Data Processing Agreement

1. Parties

1. The Company AB, company reg. no XXXXXX-XXXX, at The Street 17, 11160 The City, referred to below as "**Data Controller**"; and

2. Rule Communication – Nordic AB, company reg. No. 556740-1293, at Kammakargatan 48, 111 60 Stockholm, referred to below as "**Data Processor**".

3. The Data Controller and the Data Processor are individually referred to as "the **Party**", and together as "**the Parties**".

2. Background and Purpose

2.1 Regarding Data Protection Regulation, a written agreement is required that regulates under which circumstances and terms a data processor can process personal data on behalf of a data controller.

2.2 The Parties have entered into an agreement concerning the service Rule ("the Principal Agreement"), that means that the Data Processor will process personal data on behalf of the Data Controller. If provisions of the Agreement ("the Agreement") are in conflict with the Principal Agreement, the provisions of the Agreement shall have priority.

2.3 The Data Controller hereby commissions the Data Processor to store personal data from digital marketing, web traffic etc. and to communicate the results of these to the Data Controller. The Data Processor can gather the personal data in the following ways:

Digital Communication

The Data Processor saves all the information surrounding the digital communication from the Data Controller's account in Rule and stores all the information regarding the visitor's email address, mobile phone number, profile, geographical position, user-agent, time and clicks.

Forms Published from Rule

It is also possible for the Data Controller, to via Rule create their own forms ("Widgets") that are displayed on the website. These can be used to gather personal data.

Import or Manually Submit Personal Data

The Data Controller can independently, or with the help of the Data Processor, import personal data into the Rules data base. This can happen indirectly, via the website, through digital communication, by importing data directly in the Rules interface or via API. The Data Controller can also choose to activate add-ons for integrations with other systems (email, CRM, event systems etc.). These integrations can supply Rule with personal data.

2.4 In Rule, the Data Controller can perform a match between subscription/member bases with the purpose of identifying behaviours.

2.5 The purpose of this match is to be able to direct more relevant digital communication to the subscriber/member and to offer the subscribers/members who can be identified, a more tailored offer. Rule will therefore, as part of this matching assignment, process personal data on behalf of the Data Controller.

2.6 The protection of the integrity of the Data Controller's clients is of great ethical and commercial importance to the Data Controller, therefore the Data Processor shall process the Personal Data in accordance with this Agreement, applicable law, regulations and industry standards.

3. Definitions

3.1 "Personal Data" below, refers to all kinds of data that directly or indirectly can be attributed to a natural person who is alive and, by using the Rule service, is processed on behalf of the Data Controller.

3.2 “Registered” below, refers to the person whom the Personal Data concerns.

3.3 ”Processing” below, refers to every measure or series of measures that is taken when it comes to Personal Data, whether it takes place automatically or not, e.g.

collection, registration, organizing, storing, editing or changing, recycling, acquisition, use, disclosure by transmission, spread or other provision of data, compilation or cross referencing, blocking, erasure or destruction.

3.4 “Data Protection Regulation” refers to the European Parliament and the Council’s Regulation (EU) 2016/679 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), also called GDPR. “Data Protection Regulation” also refers to additional national legislation, regulations, and general guidelines from the supervisory authority (the Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten)) and EU organisations as well as indicative rulings from the Swedish Court and the European Court of Justice.

4. The Data Processor’s Obligations

4.1 The purpose of the Agreement is for the Data Processor to ensure that the Processing of Personal Data takes place in accordance with the Data Protection Regulation and applicable regulations and industry standards.

4.2 The Data Processor and the person or persons who work under his/her guidance may only Process Personal Data in accordance with the instructions, that from time to time are supplied by the Data Controller.

4.3 The Data Processor may only collect Personal Data in accordance with the instructions issued by the Data Controller. As the Data Processor only delivers the tools for the collection of Personal Data it is the Data Controller’s responsibility to ensure that the processing takes place on legal grounds, e.g. that the necessary consents have been acquired by the Registered and that the Registered obtain information in accordance with the Data Regulations requirements. The Data Processor shall upon request from

the Data Controller without delay submit the data that the Data Controller needs to be able to show that the Registered have been informed, in those cases where the Data Processor holds this data.

4.4 The Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR, including, inter alia, encryption, measures ensuring confidentiality, integrity and availability, as well as procedures for incident management and regular testing of the effectiveness of the measures.

4.5 In the event of the Registered, the Swedish Authority for Privacy Protection or other third party requesting information from the Data Processor regarding the Processing of Personal Data, the Data Processor shall refer to the Data Controller. The Data Processor may not disclose Personal Data or other information regarding the Processing of Personal Data without express instructions from the Data Controller.

4.6 The Data Controller has the right to, at his/her own expense or via third party, monitor that the Data Processor is following the Agreement. The Data Processor shall enable and contribute to reviews, including inspections, that are conducted by the Data Controller or other auditors that have been authorized by the Data Controller.

4.7 When the Agreement expires the Data Processor shall make the Personal Data available to the Data Controller via the Rule service and, when the Data Controller has notified the Data Processor that the Personal Data has been collected, he/she shall in writing request the Personal Data be erased. The Data Processor shall in every event, 30 days at the latest after the expiration of the Agreement make sure that there is no Personal Data remaining with the Data Processor, unless otherwise is agreed upon by the Data Processor and the Data Controller.

4.8 The Data Processor shall upon finding out about a personal data breach, that includes the Data Controller's Personal Data, without any unnecessary delay, notify the Data Controller about the breach. The notification shall include the information necessary for the Data Controller to be able to fulfil his/her obligations according to the Data Protection Regulation to report the personal data breach to the supervisory authority as well as notifying the Registered about the personal data breach. Such a

notification shall be given to the person of contact, assigned by the Data Controller, to be in contact with the Data Processor.

4.9 Unless otherwise provided in section 7.3, the Data Processor shall ensure that the Personal Data is not Processed outside the EU/EEA.

4.10 The Data Processor shall when necessary help the Data Controller with the execution of a data protection impact assessment as well as any prior consultations with the supervisory authority.

5. Confidentiality

5.1 The Data Processor agrees not to disclose or in any other way reveal to any third party information regarding Processing of Personal Data that is included in the Agreement or any other information that the Data Processor has acquired in connection with the Agreement. The Data Processor also agrees not to use the Personal Data for his/her own purposes.

5.2 The undertaking in the first sentence of paragraph 5.1 does not apply to a) information that a party can show was publicly known at the time of receipt, or b) information that a party is ordered to provide to an authority. The confidentiality undertaking also applies after the Agreement in other respects has expired.

5.3 The Data Processor shall ensure that all natural persons working under its authority who take part in the Processing are bound by a confidentiality undertaking regarding the Processing. This is not required if they are already subject to a statutory duty of confidentiality under penalty of law. The Data Processor further undertakes to ensure that a confidentiality agreement is in place with each sub-processor, as well as confidentiality undertakings between the sub-processor and all natural persons working under its authority who take part in the Processing.

6. Intellectual Property Rights Etc.

6.1 All intellectual property rights for the collection of Personal Data belong to the Data Controller and the Data Controller provides only a non-exclusive right for the Data Processor to use the Personal Data for the execution of assignments according to the Agreement.

7. The Hiring of Sub-Processors

7.1 If the Data Processor, with the permission of the Data Controller, transfers its obligations according to the Agreement to a sub-processor, this may only happen by entering into a written agreement with the sub-contractor, whereby the same obligations that, according to the Agreement are imposed on the Data Processor, will be imposed on the sub-processor.

7.2 The Data Processor shall notify the Data Controller in writing regarding the intention to sign an agreement with a sub-contractor. If the Data Controller does not submit a

written objection to this, that is objectively justified, within 14 days of receipt of the notification, the Data Processor is free to hire the sub-processor. At the time of the signing of the Agreement, the sub-processors that appear in Appendix 1 are approved by the Data Controller.

7.3 Where Processing of Personal Data is to be performed by a sub-processor in a third country, the Data Controller authorises the Data Processor to take, on behalf of the Data Controller, the measures necessary to ensure a lawful basis for such transfer, in the following order of priority:

a) USA, DPF-certified sub-processor: If the sub-processor is established in the United States and, at the time of the transfer, is certified under the EU-U.S. Data Privacy Framework (“DPF”) pursuant to the European Commission’s adequacy decision for the DPF (Commission Implementing Decision (EU) 2023/1795), the transfer may take place on the basis of that adequacy decision, without any further transfer mechanism under b) below.

b) Other third countries, or the USA without valid DPF certification: In all other cases, including where the sub-processor is established in the United States but is not, or ceases to be, DPF-certified, or where the DPF decision under a) is annulled, revoked or

otherwise ceases to be valid, the Data Processor shall enter into a data processing agreement with the sub-processor based on the European Commission's standard contractual clauses for the transfer of personal data to third countries, as applicable from time to time.

In all cases, the Data Processor shall inform the Data Controller of the country in which the Processing takes place and which transfer basis under a) or b) applies. The requirements of Chapter V GDPR shall also be met at all times. The Data Processor shall inform the Data Controller without delay if a sub-processor's DPF certification ceases, or if the DPF decision is challenged in a way that materially affects the lawfulness of the transfer, so that the transition to the mechanism under b) can be ensured.

7.4 If the sub-processor does not meet the obligations regarding Processing, according to the sub-processing agreement, the Data Processor shall remain fully responsible towards the Data Controller for the sub-processor's fulfilment of his/her obligations according to the Agreement.

8. Financial Compensation

8.1 The Data Processor is not entitled to any particular financial compensation for the Processing of Personal Data according to the Agreement.

9. Limitation of Liability

9.1 In the event of the Registered, or other third-party directing claims against the Data Controller due to the Data Processor's Processing of Personal Data, the Data Controller shall report this to the Data Processor.

9.2 If the Data Processor has failed to fulfil his/her undertaking according to the Agreement, the Data Controller has the right to be compensated. The Data Processor's responsibility to the Data Controller under the Agreement is limited to 50% of the payment received, according to the Principal Agreement, from the Data Controller during the 12-month period preceding the notification.

10. Force Majeure

10.1 None of the parties are responsible for damages or delays arisen due to labour disputes, official decisions or other circumstances beyond the control of the parties.

11. Agreement Period

11.1 The agreement is valid from the date of signature and for as long as the Data Processor Processes the Personal Data according to the Principal Agreement.

12. Applicable Law and Dispute Resolution

12.1 The Agreement and all Processing of personal data that takes place within the Agreement is regulated by Swedish law, with the exception for applicable choice of law rules. Disputes regarding interpretation or application of the Agreement shall be settled according to the Principal Agreement's dispute resolution provisions.

This agreement has been drawn up in two copies, of which the parties have received one each.

Stockholm 2026- Stockholm 2026-

_____ _____

Sam Jahanfar Data Controller
Rule Communication – Nordic AB

Rule Communication – Nordic AB ▪ Kammakargatan 48 ▪ 111 60 Stockholm
Company reg. no: 556740-1293 ▪ Telephone: +46 8 5250 7580 ▪ Email: info@rule.se
v2026_2