidance

documentation available on <https://docs.teamcloud.nz> (or other applicable primary support tool or support contact provided for the Services).

4.2 To the extent access to the Services is not available to You or otherwise not responsive to the request or inquiry, You can submit a “service request” via <https://support.teamcloud.nz> (or other applicable primary support tool or support contact provided for the Services, such as Your project manager) with detailed written instructions to TEAM IM on how to assist You with such request.

4.3 If TEAM IM directly receives any requests or inquiries from Individuals that have identified You as the Controller, it will promptly pass on such requests to You without responding to the Individual. Otherwise, TEAM IM will advise the Individual to identify and contact the relevant controller(s).

5. TEAM IM Affiliates and Third Party Subprocessors

5.1 You provide TEAM IM general written authorisation to engage TEAM IM Affiliates and Third Party Subprocessors as necessary to assist in the performance of the Services.

5.2 To the extent TEAM IM engages such Third Party Subprocessors and/or TEAM IM Affiliates, it requires that such entities are subject to the same level of data protection and security as TEAM IM under the terms of this Data Processing Agreement and Applicable Data Protection Law. You will be entitled, upon written request, to receive copies of the relevant privacy and security terms of TEAM IM's agreement with any Third Party Subprocessors and TEAM IM Affiliates that may Process Personal Information. TEAM IM remains responsible for the performance of the TEAM IM Affiliates' and Third-Party Subprocessors' obligations in compliance with the terms of the Services Agreement.

6. Security and Confidentiality

6.1 TEAM IM has implemented and will maintain appropriate technical and organisational security measures for the Processing of Personal Information designed to prevent accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Information. These security measures govern all areas of security applicable to the Services, including physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement and other security controls and measures.

6.2 All TEAM IM and TEAM IM Affiliates employees, and Third Party Subprocessors that Process Personal Information, are subject to appropriate written confidentiality arrangements, including confidentiality agreements, regular training on information protection, and compliance with TEAM IM policies concerning protection of confidential information.

7. Audit Rights and Assistance with Data Protection Impact Assessments

7.1 You may audit TEAM IM's compliance with its obligations under this Data Processing Agreement up to once per year, including inspections of the applicable Services data center facility that hosts Personal Information. In addition, to the extent required by Applicable Data Protection Law, You or Your Regulator may perform more frequent audits.

7.2 If You engage a third-party auditor, the third party must be mutually agreed to by You and TEAM IM (except if such third party is a Regulator). TEAM IM will not unreasonably withhold its consent to a third-party auditor requested by You. The third party must execute a written confidentiality agreement acceptable to TEAM IM or otherwise be bound by a statutory or legal confidentiality obligation.

7.3 To request an audit, You must submit a detailed proposed audit plan to TEAM IM at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. TEAM IM will review the proposed audit plan and provide You with any concerns or questions. TEAM IM will work cooperatively with You to agree on a final audit plan within a reasonable timeframe.

7.4 The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and TEAM IM's health and safety or other relevant policies, and may not unreasonably interfere with TEAM IM business activities.

7.5 Upon completion of the audit, You will provide TEAM IM with a copy of the audit report, which is subject to the confidentiality terms of Your Services Agreement. You may use the audit reports only for the purposes of meeting Your regulatory audit requirements and/or confirming compliance with the requirements of this Data Processing Agreement.

7.6 Each party will bear its own costs in relation to the audit, unless TEAM IM promptly informs you upon reviewing Your audit plan that it expects to incur additional charges or fees in the performance of the audit that are not covered by the fees payable under Your Services Agreement, such as additional license or third party contractor fees. The parties will negotiate in good faith with respect to any such charges or fees.

7.7 Without prejudice to the rights granted in Section 6.1 above, if the requested audit scope is addressed in a SOC, ISO, NIST, PCI DSS, HIPAA or similar audit report issued by a qualified third party auditor within the prior twelve months and TEAM IM provides such report to You confirming there are no known material changes in the controls audited, You agree to accept the findings presented in the third party audit report in lieu of requesting an audit of the same controls covered by the report.

7.8 You may also request that TEAM IM audit a Third Party Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist You in obtaining a third-party audit report concerning the Third Party Subprocessor's operations) to verify compliance with the Third Party Subprocessor's obligations.

7.9 TEAM IM provides You with information and assistance reasonably necessary for You to conduct Your data protection impact assessments or consult with Your Regulator(s), by granting You electronic access to a record of Processing activities and TEAM IM Product/Service privacy & security functionality guides for the Services.

8. Incident Management and Breach Notification

8.1 TEAM IM has implemented controls and policies designed to detect and promptly respond to incidents that create suspicion of or indicate destruction, loss, alteration, unauthorised disclosure or access to Your Content (as such term is defined in the Services Agreement) transmitted, stored or otherwise Processed. TEAM IM will promptly define escalation paths to investigate such incidents in order to confirm if an Information Breach has occurred, and to take reasonable measures designed to identify the root cause(s) of the Information Breach, mitigate any possible adverse effects and prevent a recurrence.

8.2 TEAM IM will notify you of a confirmed Information Breach without undue delay but at the latest within 24 hours. As information regarding the Information Breach is collected or otherwise reasonably becomes available to TEAM IM, TEAM IM will also provide You with (i) a description of the nature and reasonably anticipated consequences of the Information Breach; (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence; and (iii) where possible, information about the types of information that were the subject of the Information Breach. You agree to coordinate with TEAM IM on the

content of Your intended public statements or required notices for the affected Individuals and/or notices to the relevant Regulators regarding the Information Breach.

9. Return and Deletion of Personal Information

9.1 Upon termination of the Services, TEAM IM will promptly return, including by providing available data retrieval functionality, and subsequently delete any remaining copies of Personal Information on TEAM IM systems or Services environments, except as otherwise stated in the Services Agreement.

9.2 For Personal Information held on Your systems or environments, or for Services for which no data retrieval functionality is provided by TEAM IM as part of the Services, You are advised to take appropriate action to back up or otherwise store separately any Personal Information while the production Services environment is still active prior to termination.

10. Legal Requirements

10.1 TEAM IM may be required by law to provide access to Personal Information, such as to comply with a subpoena or other legal process, or to respond to government requests, including public and government authorities for national security and/or law enforcement purposes.

10.2 TEAM IM will promptly inform You of requests to provide access to Personal Information and use reasonable efforts to redirect the authority that made the request to You, unless otherwise required by law.

10.3 To the extent TEAM IM is required to respond to the request, it will first assess on a case-by-case basis whether the request is legally valid and binding on TEAM IM, including whether the request is consistent with Applicable Data Protection Law. Any request that is not legally valid and binding on TEAM IM will be resisted in accordance with applicable law.

11. Data Protection Officer

11.1 TEAM IM has appointed a Chief Privacy Officer. Further details on how to contact TEAM IM's Chief Privacy Officer and, where applicable, the local Data Protection Officer, are available [here](#).

11.2 If You have appointed a Data Protection Officer, You may request TEAM IM to include the contact details of Your Data Protection Officer in the relevant Services order.

12. Definitions

"Applicable Data Protection Law" means all data privacy or data protection laws of New Zealand or regulations that apply to the Processing of Personal Information under this Data Processing Agreement.

"Individual" shall have the same meaning as the term "data subject" or the equivalent term under Applicable Data Protection Law.

"Information Breach" means a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Your Content transmitted, stored or otherwise Processed on TEAM IM systems or the Services environment that compromises the security, confidentiality or integrity of Your Content.

“Process/Processing”, “Controller”, “Processor” and “Binding Corporate Rules” (or the equivalent terms) have the meaning set forth under Applicable Data Protection Law.

“TEAM IM Affiliate(s)” means the subsidiar(y)(ies) of TEAM IM that may Process Personal Information as set forth in this Data Processing Agreement.

“TEAM IM” means the TEAM IM Affiliate that has executed the Services Agreement.

“Personal Information” shall have the same meaning as the term “personal data”, “personally identifiable information (PII)” or the equivalent term under Applicable Data Protection Law.

“Regulator” shall have the same meaning as the term “supervisory authority”, “data protection authority” or the equivalent term under Applicable Data Protection Law.

“Services” or the equivalent terms “Service Offerings” or “services” means the Cloud, Advanced Customer Support, Consulting, or Global Technical Support services specified in the Services Agreement.