DATA PROCESSING AGREEMENT

Last modified: October 2, 2023

This IPRally Data Processing Agreement and its Annexes (hereinafter the "**Data Processing Agreement**" or "**DPA**") reflects the parties' agreement with respect to the Processing of Personal Data by

us, **IPRally Technologies Oy**, address: Mikonkatu 15 A, 00100 Helsinki, Finland, Business ID: 2901197-7, including its affiliates ("**IPRally**" or the "**Supplier**") as the Processor AND

you (the "**Customer**") as the Controller,

on behalf of you in connection with the IPRally service.

The Customer and the Supplier hereinafter each separately referred to as a "**Party**" and together as the "**Parties**."

1. SUBJECT AND PURPOSE

A) Unless otherwise expressly provided therein, or a separate written data processing agreement has been entered into between Parties, this DPA is applied to the processing of Personal Data under, and part of the Software as a Service agreement (the "**Agreement**") between Supplier and Customer. This DPA is part of the Agreement and prevails over any conflicting provisions of the Agreement concerning data processing.

B) The purpose of this DPA is to ensure the implementation of consistent data protection practices to be applied in the provision of services by the Supplier to the Customer. The Parties recognize and agree that well-managed data and privacy protection is a fundamental necessity of the Customer's operations. Furthermore, the Parties recognize and agree that proper data protection is required by applicable legislation.

2. DEFINITIONS

A) "**Controller**" shall mean, as defined in the Data Protection Laws, an entity which determines the purposes and means of the processing of Personal Data under this DPA.

B) "**Data Subject**" shall mean a person, as defined in the Data Protection Laws, whose Personal Data the Supplier processes under this DPA.

C) "**Data Protection Laws**" shall mean, without limitation and as applicable, all EU legislative acts related to protection of personal data as in force from time to time such as the EU General Data Protection Regulation (2016/679) (the "**GDPR**"), and all other applicable EU and national data protection, privacy, data security and data protection laws, regulations, rulings, regulatory guidance and other binding

restrictions of, or by, any judicial or administrative body, as in force from time to time and any amendments thereof.

D) "**Personal Data**" shall mean personal data as defined in the Data Protection Laws.

E) "**Processor**" shall mean, as defined in the Data Protection Laws, an entity which processes Personal Data on behalf of the Controller for the purposes specified in this DPA. For avoidance of doubt, it is noted that "processing" Personal Data refers to any operation, or set of operations, performed on Personal Data, as defined in the Data Protection Laws, including by collection, recording, organization, storage, adaptation or alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

The terms related to data protection which are not defined in this DPA, are used in accordance with the GDPR.

3. COMPLIANCE WITH LAWS AND CUSTOMER'S INSTRUCTIONS

A) The Parties agree, in the processing of Personal Data under this DPA, to comply with the Data Protection Laws. The Supplier shall, and shall procure that any subprocessors shall, process Personal Data only in accordance with the written instructions from the Customer, unless required to do so by applicable legislation to which the Supplier is subject; in such a case, the Supplier shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Should any future written instructions of the Customer go beyond the legally necessary, or if the Customer submits new instructions, the Supplier shall be entitled to a reasonable compensation in accordance with incurred costs, or as agreed between the Parties.

B) The Supplier shall not process the Personal Data for any other purposes than those necessary to provide the services to the Customer specified in the Agreement and this DPA (including any appendices) or fulfill other obligations under this DPA.

C) The Supplier shall notify the Customer if the Supplier cannot fulfil its obligations under this DPA or if the Supplier is of the view that an instruction regarding the processing of Personal Data would be in breach of the Data Protection Laws unless the Supplier is prohibited from notifying the Customer under any applicable legislation.

D) For the sake of clarity, it is stated that it is the Customer's responsibility to ensure, as the Controller, that the Customer has the right to disclose or otherwise give access to the Personal Data to the Supplier and the Supplier's personnel based on the applicable legislation.

4. PROCESSING PERSONAL DATA OUTSIDE THE EU/EEA

The Supplier shall not transfer Personal Data to a country outside the EU/EEA or otherwise process Personal Data in a country outside the EU/EEA without prior written

authorization of the Customer. If Personal Data is transferred outside the EU/EEA, there must be appropriate safeguards in place for the transfer, such as the EU Commission standard contractual clauses for international transfers (SCCs). The Supplier shall, upon request, provide evidence of these safeguards to the Customer.

5. CONFIDENTIALITY

The Supplier, and people working under the Supplier, shall keep the Personal Data received from the Customer confidential and ensure that only authorized persons can access the Personal Data for processing. The Supplier shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6. DELETION OR RETURN OF PERSONAL DATA

Upon termination or expiry of the Agreement, the Supplier shall delete or return to the Customer within a reasonable time all Personal Data processed on behalf of the Customer and delete existing copies, unless the applicable legislation/regulation requires to store the Personal Data.

7. SUBPROCESSORS

A) The Supplier may engage subprocessor(s) to process Personal Data, provided that:

i) such engagement will be under a written contract or terms; and
ii) the contract or terms will require the subprocessor(s) to comply with similar obligations applicable to the Supplier under this DPA and the Data Protection Laws.

B) Upon written request, the Supplier will inform the Customer of the subprocessors it uses and about any subsequent change of subprocessors. For a justified reason, the Customer has the right to object to the use of a new subprocessor within fourteen (14) days of the Supplier's notification. Objection must be notified in writing to the Supplier. If the Parties cannot reach an agreement on using a new subprocessor, both Parties have the right to terminate the Agreement by giving a thirty (30) days' prior written notice.

C) In any event, the Supplier will remain fully liable for the acts and omissions of its subprocessors towards the Customer.

8. SECURITY OF DATA PROCESSING

A) The Supplier shall implement and use its reasonable efforts to maintain appropriate technical and organizational measures to protect the Personal Data against accidental, unauthorized or unlawful destruction, loss, alteration, disclosure or access so that the processing is in compliance with the Data Protection Laws and the Customer's written instructions.

B) The Supplier shall implement at least the following measures as appropriate:

i) the pseudonymization and encryption of Personal Data;
ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

9. DATA BREACHES

A) In the event of data breach, the Supplier shall notify the Customer without undue delay upon the Supplier becoming aware of the data breach affecting Personal Data, to the extent that the Data Protection Laws requires such notification.

B) Upon the Customer's request, the Supplier shall provide the Customer with reasonably detailed written notice of its discovery of any data breach. The data breach notification shall contain the following:

i) description of the nature of the data breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
ii) the name and contact details of the contact point where more information can be obtained;
iii) description of the likely consequences of the data breach;
iv) description of the measures taken or proposed to be taken by the Supplier to address data breach, including, where appropriate, measures to mitigate its possible adverse effects.

C) The Supplier shall co-operate with the Customer and take reasonable commercial steps as are directed by the Customer to assist in the investigation, mitigation and remediation of each such data breach.

10. RIGHT TO AUDIT

A) The Customer or a third-party auditor mandated by the Customer, shall have the right to audit the processing activities of the Supplier under this DPA to examine the level of protection and security provided for Personal Data processed under this DPA. Such third-party auditor must not be a competitor of the Supplier.

B) The Customer may audit the Supplier's compliance with this DPA no more than once a year. The Customer may request more frequent audits if required by the legislation applicable to the Customer.

C) The audit timetable, method and scope shall be agreed beforehand between the Parties and the audit shall not unduly interfere with the Supplier’s business operations.

D) The Customer shall be responsible for all costs of the audits it requests. The Supplier has the right to charge the Customer for assistance provided in connection with the audit.

11. OBLIGATION TO ASSIST

A) Taking into account the nature of the processing, the Supplier shall assist the Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests to exercise Data Subjects' rights under the Data Protection Laws.

B) If requested by the Customer in order for the Customer to comply with the Data Protection Laws, the Supplier shall provide relevant information and reasonable assistance to the Customer to meet its reporting obligations and other obligation under the Data Protection Laws, taking into account the nature of processing and the information available to the Supplier. Such other obligations may include data protection impact assessment and supervisory authority's prior consultations.

C) The Supplier is entitled to charge the Customer for the costs for assisting with the above, if the content of the requests deviates from the standard information or assistance provided by the Supplier under the Data Protection Laws and results in additional work for the Supplier.

12. LIABILITY

A) The limitations of liability and liability cap(s) agreed between the Parties in the Agreement shall apply to the Supplier's liability arising under or in connection with this DPA. In case the Parties have not agreed on a liability cap applicable to the Supplier's liability arising under or in connection with this DPA elsewhere, the Supplier's total aggregate liability arising under or in connection with this DPA shall not exceed the fees paid by the Customer to the Supplier under the Agreement during a period of twelve (12) months immediately preceding the event giving rise to the claim.

B) However, neither Party shall under any circumstances be liable for any indirect, consequential or special damages incurred by the other Party arising under or in connection with this DPA.

C) The limitations of liability under this section 12 (Liability) shall not apply to damages caused by willful misconduct or gross negligence.

D) Each Party is responsible for the administrative fines which the supervisory authority has imposed to the Party in question, and which result from that Party's infringement of the Data Protection Laws.

13. DURATION OF OBLIGATIONS UNDER THIS DPA

This DPA shall remain in force for as long as the Supplier process the Personal Data on behalf of the Customer in order to provide the services under the Agreement and

for such period thereafter as is necessary for the activities to be complete, including but not limited to, the return of Personal Data to the Customer and the deletion of Personal Data, or, if longer, as may be required by any applicable law.

14. GOVERNING LAW AND DISPUTE RESOLUTION

The terms of the Agreement shall apply herein.

15. MISCELLANEOUS

A) This DPA (including appendices) constitutes the entire agreement between the Parties and replaces any prior agreements and understandings, oral and written, between the Parties on the processing of Personal Data.

B) If any provision of this DPA shall be found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, so far as permissible, such unenforceability or invalidity shall not affect the other provisions of this DPA, which shall remain in full force and effect.

C) IPRally may change the content of this Agreement, subject to posting a notice of change in its web page.

D) The appendices listed here below shall form an integral part of the DPA.

16. APPENDICES

Annex A: Description of the Processing of Personal Data
Annex B: List of subprocessors

ANNEX A: Description of the processing of Personal Data

Last modified: October 2, 2023

The Supplier performs services to the Customer that will include processing of Personal Data by Supplier as further specified below with respect to: (a) the nature and purpose of the processing of Personal Data; (b) the type of Personal Data and categories of Data Subjects; (c) the applicable security measures; (d) duration of the processing, as further agreed below.

(a) Nature and purpose of the processing of Personal Data

The Supplier processes personal data on behalf of the Customer in relation to the Supplier's services relating to its Software as a Service (SaaS) application according to the Agreement insofar as the services require processing of personal data.

(b) Type of Personal Data and categories of Data Subjects

The type of personal data is data subjects' contact information such as name and email address. The categories of data subjects are the Customer's named users of the Supplier's Software as a Service (SaaS) application, such as Customer's employees or contractors.

(c) Applicable security measures

The information security instructions are set out in Section 8 (Security of Data Processing) of this DPA.

(d) Duration of the processing of Personal Data

The Supplier processes personal data on behalf of the Customer during the term of the Service Agreement and after termination for the actions required after termination of the Agreement under the Agreement, its attachments, this DPA and its annexes.

ANNEX B: List of subprocessors

Last modified: January 24, 2025

Name	Address	Subject/purpose and location of processing	Data processed
Okta, Inc	San Fransisco, California, USA	Auth0 Authentication and Access management for the application Location of processing: EU	name, e-mail
Google Cloud EMEA Limited	Dublin, Ireland	Main cloud provider Location of processing: EU	name, e-mail
Hubspot Inc	Cambridge, Massachusetts, USA	Cloud service used for CRM and customer communications Location of processing: EU	name, e-mail
Intercom, Inc	San Fransisco, California, USA	Customer support and communications platform Location of processing: US	name, e-mail
Planhat AB	Sweden	Customer success platform Location of processing: EU	name, e-mail
Mailgun, Inc	San Antonio, Texas, USA	Transactional e-mails for customer communications from the application Location of processing: EU	name, e-mail
Zapier, Inc	San Fransisco, California, USA	Message relaying between the application and subprocessors Location of processing: US	name, e-mail
Slack Technologies Limited	Dublin, Ireland	User onboarding and support notifications Location of processing: US	name, e-mail
Pendo.io, Inc	Raleigh, North Carolina, USA	Customer success and analytics platform Location of processing: EU	name, e-mail