Data Processing Agreement – Sigilium

Version 1.7

First version–December 2018
Updated in Janvier 2025

1 - Data processing addendum

Data processing subcontracting agreement.
This agreement is concluded between the following parts:

Client's name and address:

hereinafter referred to as the Data Controller

And:

Sigilium limited liability company (SARL) with a capital of 7,000 euros
Registered to the Paris Register of Commerce under B 809 637 382
141 avenue de Wagram - 75017 Paris, FRANCE

hereinafter referred to as the Data Processor.

This agreement has the following appendix attached:

1. Personal data categories and types

Preamble

The Data Controller is responsible for the processing of personal data under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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), hereinafter referred to as the GDPR.

The processing of personal data is also regulated by French law CNIL n°78-17 of 6 January 1978 on information technology, data files and individual liberties (amended).

The Data Controller wants to outsource the processing of personal data to the Data Processor, in compliance with article 28 of the GDPR. Both Parties commit to strictly comply with the GDPR, which will prevail in any circumstances, notwithstanding any contrary provision.

Declaration of the Data Processor

The Data Processor declares that he owns all warranties necessary to implement appropriate technical and organizational measures to ensure that the processing complies with the GDPR requirements and guarantees the protection of the data subject's rights.

Personal data processing specifications

The Data Controller defines terms, purpose and scope as follows:

Purpose of the data processing – The purpose of the processing operation is the proper performance of the service offered by Sigilium, i.e. the centralized management of email signatures from the Client.

Duration of data processing – The processing operation starts from the implementation of the service until 9 months after termination by the client, in order to be able to comply with related legal obligations.

Nature and goal of the data processing – Sigilium's service uses a Web platform containing the contact details of employees who have a Sigilium email signature. The processing operation ensures that the signature is updated on each employee's desktop computer. The purpose of the processing operation is also to compile how many clicks each relayed notice receives. Furthermore, the processing of data is necessary for the adequate execution of the service, including sending alerts in case of software malfunction.

Type of personal data– The personal data collected are those provided by the Client:

- Employee's email address
- Other common information, if provided by the Client: full name, job title, phone number, fax number, Skype ID, company mailing address, profile picture.
- IP addresses of individuals who click on an employee ad in his/her signature or contact card. We do not store additional identification cookies allowing to identify this individual. This IP base is strictly reserved for internal use at Sigilium and is not shared with any other partner. IPs are stored for 6 months.
- The IP address of people clicking on an employee's email signature link, and redirecting to sigilium.com initially. This IP address is only stored for 1 week, in order not to count a click on an ad from the same IP address several times.
- Any other information provided by the client, under the client's responsibility, subject to the information usefulness under the performance of the service. Any sensitive data, such as religious views, ethnic origin and others are prohibited in the use of our service.

Categories of individuals – Individuals subject to data processing are selected by the client, and are generally employees of the company/branch using the service.

Data encryption

To minimize the risk of data being stoled, in December 2021, Sigilium did encrypt all the job titles.

In case a backup was stolen, or an access to the server was given (inadvertently) to a malicious user, he could not use the data without the master key.

The master key is not stored on the drives of the server at any moment.

Data Controller's rights and obligations

The Data Controller defines the purposes and means of the personal data processing.

The Data Controller ensures that the processing is lawful and personal data is collected and processed in compliance with the GDPR and French law. The Data Controller also commits to

provide all requested information to all subjects involved with the processing operations, at the moment of collecting data when personal data are collected directly from the data subject, or in the timeframe requested when personal data were not collected from the data subject, following articles 12 to 14 of GDPR. The Data Controller releases the Data Processor from any consequences of a possible violation by the Data Controller of their obligations under the GDPR.

The Data Controller will provide the Data Processor with all necessary information to allow the Data Processor to perform the services, as per the GDPR and French law.

Data Processor's obligations

By no means does the Data Processor define the purposes and means of the processing. Failing that, the Data Processor is considered as a Data Controller with regard to the processing involved.

The Data Processor and any individual acting under the Data Processor's authority with access to personal data may not process these data, except upon request from the Data Controller, or unless they are compelled to do so by the EU legislation or an EU Member State legislation.

The Data Processor only processes personal data upon documented request from the Data Controller, including with regard to transfers of personal data to countries outside the European Union or an international organization, unless the Data Processor is compelled to do so by the EU legislation or an EU Member State legislation Data Processor he is subject to. In which case, the Data Processor must inform the Data Controller of such legal obligation before the processing operation unless such notification is forbidden by law for major public interest reasons.

The Data Processor makes sure that individuals authorized to process personal data are committed to maintain privacy or are subject to a statutory duty of confidentiality.

The Data Processor must implement all measures requested by article 32 of the GDPR, including:

- Limiting access to data to individuals (hereinafter referred to as Sub-Managers) involved in the proper execution of the service, and whose name and motivations are available upon simple request, as well as keeping updated records if a new individual needs to access data during the time of performance of the agreement;
- Securely safekeeping the data provided by the client;
- Updating protection measures on a regular basis.

The Data Processor takes into consideration the nature of the processing operation, helps the Data Controller, through appropriate technical and organizational actions (to the fullest extent possible) to carry out the Data Controller's obligation to comply with the requests of data subjects involved in the processing operation to use their rights as defined in section III of the GDPR.

The Data Processor helps the Data Controller ensure the compliance with obligations defined in articles 32 to 36 of the GDPR, in view of the nature of the processing operation and information available to the Data Processor.

The Data Processor must immediately inform the Data Controller if in their opinion any given request is a violation of the GDPR or other provisions of the EU legislation or EU Member States legislation in relation with personal data.

Data storage and destruction

Depending on the Data Controller's choice, the Data Processor must delete all personal data or send them to the Data Controller after termination of the performance of services in relation with the processing operation, and destroy all existing copies, unless EU law or applicable law of an EU Member State requests to store said personal data.

All Sigilium data are stored in the EU.

Audit

The Data Processor provides the Data Controller with all necessary information to prove compliance with obligations defined in this agreement and to allow the performance of audits, including examinations, by the Data Controller or any other appointed auditor, and to contribute to the audits. Given the ratio between the amount of time dedicated to an audit and the cost of service, the audit will be invoiced on a spent time basis, with an hourly fee of €150 pre-tax.

Additional subcontractor

The Data Processor must comply with the following conditions to recruit an additional subcontractor to act in the Data Processor's operations.

The client usually allows the Data Processor to choose its own contractors, who must comply with the GDPR. The Data Processor must notify the Data Controller of any change in relation with the addition or substitution of any additional subcontractor, in order to give the Data Controller the opportunity to oppose said changes.

When a Data Processor recruits an additional subcontractor to perform specific processing operations on behalf of the Data Controller, the same obligations in terms of data protection than those defined in this agreement apply to the new subcontractor, and the latter is bound by said agreement or, if applicable, by any other legal act as part of the EU legislation or an EU Member State legislation, including in terms of presenting satisfactory guarantees regarding the implementation of adequate technical and organizational measures ensuring the processing operation complies with the GDPR. When said additional subcontractor doesn't comply with obligations in relation with data protection, the initial Data Processor is still fully liable before the Data Controller for the performance by the other subcontractor of its obligations.

Sigilium will inform the Client prior to the occurrence of a change of Sub-Contractor, using the usual communication media such as emails, websites and portals. If the Client reasonably opposes the addition of new Sub-Contractors (for example, if said change results in the Client's violation of laws and regulations regarding data protection), the Client will inform Sigilium by writing of their specific oppositions under thirty (30) days after receipt of the new notification. If the Client does not oppose the addition during this period, the addition of the new Sub-Contractor and, if appropriate, the agreement provided as part of this DPA will be deemed accepted. If the Client is opposed to the addition of a new Sub-Contractor, but Sigilium cannot comply with the Client's opposition, the Client may terminate the Services and Software by writing under sixty (60) days after receipt of Sigilium's notification.

The list of subcontractors involved in personal data processing is available as an annex to this document.

Duration

This agreement stays in force for the full duration of the subcontractor's retention of personal data. This agreement regulates the sub-processing of personal data mentioned in this document at any time, including after the agreement termination.

Applicable law and choice of forum clause

This agreement is ruled by French law and subject to the exclusive jurisdiction of courts having local jurisdiction for the city of Paris, France.

Appendix 1: Categories and types of personal data

- Last name
- First name
- Full professional mailing address
- Professional landline and mobile phone numbers
- Company job title
- Professional email address

Appendix 2: List of approved subcontractors

- Server hosting : Servers are hosted by Amazon company (AWS service) in its Paris Data Center at 67 Boulevard du Général Leclerc, Clichy, France, a branch of Amazon, located at 410 Terry Avenue North P.O. Box 81226 Seattle, WA 98108-1226–USA. Represented by Mr. Frédéric Duval (Amazon AWS France)
- HoneyBadger (Honeybadger Industries LLC 11410 NE 124th Street #246 Kirkland, WA 98034), represented by Ben Curtis, has the role to send error alerts.
- Postmark by ActiveCampaign, represented by Jason VandeBoom (CEO), is required to send installation emails to employees.

Appendix 3: List of individuals allowed to process personal data

Thomas Darde and Xavier Trannoy each being an associate or full-time employee at Sigilium) are allowed to process personal data.

Appendix 4: Personal data storage location

The Data Controller's data are stored in a server farm rented by the Data Processor. These servers are located in mainland France by territorial obligation.

Appendix 5: Additional IT security measures

All passwords are secured by the obligation to use complex characters, and the use of at least 12 characters.

Client access to data is encrypted with an SSL certificate.