relation & brand

Personal Data Processor Agreement

This personal data processor agreement (the "**Data Processor Agreement**") was on this day entered into between:

(1) The user of an eGenerator account (the "**Customer**") and

(2) Relation & Brand AB, company reg. no. 556573-6500, Stora Nygatan 33, SE-111 27 Stockholm (the "**Supplier**"),

each individually referred to as a "**Party**" and collectively as the "**Parties**".

1 CONTENTS AND PURPOSE

1.1 An agreement has been signed (the "**Service Agreement**") between the Customer and the Supplier in respect of the services which the Supplier shall provide to the Customer in its capacity as data processor. The agreed services entail the processing of personal data by the Supplier on behalf of the Customer, to an extent regulated by the Service Agreement and the Data Processor Agreement.

1.2 In accordance with Applicable Data Protection Law (see sub-clause 2.5 below), any processing of personal data performed by a data processor on behalf of a data controller shall be regulated by an agreement. For this reason, the Parties have entered into the Data Processor Agreement.

1.3 The purpose of the Data Processor Agreement is to ensure that any processing of personal data by the Supplier on the Customer's behalf is done in accordance with Applicable Data Protection Law, official decisions and the Customer's instructions.

1.4 The Data Processor Agreement constitutes an Appendix to the Service Agreement. In the event of any contradictory provisions, the Data Processor Agreement shall take priority.

2 DEFINITIONS

2.1 "Personal Data" below means all types of information that, directly or indirectly, can be attributed to a living natural person and that is processed on the Customer's behalf.

2.2 "Data Subject" means the natural person to whom the Personal Data relates.

2.3 "Processing" or "Process" refers to any action or combination of actions relating to Personal Data, whether performed automatically or not, such as collection, registration, organisation, structuring, storage, adaptation or modification, production, reading, use, distribution through transfer, dissemination or provision in some other way, adjustment or collation, restriction, erasure or destruction.

2.4 "Sub-Processor" means a natural person or legal entity, authority or other body engaged by the Supplier for the Processing of Personal Data.

2.5 "Applicable Data Protection Law" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (the General Data Protection Regulation or GDPR) and associated implementation statutes, as well as all other legislation (including regulations and provisions) that applies to the Processing of Personal Data, as this may be amended over time.

2.6 Terms and expressions relating to personal data and the processing of personal data which are spelled with an initial lower-case letter, e.g. "data controller", "data processor", "personal data incident", etc., shall be given the meaning indicated in Applicable Data Protection Law.

3 CUSTOMER'S RESPONSIBILITIES

3.1 In its capacity as data controller, the Customer is responsible for ensuring that the Processing of Personal Data is done in accordance with Applicable Data Protection Law.

3.2 The Customer undertakes to draw up written instructions so that the Supplier and any Sub-Processors shall be able to conduct their task in accordance with the Data Processor Agreement. The Customer's instructions to the Supplier in respect of the nature and purpose of the Processing, its duration, the type of Personal Data and the categories of Data Subjects can be found in the Appendix "Instructions for the Processing of Personal Data".

3.3 The Customer undertakes to inform the Supplier without delay of any changes to the Processing of Personal Data that affect the Supplier's obligations under Applicable Data Protection Law or other relevant legislation.

3.4 The Data Processor Agreement, including the Appendix "Instructions for the Processing of Personal Data", constitutes all of the Customer's instructions for the Processing of Personal Data under the Data Processor Agreement, except for any instructions in writing that the Customer has a duty to provide during the term of the agreement in order to comply with Applicable Data Protection Law. Any other changes shall be agreed separately. All changes to the Appendix "Instructions for the Processing of Personal Data" shall be documented.

4 SUPPLIER'S UNDERTAKINGS

4.1 The Supplier, and each person authorised to perform work on its behalf, undertakes to Process Personal Data on behalf of the Customer only in accordance with the Data Processor Agreement, the Service Agreement and any documented instructions from the Customer applicable at the time.

4.2 When Processing Personal Data, the Supplier shall comply with Applicable Data Protection Law and the pronouncements and recommendations of the authorised supervisory authority.

4.3 The Supplier shall inform the Customer without delay if the Supplier has inadequate or incorrect instructions regarding the Supplier's Processing of Personal Data, or if the Supplier suspects or discovers that the Customer's instructions are in breach of Applicable Data Protection Law.

5 SECURITY

5.1 When Processing Personal Data, the Supplier shall take all suitable technical and organisational measures to ensure that the level of security is appropriate with regard to the risk, and to protect Personal Data from unauthorised or unlawful processing, unintentional or unlawful loss,

destruction or modification, or the unauthorised disclosure of or access to such Personal Data ("Security Measures"). In all circumstances, the Supplier shall take such Security Measures as shown in the Appendix "Instructions for the Processing of Personal Data".

5.2 The Customer is responsible for ensuring that the Security Measures agreed in sub-clause 5.1 above meet the Customer's obligations under Applicable Data Protection Law in respect of the requirement for security in connection with the Processing of Personal Data.

5.3 If the Supplier discovers that the Security Measures in accordance with sub-clause 5.1 above are in full or partial breach of Applicable Data Protection Law, the Supplier shall – within a reasonable time – notify the Customer of its view and await instructions in writing from the Customer.

6 PERSONAL DATA INCIDENTS

6.1 The Supplier shall notify the Customer without undue delay in the event of any suspected or noted personal data incident that may lead to the unintentional or unlawful destruction, loss or modification, or to the unauthorised disclosure of or unauthorised access to, Personal Data.

6.2 Taking into account the type of processing and the information to which the Supplier has access, such notification shall:

a) describe the nature of the personal data incident and, where possible, the categories and approximate number of Data Subjects affected, as well as the categories and approximate number of personal data entries affected;

b) indicate the name and contact details of the data protection officer, or of other contact points where more information may be obtained;

c) describe the probable consequences of the personal data incident; and

d) describe the measures taken, or the measures that should be taken, in order to deal with the personal data incident or to alleviate its potential negative effects.

6.3 If and insofar as it is not possible to provide the information at the same time, the information may be provided in batches provided there is no undue further delay.

7 SUB-PROCESSORS

7.1 The Supplier is entitled to engage a Sub-Processor to conduct the Supplier's undertakings under the Data Processor Agreement, provided that:

a) the Supplier informs the Customer of its intentions to replace or engage a new Sub-Processor, upon which the Customer will be entitled to object to such a change; and

b) the Supplier ensures that the Sub-Processor is bound by an agreement in writing that imposes on the Sub-Processor the same obligations when Processing the Personal Data as those that apply according to the Data Processor Agreement.

The Supplier's obligation to inform the Customer under sub-clause 7.1 here is met by the Supplier providing information on the website [www.relationbrand.com/dataskydd/underbitraden]

and, at the time that new information is placed on the website, the Customer will notify this by e-mail. By signing the Data Processor Agreement, the Customer accepts the Sub-Processors published on the website [www.relationbrand.com/dataskydd/underbitraden] on the date of the agreement.

7.2 If the Sub-Processor fails to meet its obligations in a matter relating to the Processing of Personal Data in accordance with the sub-processor agreement, the Supplier shall remain fully liable to the Customer for the Sub-Processor's performance of the Sub-Processor's obligations in accordance with the Data Processor Agreement and Applicable Data Protection Law.

7.3 If the Customer wishes to make use of its right under sub-clause 7.1 above to object to a proposed new Sub-Processor, the Customer shall notify the Customer of this in writing within thirty (30) days of receiving notification from the Supplier. If, despite the Customer's objection, the Supplier still wishes to replace or engage a new Sub-Processor, the Customer shall be entitled to give written notice of termination of the Service Agreement within thirty (30) days of the Supplier's notification thereof. The Supplier shall then reimburse any fees paid for the period following the expiry of the notice of termination.

7.4 If the Customer has legitimate grounds for its objection, the Supplier may not engage the new Sub-Processor for the Processing of Personal Data during the Customer's period of notice of termination. If the Customer does not have legitimate grounds for its objection, the Customer's notice of termination shall be deemed to be a premature notice of termination without grounds, in which case the Customer shall pay compensation as shown in the Service Agreement for notice of termination of this kind. As far as this clause is concerned, "legitimate grounds" means circumstances on the part of the Sub-Processor that to a significant extent affect, or probably risk affecting, the protection of the personal integrity of Data Subjects, such that the new Sub-Processor does not meet the requirements of a data processor as stipulated in Applicable Data Protection Law.

7.5 The Supplier shall ensure that the Customer is aware of which Sub-Processors are Processing Personal Data by – at the Customer's request – providing full, correct and up-to-date information about all Sub-Processors, in which the following information is specified for each individual Sub-Processor:

a) definition of the Sub-Processor, including its contact details, company form and geographical location;

b) what type of service the Sub-Processor performs;

c) guarantees set up in order that the requirements of Applicable Data Protection Law are complied with; and

d) where the Sub-Processor Processes Personal Data that is covered by the Data Processor Agreement.

8 TRANSFERS TO THIRD PARTY COUNTRIES

8.1 The Supplier may, either by itself or through a Sub-Processor, Process Personal Data in a third-party country.

8.2 If the Supplier will be Processing Personal Data in a third-party country, the Supplier shall first:

a) investigate whether or not the third-party country provides an adequate level of security for personal data in accordance with a ruling notified by the EU commission, in which case Personal Data may be transferred to that third-party country; or, where no such ruling is in place,

b) ensure that suitable protective measures are in place in accordance with Applicable Data Protection Law, e.g. standardised data protection provisions approved by the EU commission or binding company regulations that include the Processing of Personal Data.

8.3 If the Processing of Personal Data in a third-party country requires entry into a separate agreement based on standardised data protection regulations, the Supplier – irrespective of whether it is the Supplier or a Sub-Processor who shall be entering into the agreement – is entitled to sign such an agreement on the Customer's behalf.

9 CONFIDENTIALITY

9.1 When Processing Personal Data, the Supplier and those working under the direction of the Supplier, shall observe confidentiality, which covers both document secrecy and the duty of confidentiality.

9.2 The Supplier undertakes to ensure that all persons authorised to Process Personal Data shall either subscribe to an individual confidentiality undertaking or be informed that a duty of confidentiality applies by law or agreement.

9.3 The Supplier's confidentiality undertaking will also apply after the Data Processor Agreement has ceased to be in force, without limit of time.

10 DUTY TO SUPPORT THE CUSTOMER

10.1 In addition to the provisions of clause 5 above, the Supplier shall implement appropriate technical and organisational measures in order to assist – at the Customer's written request – the Customer in complying with the rights of Data Subjects under Chapter 3 of the General Data Protection Regulation, such as transparency and terms and conditions. information and access to Personal Data, rectification and erasure, as well as the right to object and automated individual decision-making. The Supplier's obligation under this clause shall apply only insofar as this is possible, and to the extent required by the nature of the Processing.

10.2 Taking into account the type of Processing and the information to which the Supplier has access, the Supplier shall be obliged – at the Customer's written request – to support the Customer in meeting the obligations of the Customer with regard to security, personal data incidents, impact assessments regarding data protection, and advance consultation with the authorised supervisory authority in accordance with Applicable Data Protection Law.

11 ISSUING OF PERSONAL DATA

11.1 The Supplier shall not issue or otherwise disclose Personal Data to any Data Subject or third party unless required to do so by the Service Agreement or by law, or by a ruling by a court or official authority. In cases where the Supplier is obliged to issue such information by law, or due to a ruling by a court or official authority, the Supplier – save where this is prohibited by current law, or by a ruling by a court or official authority – shall notify the Customer thereof.

11.2 The Supplier shall, without undue delay, inform the Customer if a Data Subject requests information relating to its Processing of Personal Data, or else refer the Data Subject to the Customer. In accordance with sub-clause 10.1 above, the Supplier shall provide support to the Customer in responding to such an enquiry.

11.3 According to Applicable Data Protection Law, the Supplier and its representatives have an obligation to cooperate with an authorised supervisory authority with regard to any supervisory measures, if requested to do so by the authorised supervisory authority. The Supplier shall, without undue delay, inform the Customer of any contacts with the authorised supervisory authority or any other authority that affect, or may be important to, the Supplier's Processing of Personal Data. The Supplier is not entitled to represent the Customer, or to act on the Customer's behalf, with such enquiries.

12 AUDITING

12.1 In addition to what is stipulated in the Service Agreement, the Supplier shall provide the Customer with access to all information required to demonstrate that the obligations in respect of requirements on data processors under Applicable Data Protection Law have been complied with, as well as facilitating and contributing to audits – including inspections – conducted by the Customer or by an auditor appointed by the Customer. In the event of the Customer wishing to perform an inspection, the Customer shall inform the Supplier of this in reasonable time in advance, and shall at the same time specify the content and scope of the inspection. Inspections may only be conducted if an audit in accordance with Applicable Data Protection Law cannot be completed through the provision of information by the Supplier.

12.2 An audit in accordance with sub-clause 12.1 above requires the Customer, or an auditor appointed by the Customer, to have agreed to the necessary confidentiality undertakings and to comply with the Supplier's security regulations on the site at which the inspection is to take place, as well as for the inspection to be conducted without risk of interfering with the Supplier's operation or the protection of other customers' information. Information gathered as part of the audit shall be erased once the inspection is complete, or once it is no longer required for the purpose of the audit.

13 PAYMENT

13.1 Other than as stated in the Service Agreement, the Supplier is not entitled to any special payment for meeting its obligation under the Data Processor Agreement or Applicable Data Protection Law.

14 LIABILITY FOR DAMAGE

14.1 A Party's liabilities and entitlement to payment for damage claims from a Data Subject are regulated in accordance with Article 82 of the General Data Protection Regulation. Each Party is also entitled to receive reasonable and proportionate payment for the costs of any legal action to defend itself against a Data Subject's claim. The Supplier's total liability under the Data Processor Agreement in accordance with this sub-clause 14.1 is limited to an amount equivalent to the annual fee that the Customer has paid, or will pay, under the Service Agreement.

14.2 A Party must lodge a claim for damages to a counterparty under this clause 14 by no later than six (6) months from the time at which the Party became liable for damages to the Data Subject.

15 CHANGES TO THE AGREEMENT

15.1 In order to have binding effect, any changes or additions to the Data Processor Agreement shall be framed in writing and authorised signatures from the Parties provided.

16 TERM OF THE AGREEMENT AND ACTIONS ON EXPIRY OF THE AGREEMENT

16.1 The Data Processor Agreement enters in force after having been signed by both Parties, and shall thereafter apply for as long as the Supplier Processes Personal Data under the Service Agreement.

16.2 On expiry of the Service Agreement, at the Customer's request – which must be lodged within thirty (30) days of the expiry of the Service Agreement – the Supplier shall, at the Customer's option, either erase or promptly return all Personal Data to the Customer or to a person or entity designated by the Customer. At the end of the period indicated above, and unless otherwise required by law, the Supplier may erase any existing Personal Data. Following transfer of the Customer's Personal Data, or, where no transfer has been requested by the customer at the end of the period indicated in the preceding paragraph, the Supplier shall erase the Customer's Personal Data within a reasonable time, though by no later than six (6) months following expiry of the Service Agreement. After expiry of the Service Agreement, the Supplier may not Process Personal Data for any purposes other than to erase the Personal Data, unless otherwise stipulated by law.

16.3 If requested to do so, the Supplier shall provide written notification of the actions taken at the time of expiry of the Service Agreement, or confirm that the Supplier has taken the actions required in order to comply with this clause 16.

17 APPLICABLE LAW AND DISPUTES

17.1 Swedish law applies to the interpretation and application of the Data Processor Agreement.

17.2 Any disputes arising from the Data Processor Agreement shall be decided by an ordinary Swedish court of law.

Two (2) copies of the Data Processor Agreement have been produced, with each Party taking its own.

On behalf of the Customer	On behalf of the Supplier
[Name]	Relation & Brand AB
[Place and date]	Stockholm 2018-05-21
.....	.....
[Signature]	
.....	.....
[Name in block letters]	Nichlas Spångberg

Appendix: Instructions for the Processing of Personal Data

1 DESCRIPTION OF PROCESSING

1.1 Subject of the processing

The subject of the Processing is the Personal Data that the Supplier processes on behalf of the Customer in conjunction with its fulfilment of the Service Agreement.

1.2 Purpose of the processing

The Supplier Processes Personal Data for the purpose of providing and delivering the service to the Customer and meeting its obligations under the Service Agreement.

1.3 Nature and scope of processing

Personal Data is processed in both a partially automated and fully automated manner. The stages of processing performed by the Data Processor on behalf of the Data Controller can be seen in the table below and as otherwise indicated in the Service Agreement.

Processing stage	*Description*
Collection	The Customer supplies the Personal Data to the Supplier via digital media. In addition, the Supplier measures the effectiveness of marketing flyers by collecting data.
Transfer	Personal Data collected is transferred to the Supplier's IT system.
Storage	The Personal Data collected is stored on the Supplier's IT system.
Erasure	The Customer may erase Personal Data via the online interface. The Supplier erases Personal Data on receipt of the Customer's instructions in writing.
Flyers	The Customer may use the online interface to issue digital marketing campaign flyers to its customers. Flyers may be based on analysis results (see below).
Analysis	The Supplier registers and analyses the reactions of the Customer's customers to digital marketing campaigns over time at individual level and produces individual statistics based on the analysis. The analysis results are provided by the Customer via the online interface.

Sharing	Personal Data is not shared with third parties without the written consent of the Data Controller.
Administration	The Supplier processes and administers the Personal Data necessary to provide the Customer's employees with access to the service.

1.4 **Type of personal data**

Processing includes the name, street address, e-mail address, telephone number, mobile phone number, date of birth, personal ID number, gender, customer number, purchase transactions (including receipts), IP number, network identifiers, weblogs and other types of Personal Data as shown in the Service Agreement.

1.5 **Categories of Data Subject**

The Processing includes the Customer's customers, employees and any other categories shown in the Service Agreement.

1.6 **Site where processing conducted**

The processing will be conducted on equipment that is physically located in the EU/EEA.

1.7 **Duration of processing**

Processing will continue for as long as it is necessary for the Supplier to provide and deliver the service to the Customer, and for the Supplier to be able to meet its obligations under the Service Agreement.

2 SECURITY MEASURES

2.1 **Physical security**

Appropriate and adequate measures shall be taken to ensure the physical security of IT areas,[1] including – but not limited to – perimeter protection, access restriction, protection from fire, protection from power cuts, protection from theft and protection from damage.

2.2 **Inventory of computer equipment and systems**

A list shall be kept of computer equipment and systems used for the Processing of Personal Data. Documented procedures shall be in place for keeping this list continuously up-to-date.

2.3 **Computers**

Employees' computers must be automatically locked following inactivity and must require a strong password in order to be unlocked. The number of open communication ports on the

[1] "IT areas" means all premises designated for IT operations and where IT equipment is stored.

computers shall be kept to a minimum, and firewalls, antivirus software and security updates shall be installed and updated regularly. Hard disks associated with portable computers shall always be encrypted using a sufficiently strong key. The Processing of Personal Data on mobile devices shall be restricted in accordance with documented procedures.

2.4 **Authentication**

Logging into systems shall be done using a personal user ID and password. Passwords must be sufficiently strong. It shall not be permitted to transfer or share login information with other people. A register shall be kept of users' logins to systems.

Permissions control

Employees shall be given the least possible access when processing Personal Data. Only those employees who require access to Personal Data for the purpose of their work shall be given access. Documented procedures shall be in place for allocating and removing permissions.

2.5 **Servers**

Access to administrator tools and interfaces on servers must be restricted. Employees with administrator rights must use strong passwords. It shall not be permitted to transfer or share login information with other people. There shall be documented procedures in place to ensure that important updates to operating systems and applications are installed immediately.

2.6 **Network security**

Networks shall be protected from external attacks and data loss. Wireless networks shall be protected by encryption. Incoming and outgoing network traffic must be filtered, for example using firewalls.

2.7 **Security copies**

Security copies shall be taken of personal data at regular intervals. These security copies shall be stored separately and shall be well protected so that Personal Data can be recreated following a disruption. Documented procedures shall be in place for taking security copies, re-inputting security copies and testing the re-input of security copies.

2.8 **Data communication**

Connections for external data communication shall be protected using such technical functionality that ensures that the connection is authorised. Personal Data transferred by electronic communication outside networks controlled by the Supplier (e.g. the Internet) shall be protected by encryption.

2.9 **Data wiping**

There shall be documented procedures in place to ensure that Personal Data can be erased once no longer required for the purpose.

2.10 **Reporting of personal data incidents**

Procedures shall be in place for reporting and following up personal data incidents and other security incidents, and these must be followed.

2.11 **Operating documentation**

Documentation describing the day-to-day operation of the system shall be of sufficient quality to guarantee that availability is maintained.

2.12 **Separation**

The Personal Data shall be separated physically and/or logically from other personal data.

2.13 **Training of personnel**

The requirements that apply to employees with access to systems shall be defined by the system owner. The requirements shall relate to both security and skills and shall be documented and communicated. Employees shall be given regular training in data protection. Newly-appointed employees shall undergo training in data protection before they are given access to Personal Data.

2.14 **Documentation of measures**

The implementation of all security measures in accordance with this Appendix shall be documented and provided to the Customer on request.

3 CONTACT DETAILS

Customer: [Specify]

Company reg. no.: [Specify]

Representative: [Specify]

Data Protection Officer [Specify]

Supplier: Relation & Brand AB

Company reg. no.: SE556573650001

Representative: [Specify]

Data Protection Officer [Specify]