# Contract for commissioned processing of personal data according to art. 28 EU General Data Protection Regulation (GDPR)

Between the Controller:

Company Name: _____

Company Address: _____

_____

Hereafter referred to as ”Controller“,

and the Processor:

Sendinblue GmbH (formerly known as Newsletter2Go GmbH)
Köpenicker Str. 126, 10179 Berlin

Hereafter referred to as "Sendinblue" or “Processor”.

## § 1 Subject and duration of the commission

Sendinblue processes personal data commissioned by the Controller.

The subject of the commission concerns the application of address data of the Controller in order to send newsletters via email and further transactional emails.

The details of the services result from the general terms and conditions of business (www.Sendinblue.de/agb), which are explicitly accepted by the Controller during the registration process. The services are explicitly indicated (hereafter referred to as **Service Agreement**).

The term of the commission complies with the term of the Service Agreement. The provisions concerning the termination also apply to this contract. A termination of the Service Agreement enables both parties to terminate this contract.

Furthermore, both parties mutually agree to terminate earlier contracts for commissioned data processing by the conclusion of this contract.

## § 2 Appropriation to the commission’s content (Scope, type/purpose of the data processing, type of data, and persons concerned)

Scope, type, and purpose of the data processing are limited to the application of address data in order to send newsletters via email.

The processing and application of the data will only take place in Germany, another member state of the European Union, or in a contractual state of the agreement of the European Economic Area (EEA).

Any relocation to a third-party country requires a prior consent from the Controller and is only allowed if the special requirements of art. 44 GDPR are fulfilled.

The personal data that is implemented is client data of the controller.

Persons who are affected by the usage of this personal data (data subjects) by this commission are clients, business contacts, and prospective customers.

The processed types of data and categories of data subjects arise in § 15 of this contract.

## § 3 Technical and organizational measures, impact assessment

The Processor is required to implement the technical and organizational measures according to art. 32 GDPR prior to the beginning of the collection, processing or subsequent use of the personal data. The Processor is also required to document these processes under special consideration of the specific implementation of the commission. The Processor will make this documentation available to the Controller on demand.

The required technical measures according to art. 32 GDPR are specified in the data security concept in attachment 1. They refer to the stated purpose and are explicitly included in this contract.

The technical and organizational measures are subject to technological progress and further development. The Controller is allowed to implement alternative appropriate measures if the level of security is not below legal provisions.

The Processor has to implement technical and organisational measures that permanently guarantee the confidentiality, integrity, availability, and the capacity of the systems and services in relation to the reduction of security measures. The Controller is aware of these technical and organizational measures and is responsible for offering an adequate level of protection against the given risks.

In order to prove the compliance of the safety measures and their effectiveness, Sendinblue refers to its certification of TÜV Rheinland. Sendinblue proves that appropriate guarantees concerning the compliance of the Processor are accepted by providing the certificate to the Controller (cf. attachment 3).

## § 4 Correction, deletion, and blocking of data

The Processor is obligated to correct, delete, or block personal data that is collected, processed or used on behalf of the Controller.

In the event that a data subject contacts Sendinblue directly for the purpose of correction, deletion, or blocking of data, the Processor is explicitly required to send the request immediately to the Controller upon its receipt.

If costs arise, they must be paid by the Controller.

## § 5 Data protection control and duty to supply information

The Processor fulfills the following duties according to art. 28ff. GDPR:

- The appointment, by written order, of a data protection officer, in the event it is required by law.
- Protection of data secrecy according to art. 29 GDPR. All employees and other persons who may have access to personal data will be committed to data confidentiality. Furthermore, these persons will be instructed about the data protection obligations by this order, as well as its directives and purposes.
- Immediate information by the Controller concerning control actions and measures by the supervisory authority according to art. 57 GDPR. This also applies if the responsible authority investigates the Processor according to art. 83 GDPR.
- Reports to the Controller in all cases of violations by the Processor or his employees or subcontractors against regulations for the protection of personal data or against this contract. This applies to all cases of loss or unlawful transmission of personal data, as well as severe malfunction of the operation, suspicion of further violations against regulations that are protecting personal data, or other irregularities in the handling of personal data belonging to the Controller.
- The implementation of the order is fulfilled through periodic checks by the Controller in terms of the execution or fulfillment of the contract, especially the compliance and, if needed, possible adaptation of regulation and measures for the implementation of the commissioned processing.

## § 6 Sub-contractual relations

The Processor is entitled to use sub-contractors to fulfil of the Service Agreement and/or this contract. Therefore, the approval of the Controller is required. The approval is regarded as given if

- the Processor informs the Controller of the identity of the sub-contractor in text form (attachment 2);
- the contractual agreement with the sub-contractor corresponds to the data protection provisions of the contractual relationship between the Controller and the Processor;
- the ordering party is granted rights to the control and examination of the sub-contractor according to this contract by the assignment of the sub-contractor. This explicitly covers the right of the ordering party to receive information about the main content of the contract and the implementation of data protection obligations in relation to the sub-contractor. The information will be given, upon request, in written form. The ordering party will be given access to the relevant contracts if necessary; and
- the ordering party did not disagree with the decision within a week of notification.

The Processor may only disagree to the use of the sub-contractor if there is sufficient grounds.

Third-party services that the Processor is using as an ancillary service for the fulfillment of the contract are not regarded as sub-contractual relations.

These include, for example, telecommunication services, maintenance and user support, cleaners, investigators, or data storage and disposal devices.

The Processor is obligated to guarantee sufficient data protection and security for the Controller if there is the use of ancillary services by third parties. This is ensured by contracts that meet the legal requirements of data protection law as well as third-party inspection measures.

## § 7 Duties of the Controller

The Controller assumes full responsibility for complying with the legal requirements for data protection, particularly for the integrity of the data processing by the Processor. The Controller is the sole person in charge according to art. 4 No. 7 GDPR.

This responsibility applies explicitly to a potential duty to maintain a register of processing information according to art. 30 GDPR and fulfill information requirements according to art. 12 to 14 GDPR.

In the case of a request from a data subject regarding the Controller according to claims pursuant to art. 82 GDPR, § 8 sec 9 applies accordingly.

The Controller informs the Processor immediately if mistakes or irregularities in connection with the processing of personal data by the Processor arise.

The Processor directs the Controller to the relevant contact person for data protection questions regarding this contract.

## § 8 Right of command of the Controller / duties of the Processor

(1) The Processor may only process data of data subjects within the scope of this contract and with the authorization and direction from the Controller. This does not apply if there is an exception according to art. 28 para. 3 a) GDPR.

The Controller has full authority to give directions about the type, extent, and method of data processing within the scope of this contract. The Controller can exert this authority through individual instructions.

Changes to the processing methods and to the data being processed must be documented and agreed to by both parties.

Information for third parties or data subjects may only be given by the Processor after previous written consent from the Controller.

Direction and guidance, which is not provided by the contract, will be treated as a request for a change of duties.

If the Controller issues individual directives concerning the handling of personal data that transcend the scope of services as contracted, the subsequent costs must be paid by the Controller.

Verbal directions will be immediately confirmed by the Controller in written form or via email (in text form).

The Processor will not use data for any other purposes than directed. The Processor is not authorized to pass on the data to third parties. Copies and duplicates of data will not be created without the knowledge of the Controller. An exclusion exists for security backups provided they are necessary for correct data processing. There is also an exclusion for data that needs to be stored to comply with legal requirements for data storage.

The Controller has exclusive use of the provided personal data for the service as contracted. This does not apply if the requirements of the exception in art. 28 sec. 3 a) GDPR are fulfilled.

The Processor informs the Controller immediately if an instruction might violate an applicable law.

The Processor may suspend the implementation of an instruction until the instruction has been confirmed or changed.

Illegal directions concerning data protection law do not need to be executed by the Processor.

(2) The Processor shall make best efforts to support the Controller in fulfilling requests and claims of data subjects according to the obligations in art. 33 to 36 GDPR. For these supporting services, the Processor charges a fee of 75 euro per started working hour.

(3) The Processor guarantees that employees who process data for the Controller are prohibited to process data that fall outside of instructions. Furthermore, the Processor guarantees that employees with access to personal data are bound to a confidentiality agreement or are subjected to an adequate legal obligation to secrecy. The obligation to secrecy/confidentiality holds after the termination of the contract.

(4) The Processor immediately informs the Controller if there is a violation of the Controller's personal data.

The Processor takes necessary measures to secure the data. Furthermore, the Processor takes measures to limit any possible harmful effects to data subjects and immediately creates an agreement regarding these measures with the Controller.

(5) The Processor designates a contact person for data protection issues pertaining to this contract to the Controller.

(6) The Processor guarantees to fulfill duties according to art. 32 sec. 1 d) GDPR and to therefore implement a method for the continual inspection of the effectiveness of the technical and organizational measures that guarantee the security of the data processing.

(7) Under instruction from the Controller, or as dictated by the instructional framework, the Processor will correct or delete data.

If deletion of data or restrictions on data processing are not compliant with data protection regulations, the Processor accepts responsibility for the deletion/destruction of data storage devices and other material as instructed by the Controller. The Processor will return the data storage devices in the event that this is not already agreed to in the contract.

For these additional services, the Controller charges a fee of 75 euro per started working hour.

In certain cases determined by the Controller, the data storage devices will be stored or returned. A fee as well as security measures may be agreed on, if such an agreement is not already covered by the contract. For these security measures, the Controller charges 75 euro per started working hour. The costs for the commercial storage of data is determined by the size of the data, as well as the duration of the storage. If storage is preferable, an individual contract must be drawn up.

(8) Data, data storage devices, and any other materials must be either deleted/destroyed or returned to the Controller upon request at the termination of the contract.

If additional costs arise due to differing specifications according to the delivery or deletion of data, these costs will be assumed by the Controller.

(9) The Processor shall make best efforts to support the Controller in the defence against claims from a data subject according to art. 82 GDPR.

For these additional services, the Controller charges a fee of 75 euro per started working hour.

## § 9 Requests from data subjects

If a data subject makes a request to the Processor for information or the correction or deletion of data, the Processor will refer the data subject to the Controller to the extent that a referral to the Controller is possible, given the available information.

The Processor will immediately forward the request to the Controller. The Processor shall make best efforts to support the Controller as agreed to in the contract.

The Processor is not liable if the request from the data subject is not answered properly or in a timely manner.

## § 10 Deletion of personal data after termination of the commissioned processing

After the termination of the contractual work, or earlier upon request, the Processor must return or delete all documents in possession to the Controller upon request according to data protection regulations. This also applies to the results of the processed and/or used data. These provisions apply to test material as well as rejected material and must be completed by the termination of the service agreement.

The protocol for the deletion must be provided upon request.

Documentation proving that data processing complies with data protection regulations must be stored by the Processor beyond the end of the contract according to the relevant record-retention periods.

The Processor may give this documentation to the Controller after the termination of the contract.

## § 11 Verification

(1) The Processor will prove the compliance of the duties in the contract to the Controller through adequate measures.

(2) If individual inspections and examinations by the Controller or by an auditor on behalf of the Controller are necessary, these inspections will take place during usual business hours without disturbing the business processes, with prior scheduling and adequate lead time given to the Processor.

The Processor can make this inspection dependent to the prior registration and to the signing of a confidentiality agreement with reference to the data of further clients and the technical and organisational measures.

If the auditor working on behalf of the Controller happens to be in a potential conflict of interests with the Processor, the Processor is granted right of objection.

For support during the implementation of the inspection, a compensation is calculated in the amount of 600 euro per workday. The expenses of the inspection are limited to one workday per legal year for the Processor.

(3) If the data protection authority or other public administrative authorities governing the Controller perform an inspection, sec. 2 is applied correspondingly. The signing of a confidentiality agreement is not necessary if the authority is bound to a legal or professional obligation to confidentiality and its violation would be punishable under criminal law.

## § 12 Reference to lawful behavior

The Processor notifies the Controller that no advertisement will be allowed to be send if it is in violation of legal regulations.

The Controller assumes responsibility for the legal requirements for the collection, processing, and use of the data. This applies to the obligation of the Controller according to the law against unfair competition (UWG) and the telecommunication confidentiality according to the telecommunication laws (para. 88 TKG). Furthermore, the Processor explicitly refers to securing consent according to para. 7 UWG.

## § 13 Duty to supply information, written form clause, choice of law and place of jurisdiction, governing contract

(1) If the Controller's data is compromised through seizure or distraint; bankruptcy measures or settlement proceedings; or other events or actions of third persons, the Processor is obligated to inform the Controller immediately. The Processor will immediately inform all persons concerned that the Controller has ownership and exclusive usability of the data according to the the GDPR.

(2) Modifications and extensions to this standardized agreement and its components, including possible promises by the Processor, require a separate written agreement and furthermore the explicit note concerning the modification and extension of this contract. This applies similarly for the renunciation for this form requirement.

An agreement in digital form will be accepted as valid by both parties.

(3) In case of invalidity of particular parts of this contract, the rest of the contract remains valid. Instead of the invalid parts, the corresponding regulation by law is applicable.

(4) Only German law is applicable.

(5) The court of jurisdiction is Berlin, Germany.

(6) In the event of translation discrepancies in this contract from the original, the original contract will govern.

## § 14 Liability and damages

The Controller and the Processor are liable to data subjects according to the statutory rule in art. 83 GDPR.

## § 15 Data

According to this contract, the following types of data are processed.

**Types of data:**

**Furthermore, the following categories of natural persons are concerned:**

**Attachment 1:**
Data security concept

**Attachment 2:**
Identification of sub-contractors

**Attachment 3:**
Certificate TÜV Rheinland

Controller

| | |
|---|---|
| | |
| City | Date |
| | |
| Signature | Title of the contact person in the company |

Sendinblue GmbH:

| | |
|---|---|
| Berlin | |
| City | Date |
| Dariia Ieremenko | Data Privacy Officer |
| Signature Sendinblue | Title of the contact person in the company |

**Attachment 1**

# Data security concept

## Measures of data protection control according to art. 32 GDPR

State of revision: December 20, 2017

In case of questions about the information security of Sendinblue , please contact the responsible office:

## Contact

Sendinblue GmbH
Data protection officer
Köpenicker Str. 126
10179 Berlin
Tel.: +49 (0) 30 311 99 510
E-Mail: datenschutz@Sendinblue.com

**Measures for data security**

The data protection measures by Sendinblue are **aimed at the indemnification of availability, integrity, confidentiality, non-consolidation by purpose, transparency by auditability, and the possibility to intervene through anchor points.**

Measures for **pseudonymization** and **encryption** of personal data are implemented, which guarantee an adequate and currently acceptable level of protection. Similarly, our measures for data security operate at a **permanent and highest capacity** of our systems and services concerning the associated data processing. We ensure the ability to **rapidly re-establish the disposability** of personal data **in case of a physical or technical incident**.

Furthermore, we use processes in order to constantly inspect, review and evaluate the effectiveness of the technical and organisational measures in order to ensure the security of processing. Moreover, the Controller and Processor undertake measures to ensure that natural persons who have access are **only processing the data by order of the responsible office or person** unless they are committed to processing by the law of the European Union or a member state.

The business processes of Sendinblue are oriented on the requirements of art. 32 GDPR.

**§ 1 Protection against unauthorized acquisition of employee and client data as well as other protected personal data**

The measures of the company guarantee that unauthorized persons cannot influence data processing equipment on which personal data is processed or saved.

The Processor assures to the Controller that unauthorized persons are denied **access** and **entrance** to the data processing equipment on which personal data is processed or saved.

The systems of Sendinblue are protected by the following measures:

- entrance to the office premises by or in attendance of authorized persons
- central access regulation for the office premises (key concept)
- automatic fire detection system
- storage of confidential documents exclusively in locked, solid closets

The Processor guarantees the prevention of the unauthorized use of the data processing systems by the following measures:

- password protection: passwords requirements by at least 8 signs incl. 2 special characters
- passwords are changed every 90 days at least
- personal and individual user login in the system or the company network during the registration
- one master record per user
- IP restricted access on server
- authorization concept for digital possibilities of access

The company's measures for confidentiality and integrity ensure that authorized persons are only able to access data which is part of their access authorization. Furthermore, they guarantee that personal data cannot be read, copied, changed or removed without authority in the process of use, during processing and after saving of the data.

The business processes of Sendinblue are supported by the following measures:

- differentiated and task-related authorization and profiles
- frequent sighting of logfiles
- obligation of all employees to maintain the data secrecy and telecommunication secrecy

The company's measures guarantee an adequate **transmission control.** Personal data will not be read, copied, changed or removed during the transmission process without the possibility of review, identification or prevention.

Hereby, Sendinblue guarantees that no data will be given to third persons or parties.

The measures to achieve this target are specified subsequently:

- 256 bit SSL encryption with extended validation
- regulation for data destruction and deletion (deletion concept)

The company's measures for data integrity by Sendinblue guarantee an adequate **input control**. It is possible to retrospectively review and determine, if and by whom personal data is entered, changed or removed.

This is secured by the following measures:

- logging system and protocol evaluation system
- regulation of access rights

Furthermore, the company's measures guarantee a high quality level in the scope of **order control**. The

personal data, which is processed by order will only be processed according to the instructions of the Controller.

This is supported by the following measures:

- written agreement for commissioned processing of personal data pursuant to art. 28 GDPR including regulation concerning rights and obligations of the Controller and Processor
- formalised placing of the order

The company's measures for **availability control** guarantee a protection of the personal data against coincidental destruction or loss.

The Processor guarantees the following measures:

- 
- daily backup process
- mirroring of the hard drive of the subcontractor (RAID procedure)
- uninterruptible power supply at the subcontractor (UPS)
- virus protection/firewall at the subcontractor as well as at Sendinblue
- emergency plan
- automatic fire detection system

The company's measures for **separation control** furthermore guarantee a separate processing of personal data for different purposes.

The Processor ensures this separation control by the following measures:

- use of multitenant software
- development systems and test systems are exclusively used with test data

**§ 2 Certificate des TÜV-Rheinland**

As a further compliance measure in the area of data protection, we have received a certificate as a "service provider with certified data protection management" from TÜV-Rheinland.

As part of the data protection audit, in addition to the post-processing of the data protection legal assessment, ongoing measures are taken to prepare the data protection legal requirements, which are substantiated in annual activity reports.

## Attachment 2

# Identification of sub-contractors

**Hetzner Online GmbH**

Industriestr. 25
91710 Gunzenhausen
Deutschland

Register Court Ansbach,
HRB 3204 USt-Id Nr. DE 812871812

Hetzner is hosting the server which contains the used data within the Federal Republic of Germany.

# Attachment 3

## Certificate TÜV Rheinland

# Zertifikat · Certificate

Zertifikat für · Certificate for: Dienstleister mit geprüftem Datenschutz-Management

Zertifikats ID · Certificate ID: 0000046350


Zertifikatsinhaber · Certificate holder

Newsletter2Go

Newsletter2Go GmbH
Köpenicker Str. 126
10179 Berlin

Die Zertifizierungsstelle der TÜV Rheinland i-sec GmbH bescheinigt, dass die Newsletter2Go GmbH folgenden Nachweis erbracht hat:

Die Newsletter2Go GmbH hat ein Datenschutzmanagementsystem zum Schutz der Kundendaten gemäß dem von der TÜV Rheinland i-sec GmbH entwickelten Anforderungskatalog „Datenschutz" etabliert. Der Anforderungskatalog basiert auf der aktuellen Datenschutzgesetzgebung der Europäischen Union sowie national anwendbarem Datenschutzrecht. Er umfasst insbesondere folgende Aspekte des Schutzes personenbezogener Daten:

- Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten
- Datenschutzrechte der betroffenen Personen
- Pflichten von Auftragsverarbeitern
- Datenübermittlungen in Drittstaaten
- Umsetzung technischer und organisatorischer Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit

Der Nachweis der Konformität mit dem Anforderungskatalog wurde durch ein Datenschutz-Audit erbracht. Der Prüfbericht Nr. 63009557-01 in der Version 1.0 ist Bestandteil dieses Zertifikats.
Die Konformität der geprüften Prozesse wird durch jährliche Audits der TÜV Rheinland i-sec GmbH überwacht.

Das Zertifikat stellt kein akkreditiertes Zertifikat gemäß der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) dar.

Prüfgrundlagen · Test Requirements:
- Anforderungskatalog „Datenschutz" der TÜV Rheinland i-sec GmbH, in der jeweils aktuellen Fassung, basierend auf der aktuellen Datenschutzgesetzgebung der EU sowie der Bundesrepublik Deutschland

Zertifikat Nummer · Certificate Number: 63009557-01

Gültig bis · expiration date: 04.09.2021

Köln, den 12.10.2018

TÜV Rheinland i-sec GmbH
Am Grauen Stein · 51105 Köln

Zertifizierungsstelle
Simone Donst



www.tuv.com

TÜVRheinland®
Genau. Richtig.