

# Commissioned Data Processing Agreement

## Mailjet

This Agreement on commissioned data processing (“Agreement”) is made by and between Mailjet

SAS, a company organized under the laws of France, registered office at 13-13 bis, rue de l’Aubrac –

75012 Paris, France (“Processor”) acting on behalf of its affiliates, and the party named on the

signature page below (“Controller”), together the “Parties“.

### 1. Subject and duration

(1) The Processor and other data processing entities as listed in Clause 6 of this Agreement perform

IT Services for the controller, as part of the provision of services pursuant to the services

contract between the Parties (“Service Contract”). IT Services are defined as “distributed data

processing services” which are not characterized through a conventional bilateral cooperation

between Processor and Controller, but are generated by multiple Processors with alternating

processing duties.

(2) As personal data will be processed on behalf of the Controller and according to his instructions

for this matter, or an access to personal data cannot be excluded by performing these

IT Services, the services are commissioned data processing in accordance with the European

Regulation 2016/679 (General Data Protection Regulation, "GDPR") and all applicable data protection laws.

(3) The terms "personal data", "processing", "consent", "collection", "Third party", "Controller" and

"Processor" are to be interpreted according to the definitions given in Article 4 of the GDPR. A

reference in this Agreement to "writing" or "written" includes email.

(4) This Agreement shall – unless otherwise agreed – become effective when signed by both Parties

and shall apply as long as the Processor processes personal data on behalf of the Controller

pursuant to the Service Contract. However, it does not end before the obligation to delete and

return relevant documents and data has been fulfilled by the Processor.

## 2. Extent, type and purpose of the data processing, data types and data subjects

(1) The processing of the Controller's data within the scope of order processing shall be carried out

in accordance with the stipulations regarding the type and purpose of processing contained in

Annex 1 to this Agreement.

(2) Type and purpose of the data processing, the data types as well as the groups of data subjects

are described in Annex 1.

## 3. Provision of information

(1) The Processor warrants and undertakes to employ and document reasonable and appropriate

technical and organizational security measures for the data processing, as specified in Annex 3.

(2) In the event of major changes in the security measures, but at least once a year upon request,

the Processor will supply an update of the documentation of these technical and organizational measures.

(3) The Processor shall support the Controller upon request in creating the register of automated

processing operations according to the GDPR and in keeping it up to date as far as the applied

automated processing operations and the employed technical and organizational measures are

affected. On request, the Processor will disclose the necessary information and documents to

the Controller.

#### 4. Correction, deletion and restriction of data

The Processor shall not correct, delete or restrict personal data provided by the Controller in an

unauthorised manner, and may only do so in accordance with the instructions of the Controller. In

the event that the data subject contacts the Processor directly in this respect, the Processor may take

appropriate steps to treat the request accordingly, and should forward this request and processing

treatment to the Controller within a reasonable delay.

## 5. Duties of the Controller

(1) The Controller is responsible for its own compliance with the GDPR and other data protection

provisions. It is liable for the admissibility of the data processing and for the protection of the

data subjects' rights according to the GDPR and other data protection provisions.

(2) The Controller will inform its data subjects about its use of Processors in processing their

personal data, to the extent required under applicable data protection law.

(3) The Controller shall respond in reasonable time and to the extent reasonably practicable to

enquiries by data subjects regarding the processing of their personal data by the Controller, and

to give appropriate instructions to the Processor in a timely manner.

(4) The Controller shall respond in reasonable time to enquiries from a data protection authorities

regarding the processing of relevant personal data by Data Controller.

## 6. Duties of the Processor

(1) The Processor hereby confirms that it is aware of the relevant European data protection

regulations. The Processor's internal operating procedures shall comply with the specific

requirements of an effective data protection management.

(2) The Processor warrants and undertakes that all employees involved in the data processing are

familiar with the relevant data protection requirements. The Processor assures that those

employees are bound to maintain confidentiality as provided by the GDPR. The Processor shall

monitor compliance with the applicable data protection regulations.

(3) Personal data processed for different Controllers have to be processed separately; measures to

ensure separate handling are documented in Annex 3.

(4) The Processor shall not acquire any rights to the Controller's data and shall be obligated, upon

request by the Controller, to hand over the Controller's data in a form that can be read and

processed further. Rights of retention with regard to customer data and the associated data

carriers are excluded.

(5) The Processor is only allowed to process or use the personal data provided to it exclusively in a

Member State of the European Union (EU) or the European Economic Area (EEA).

The collection,

the processing or the use of personal data on the territory of a country which is not a Member

State of the EU or the EEA requires prior explicit consent of the Controller and may only be

carried out if the action complies with the legal requirements of the GDPR.

(6) The Processor's data processing centers are exclusively located in the European Union, as

specified in Annex 2.

(7) The Processor shall at all times have in place an officer who is responsible for assisting the

Controller:

(a) in responding to inquiries concerning the commissioned data processing, received from data

subjects; and,

(b) in completing all legal information and disclosure requirements which apply to the Controller

and are associated with the commissioned data processing.

The Data Protection Officer may be contacted directly at [privacy@mailjet.com](mailto:privacy@mailjet.com). The Processor

will ensure that this information is up to date at all times in its Privacy Policy available online.

(8) Insofar as the Processor is required by law to provide Third parties with information about

customer data, the Processor shall inform the Controller in writing about the recipient, time and

content of the information to be provided and its legal basis in a reasonable delay prior to

providing such information.

## 7. Appointment of Subcontractors

(1) The list of companies providing critical and substantial IT services for the Processor on a

contractual basis are detailed in Annex 2.

The Controller expressly agrees to their assignment. The Processor will provide notice to the

Controller for the engagement of further Subcontractors and if the Controller does not respond

after a period of 30 days, he is deemed to accept expressly their assignment, without other

specific written consent.

(2) The Processor ensures that the Subcontractor's processing is carried out under a written

contract imposing on the Subcontractor the same obligations imposed on the Processor under

this Agreement.

(3) Access to the relevant personal data may only be granted when the Subcontractor complies or

assures compliance with the obligations of this Agreement to the Controller and the Processor

controls the Subcontractor's compliance with these obligations on a regular basis.

(4) The provisions of this Clause 6 shall also apply if a Subcontractor is engaged in a country outside

the EU Territory. In such a case, the Processor shall ensure data protection law admissibility by

means of suitable legal instruments, such as EU standard contractual clauses.

(5) Ancillary services which are provided to and on behalf of the Processor by Third party service

providers and which are determined to support the Processor to execute the Services Contract,

shall not be regarded as subcontracts in the sense of this Agreement. Such services may include,

for example, services of telecommunication, support applications or tools, cleaning or facility

management. However, the Processor shall enter into legally binding and adequate Agreements

with Third party service providers regarding the protection and the security of the Controller's

data accessible by the Third party service providers and employ appropriate control measures.

## 8. Audit and control rights

(1) The Processor hereby declares that the Controller or a person who has been authorized by the

Controller for this purpose is allowed to control – to the extent necessary according to the GDPR

– the compliance with the data protection requirements and the other contractual obligations

set forth in this Agreement. This means in particular, that the Controller is allowed to inspect the

relevant computer programs used by the Processor and obtain information and documentation

relevant to review the Processor's compliance with the legal provisions on data protection and

security as well as the provisions of this Agreement. The Controller may also access the

Processor's premises for this purpose, only after reasonable notice, and only if it ensures strict

confidentiality and non-disclosure compliance. If the Processor cannot provide the relevant

information himself, it is obliged to contact the Subcontractors for further details.

(2) If, upon completion of the foregoing, the Controller is not reasonably satisfied with the security

measures taken according to clause 3 of this contract, then upon the Controller's reasonable



advance request, the Processor will provide the Controller with system test result extracts

and/or penetration testing scan result extracts for the Controller's review of the Processor's

compliance with the obligations set forth in this Agreement.

## 9. Notification in the event of data breaches

(1) The Processor shall notify the Controller according to Article 33 of the GDPR, without

unreasonable delay, of any personal data breach, including any suspected or actual unauthorised or unlawful processing of personal data and any accidental loss, alteration,

misuse, disclose or destruction of, or damage to, personal data committed by employees, the

Subcontractor or other Third parties which concern personal data provided by the Controller.

(2) The information on the personal data security incident shall include details of the time and

nature of the incident (including information concerning which and how data relating to the

contracting authority are involved), the computer system concerned, the persons concerned,

the time of discovery, all conceivable adverse consequences of the data security incident and

the measures taken by the contractor as a result thereof.

(3) The Processor shall also inform the Controller, without unreasonable delay, if it discovers that

its technical and organizational measures do not comply with legal requirements.

## 10. Instructions of the Controller

(1) The Controller is entitled to give instructions to the Processor on the extent, type and methods

of the data processing. Instructions are to be issued in writing by the Controller. If necessary, the

Controller may also issue instructions verbally to the Processor, but any instructions given

verbally must be confirmed in writing.

(2) The Processor has to process the personal data provided by the Controller exclusively on behalf

of the Controller and in accordance with its instructions.

(3) The Processor shall promptly notify the Controller if it believes that an instruction of the

Controller does not comply with the applicable legal provisions of data protection.

The

Processor shall then be entitled to suspend the execution of the instruction until confirmation or

change of the instruction by the Controller.

(4) The Controller shall promptly notify the Processor if failures or irregularities are recognized in

the course of the examination of the data processing results.

## 11. Liability

(1) The Controller shall be liable for all direct damages arising out of or in connection with any

breach by its employees, representatives, agents or subcontractors of its obligations under this

Agreement.

(2) The Processor agrees to fulfil its obligations established in this Agreement, and in the applicable legislation. Pursuant to the terms of Article 28.10 of the GDPR and other applicable data protection legislation, if the Processor breaches this Agreement in determining the purposes and means of the processing, it shall be held responsible for all direct damages arising out of or in connection with any breach by its employees, representatives, agents or subcontractors of its obligations under this Agreement.

(3) Notwithstanding the above, the Processor may not under any circumstances, be liable for any indirect damages.

## 12. Termination of the contract

(1) On termination or expiration of this Agreement the Processor shall return all documents and storage media as well as all results of the data processing which concern the commissioned data processing and contain personal data provided by the Controller, upon request. All other personal data concerning the commissioned data processing shall be destroyed, respectively erased. This provision shall not affect potential statutory duties of the Parties to preserve records for retention periods set by law, statute or contract.

(2) The Controller can terminate the contractual relationship without notice if the Processor

severely violates this Agreement or the regulations of the GDPR and the Controller can therefore

not reasonably be expected to continue the data processing until the expiry of the notice period

or the agreed termination of Service Contract.

### 13. Final provisions

(1) Insofar as this Agreement does not contain any special provisions, the provisions of the Service

contract shall apply. In case of contradictions between this Agreement and from the Service

Contract, the provisions from this Agreement take precedence.

(2) The Parties shall keep confidential all business secrets and data security measures they gain

knowledge of in the context of the contractual relationship. Business secrets are all (but not

limited to) business-related facts, circumstances and activities which are not generally

accessible, but only accessible to a limited group of persons unless the Processor has no

legitimate interest of non-proliferation. Data security measures are all measures taken to

preserve the privacy, integrity and availability of data according to the GDPR. This obligation of

secrecy remains effective after the termination of this Agreement.

(3) In case one Party is subject to further obligations of secrecy and has informed the other Party in

written form hereof, the other Party is obliged to comply with those obligations as well.

(4) In case any of the Controller's property rights are at risk in the office premises of the Processor

due to measures taken by Third parties (e.g. forfeitures and garnishments), insolvency

proceedings or any other events, the Processor shall promptly inform the Controller hereof. A

right of retention for the Processor is excluded with regard to storage media and data bases of

the Controller.

(5) Additional Agreements must be agreed upon in written form. In case individual provisions of this

Agreement are invalid, this shall not affect the validity of the remainder of the Agreement.

<p><b>Mailjet SAS</b></p> <p>Name: Darine Fayed Title: Head of Legal &amp; DPO</p> <p>Signature: </p>	<p><b>Company:</b> Address:  Provinciale weg 15b 1506 ME Zaandam</p> <p>Name: Title: Owner: J.J. van Breemen</p> <p>Signature: </p> <p>Date: 15-10-2019</p>
--	---

## Annex 1: List of contracted Services

<b>Service</b>	<b>SaaS Solution</b>
Type of data	e-mail addresses, names, telephone numbers, company titles and other specific data as entered by the Controller into the Processor platform
Group of data subjects	Newsletter subscribers, clients and customers, as well as staff and business partners of the Controller
Extent, type and purpose of the collection, processing or use of data	Service contract for email and sms sending solution and related services

## Annex 2: List of Subcontractors

<b>Subcontractors</b>	<b>Location of data processing</b>	<b>Activities</b>
<b>Google Cloud</b>	Frankfurt (Germany) St. Ghislain (Belgium)	Datacenter
<b>OVH</b>	Roubaix (France)	Datacenter
<b>Proxiad</b>	Sofia (Bulgaria)	Support functions
<b>Pontica</b>	Sofia (Bulgaria)	Support functions
<b>Attinéos</b>	Rouen (France)	IT development and operations functions
<b>Ipsip</b>	Ho-Chi Minh (Vietnam)	Support functions
<b>Infobip</b>	Rueil-Malmaison (France)	SMS Messaging services
<b>Briteverify</b>	Ireland	Email address verification services
<b>NeverBounce</b>	Europe	Email address verification services
<b>250K</b>	USA	Email marketing reports and analytics
<b>Stripe</b>	Europe	Payment service provider
<b>Paypal</b>	Europe	Payment service provider

## Annex 3: Technical and organizational measures

The Processor warrants that it has implemented the following technical and organizational measures

in relation to the processing of Controllers' data:

### 1. Measures to guarantee confidentiality

#### 1.1. Physical access control

Measures to prevent unauthorized individuals from gaining physical access to IT and data

processing systems for processing personal data and to confidential files and storage media:

At Mailjet premises :

- Door security (electronic badge system with controlled key allocation)
- Elevator security (elevator access codes)
- Surveillance equipment (alarm systems and video surveillance)
- Secured IT room
- Fire alarm and fire extinguishers
- Control system for visitors

At data centers :

- Perimeter fencing
- Door security (electronic badge system with controlled key allocation)
- Surveillance equipment (movement detection system, alarm systems, video surveillance)
- Fire alarm and fire extinguishers
- Control system for visitors
- Security staff on site 24/7

#### 1.2. Logical and data access control



Measures to prevent protected data from being processed or used by unauthorized persons so

that data cannot be read, copied, changed, stored or removed during the processing without

authorization:

- Two-step authentication process (with minimum length, regular change and strict confidentiality for passwords used)
- SSH network protocol and VPN connection to access platform infrastructure
- Automatic locking, log-off
- Authorization concepts (limitation to authorized employees based on role)
- Encrypted storage media
- Tracking of unauthorized activity/access
- Encapsulation of sensitive systems through separate network areas
- Firewall, regular updated antivirus
- Documented access control policy

### 1.3. Separation instruction

Measures that reassure that data collected for different reasons is processed separately and

therefore being separated from other data and systems in order to guarantee that an unplanned

processing of these data for other reasons is impossible:

- Authorization concepts
- Encrypted storage of personal data
- Client separation within the software
- Separation of testing and producing systems
- Geo-distribution: Resources distributed across several datacenters powered by different

networks. Redundancy is intrinsically embedded in the infrastructure.

#### 1.4. Pseudonymization

Measures that reduce the personal references during data processing to such an extent, that the

personal correlation to the affected individual is impossible without further information. Every

further information therefore has to be kept separately from the nickname:

- Hash value process

#### 1.5. Order Control

Measures to ensure that, in the case of commissioned processing of personal data, the data are

processed strictly in accordance with the instructions of the controller:

- Instructions of the principal
- Monitoring of contract execution
- Internal policies applicable to all employees

## 2. Measures to secure integrity

### 2.1. Data transfer control

Measures which guarantee that personal data cannot be read, copied, changed or removed

during the electronic transmission or during their transport or storage on data carriers without

authorization as well as measures ensuring checking and determination of the locations a

transmission of personal data is designated:

- Transmission of data via encoded data networks (https)
- Comprehensive recording processes
- No data transfer outside EU

## 2.2. Input control

Measures which guarantee that it can be subsequently checked and determined whether and by

whom personal data have been entered, changed in or removed from the data processing

systems:

- Storage of personal data for a limit of 3 months after account closing, unless otherwise

specifically instructed

- Record evaluation systems (For API, IP, date, URL and method are stored. For GUI, IP of

each session, and HTTP logs of all requests are stored)

- Documentation on requests are retained.

## 3. Measures to ensure availability and capacity

### 3.1. Availability control

Measures to ensure that personal data are protected against accidental destruction or loss:

- Data backup process

- Databases replicated in multiple systems

- Geo-distribution: Resources distributed across several datacenters powered by different

networks. Redundancy is intrinsically embedded in the infrastructure

- Uninterruptible power supply

- Fire alarm system

- Air conditioning system

- Alarm system

### 3.2. Fast recoverability

Measures that ensure a fast recovery of the availability and accessibility of data in case of a

physical or technical incident.

- Incident management process
- Disaster recovery plan and emergency plan
- Automatic switchover process for database servers
- Data backup process
- Regular tests of data recoverability

#### 4. Measures for the regular evaluation of the security of data processing

Measures that reassure safe data processing conforming with the law.

- Data protection management
- ISO 27001 certification and regular re-certification
- External penetration and vulnerability testing (including the use of a bug bounty platform)
- Data breach procedure
- Documentation of the client's instructions