DATA PROCESSING AGREEMENT

This Data Processing Agreement is a part of the GTC and SPECIFIC CONDITIONS (collectively, the "Contract") under which SESAME HR shall act as the Data Processor, and the CLIENT shall act as the Data Controller.

DATA PROCESSING AGREEMENT – GDPR COMPLIANCE

This DATA PROCESSING AGREEMENT shall only apply if the CLIENT and/or SESAME HR are subject to the GDPR.

CLAUSES

1. Object

In order to perform the services under the Contract, and to provide the Services effectively, the Data Processor may have access to personal data under the responsibility of the Controller.

2. Identification of the affected information and processing activities to be carried out

For the execution of services arising from compliance with the purpose of this Data Processing Agreement, the Data Controller shall make available to the Data Processor a series of personal data through inclusion in any of the SERVICES.

It is the Data Controller who, through their actions or those of the AUTHORISED USERS, determines the categories of data and data subjects to be processed by the Data Processor.

The authorised processing activities shall include all those necessary for the execution of the Contract.

3. Duration

This Data Processing Agreement shall enter into force on the date of acceptance of the Contract. This Data Processing Agreement is ancillary to the contract and its duration is therefore linked to the duration of it.

4. Obligations of the Data Controller

The Data Controller is responsible for carrying out the following tasks, in addition to fulfilling the obligations attributed to him/her under this Data Processing Agreement:

a) Comply with all the technical and organisational measures necessary to guarantee the safety of the processing, premises, equipment, systems, programs and individuals involved in the processing of the personal data, which are stipulated in the

regulations in force and applicable at all times

b) To deliver to the Data Processor the data referred to in clause 2 of this document, as well as the necessary instructions to carry out the processing of the data under the terms established by the Controller.

c) Respond to the rights of individuals affected by the processing, such as the rights of access, rectification, erasure and objection, restriction of processing, data portability and the right not to be subject to automated individual decisions, in cooperation with the Processor.

d) Carry out, where appropriate, an assessment of the impact on the protection of personal data of the processing operations to be performed by the Processor.

e) Ensure, before and during the processing, that the Data Processor complies with the applicable data protection regulations.

f) Supervise the processing, including carrying out inspections and audits.

g) Communicate to the Data Processor any changes in the personal data provided, so that they can be updated.

5. Duty to provide information and legitimate basis

The Controller guarantees that he/she has complied with the duty to provide all information to data subjects at the time of collection of the data undergoing processing, in compliance with the provisions of art. 12, 13 and 14 of the GDPR, as applicable.

The Controller guarantees that he/she has an appropriate legitimate basis for processing the personal data that complies with the principles of effectiveness, necessity and proportionality, taking into account the existence of other protection measures that may be less invasive, avoiding discriminatory effects and establishing appropriate safeguards.

The Data Processor shall in no case be liable for the lack of compliance or defective compliance with the duty to provide information or for the application of an appropriate basis for legitimisation.

6. Obligations of the Data Processor

The Processor declares and warrants to the Controller the following:

1. That he/she will use the personal data undergoing processing, or those collected for their inclusion, only for the purpose of this assignment. Under no circumstances may it use the data for its own purposes;

2. That he/she will process and use the personal data to which he/she has access, solely according to the instructions of the Data Controller, and in accordance with the purposes regulated in the Contract.

Instructions regarding the processing of the data and actions assigned to the Processor shall be communicated to the Processor in writing.
If the Processor considers that compliance with a particular instruction from the Controller could lead to a breach of data protection regulations, the Processor shall immediately notify the Controller. The Processor shall in this communication request the Controller to amend, withdraw or confirm the instruction given and may suspend compliance pending a decision by the Controller.

3. That, if applicable, he/she will keep, in writing, a record of all categories of processing activities carried out on behalf of the Controller, containing all the information provided for in art. 30 GDPR.

4. That he/she will maintain confidentiality and secrecy regarding the personal data to which he/she has access due to the provision of the Services.

5. That he/she will not communicate to third parties except with the express authorisation of the Data Controller, and in the legally admissible cases.
The Data Processor may communicate the data to other data processors of the same data controller, in accordance with the instructions of the latter. In this case, the data controller shall identify, in advance and in writing, the entity to which the data must be communicated, the data to be communicated and the security measures to be applied in order to proceed with the communication.

6. That he/she will provide the Controller with the information necessary to evidence compliance with the obligations set out in the Contract.

7. That he/she will provide assistance as required by the Controller for audits or inspections, carried out by the Controller or by another auditor authorised by the Controller. Audits may be carried out periodically, on a planned or ad hoc basis, upon reasonable notice to the Controller, during the Processor's normal working hours.

8. That he/she shall guarantee that the persons authorised to process personal data have undertaken, expressly and in writing, to comply with the security measures established, and to respect the confidentiality of the data. Compliance with this obligation shall be documented by the Processor and made available to the Controller.

9. That he/she has appointed a data protection officer ("DPO") whose contact details are as follows: legal@sesametime.com.

10. That he/she will collaborate in the fulfilment of the Controller's obligations and will offer support to the Controller, where appropriate and as requested by the Controller, in carrying out (i) impact assessments relating to the personal data to which he/she has access; (ii) prior consultations with the supervisory authority.

7. Destination of Data

Upon termination of the provision of the Services, the Processor shall return the personal data to which he/she has had access and any existing copies, as instructed by the Controller

in accordance with section 13.2 of the Agreement.

The Processor may retain a copy with the data duly blocked, for as long as liabilities may arise from the performance of the provision of the Services.

8. Notification of data security breaches

The Processor shall notify the Controller, without undue delay, and in any event no later than within 24 hours, of any suspected or confirmed data protection incident within its area of responsibility. Among other things, he/she shall notify the Controller of any processing that may be considered unlawful or unauthorised, any loss, destruction or damage to data and any incident considered to be a breach of data security. The notification shall be accompanied by all relevant information for the documentation and communication of the incident to relevant authorities or affected data subjects.

The Processor shall, in addition, assist the Controller in relation to the notification obligations under the GDPR (in particular, Articles 33 and 34 of the GDPR) and any other applicable present or future regulation modifying or supplementing such obligations.

9. Exercise of rights by interested parties

The Data Processor shall provide the information and/or documentation requested by the Controller in order to respond to requests for the exercise of rights that the Controller may receive from data subjects whose data are processed. The Data Processor shall provide such information within reasonable periods of time and, in any case, sufficiently in advance to enable the Controller to comply with the legally applicable deadlines for responding to the exercise of these rights.

When the data subjects exercise their rights of access, rectification, deletion and objection, limitation of processing, data portability and the right not to be subject to automated individual decisions, the Data Processor shall communicate this by e-mail to the address legal@sesametime.com. The communication must be made immediately in order to be dealt with within the established legal deadlines, and in no case more than two working days after receipt of the request, and must be submitted to the Data Controller together with any information that may be relevant to its resolution.

10. Security

Concerning technical and organisational security measures, the Data Processor shall implement mechanisms for:

- Ensuring the permanent confidentiality, integrity, availability and resilience of the processing systems and services.

- Restoring availability and access to personal data in a timely manner, in the event of a physical or technical incident.

- Verifying, evaluating and assessing, on a regular basis, the effectiveness of the technical and organisational measures implemented to ensure the security of the processing.

- Pseudonymising and encrypting personal data, where appropriate.

In particular, the Parties have agreed on a list of measures to be implemented by the Processor, set out in **Appendix A** to this Data Processing Agreement.

If the Controller, subsequent to the formalisation of the Contract, requires the Processor to adopt or maintain security measures different from those agreed in this Annex I, or if they are required by any future regulation, and this significantly affects the costs of providing the Services, the Processor and the Controller shall agree on appropriate contractual measures to address the effect that such changes may have on the price of the Services.

11. Subcontracting

The Controller grants a general authorisation for the Processor to subcontract part of the Services to third-party entities or subcontractors (the "**Sub-processor**"). The Processor shall inform the Controller of the processing operations to be subcontracted and clearly and unambiguously identify the subcontracting company and its contact details. The subcontracting may be carried out if the Controller does not express its opposition within 15 days.

The Processor shall apply due diligence to choose only those sub-processors that provide sufficient guarantees to implement appropriate technical and organisational measures, so that the outsourced processing operations are in compliance with the requirements of the GDPR and the protection of the rights of data subjects subject to processing is ensured.

The Sub-processor, who shall also have the status of data processor, shall also be obliged to comply with the obligations imposed on the Processor and the instructions issued by the Controller, as set out in this Data Processing Agreement. It is incumbent upon the Processor to regulate the new relationship in a contract signed by the Processor and the Sub-Processor, so that the Sub-Processor is subject to the same conditions (instructions, obligations, security measures...) and with the same formal requirements as the initial Processor, as regards the proper processing of personal data and the guarantee of the rights of the data subjects. In the event of non-compliance by the Sub-Processor, the Processor shall remain fully liable to the Controller with regard to compliance with the obligations included in this Data Processing Agreement.

The list of the Sub-Processors authorised by the Controller is attached to this Data

Processing Agreement as **Appendix B**.

12. International data transfers

The Data Processor shall not carry out international transfers of personal data to which he/she has access, which are the responsibility of the Controller, unless he/she has prior authorisation from the Controller or they are duly regularised in accordance with the provisions of articles 45, 46 or 47 of the GDPR. Without prejudice to the authorised sub-processors referred to in Appendix B that carry out certain processing operations on behalf of the Processor in territories outside the European Economic Area, which comply wil all regulations of Chapter V in the GDPR.

13. Liability

The Processor shall be held responsible for the processing in the event that he/she uses the data subject to this Data Processing Agreement for other purposes, communicates them or uses them in breach of the stipulations of this Data Processing Agreement, and shall be liable for any infringements that he/she may have personally incurred.

The Controller shall inform the Processor immediately of any sanctioning proceedings initiated against the Data Controller by the Spanish Data Protection Agency or any other competent authority, for such breaches or defective compliance, so that the Processor may assume the legal defense at its own expense, acting at all times in coordination with the Controller and preserving its public image and reputation.

Each Party shall indemnify the other Party against claims, damages, actions and expenses arising from claims that the Party is obliged to pay under a final judgment or award rendered by a competent court, or under an agreement reached between a Party and third party claimants, resulting from non-compliance or defective compliance with the applicable law.

DATA PROCESSING AGREEMENT

This DATA PROCESSING AGREEMENT shall only apply if the CLIENT and/or SESAME HR are subject to MEXICO'S GENERAL LAW FOR THE PROTECTION OF PERSONAL DATA IN THE POSSESSION OF OBLIGATED PARTIES

Identification of the affected information and processing activities to be carried out

For the execution of services arising from compliance with the purpose of this Data Processing Agreement, the Data Controller shall make available to the Data Processor a series of personal data.

Duration

This Data Processing Agreement shall enter into force on the date of acceptance of the Contract. This Data Processing Agreement is ancillary to the contract and its duration is therefore linked to the duration of it.

Obligations of the Data Controller

The Data Controller is responsible for carrying out the following tasks, in addition to fulfilling the obligations attributed to him/her under this Data Processing Agreement:

- Comply with all the technical and organisational measures necessary to guarantee the safety of the processing, premises, equipment, systems, programs and individuals involved in the processing of the personal data, which are stipulated in the regulations in force and applicable at all times

- To deliver to the Data Processor the data referred to in clause 2 of this document, as well as the necessary instructions to carry out the processing of the data under the terms established by the Controller.

- Respond to the rights of individuals affected by the processing, such as the rights of access, rectification, erasure and objection, in collaboration with the Processor

- Ensure, before and during the processing, that the Data Processor complies with the applicable data protection regulations.

- Supervise the processing, including carrying out inspections and audits.

- Communicate to the Data Processor any changes in the personal data provided, so that they can be updated.

Duty to provide information and legitimate basis

The Controller guarantees that he/she has complied with the duty to provide all information to data subjects at the time of collection of the data undergoing processing, in compliance with the provisions of Chapter Two of the Federal Law on the Protection of Personal Data in Possession of Private Parties.

The Controller guarantees that he/she has an appropriate legitimate basis for processing the personal data that complies with the principles of effectiveness, necessity and proportionality, taking into account the existence of other protection measures that may be less invasive, avoiding discriminatory effects and establishing appropriate safeguards.

The Data Processor shall in no case be liable for the lack of compliance or defective compliance with the duty to provide information or for the application of an appropriate basis for legitimisation.

Obligations of the Data Processor

The Processor declares and warrants to the Controller the following:

- Only processing personal data following the instructions of the data controller;
- Refraining from processing personal data for purposes other than those instructed by the data controller;
- Implementing security measures following the Federal Law on the Protection of Personal Data in Possession of Private Parties, the Regulation of the Federal Law on the Protection of Personal Data in Possession of Private Parties and other applicable provisions;
- Keeping confidentiality with respect to the personal data processed;
- Deleting the personal data subject to processing once the legal relationship with the controller has been fulfilled or on the controller's instructions, provided that there is no legal provision requiring the retention of the personal data.
- Refraining from transferring the personal data except where the controller so determines, the communication arises from outsourcing, or where so required by the competent, without prejudice to the list of sub-processors in Appendix B.

As this is a cloud computing service, the Data Processor represents and warrants to the Data Controller:

- To have and implement personal data protection policies in line with the applicable principles and duties established by the Federal Law on the Protection of Personal Data in Possession of Private Parties and the Regulation of the Federal Law on the Protection of Personal Data in Possession of Private Parties.
- To provide transparent information on subcontractors involved in data processing.
- Under no circumstances shall the processor assume ownership of the data held by the

controller that it has incorporated into SESAME HR.

- The Data Processor has mechanisms in place, at least, to:
    - Communicate to the controller about changes to the processor's privacy policy and this Data Processing Agreement.
    - Enable the controller to limit the type of processing of personal data.
    - Establish and maintain appropriate security measures for the protection of personal data.
    - Ensure the erasure of personal data upon termination of the service provided to the Controller through manual erasure by the Controller or upon the Controller's request.
    - Prevent access to personal data to persons who do not have access privileges, or in the event of a well-founded and reasoned request from a competent authority, inform the data controller of this fact.

Destination of Data

Upon termination of the provision of the Services, the Processor shall return the personal data to which he/she has had access and any existing copies, as instructed by the Controller in accordance with section 13.2 of the Agreement.

The Processor may retain a copy with the data duly blocked, for as long as liabilities may arise from the performance of the provision of the Services.

Notification of data security breaches

The Processor shall notify the Controller without undue delay of any suspected or confirmed data protection incident within its area of responsibility. Such breach of security shall take the form of unauthorised loss or destruction; unauthorised theft, loss or copying; unauthorised use, access or processing; or unauthorised damage, alteration or modification.

Exercise of rights by interested parties

The Data Processor shall provide the information and/or documentation requested by the Controller in order to respond to requests for the exercise of rights that the Controller may receive from data subjects whose data are processed. The Data Processor shall provide such information within reasonable periods of time and, in any case, sufficiently in advance to enable the Controller to comply with the legally applicable deadlines for responding to the exercise of these rights.

When the data subjects exercise their rights of access, rectification, deletion, and objection, the Data Processor shall communicate this by e-mail to the address legal@sesametime.com. The communication must be made immediately in order to be dealt with within the established legal deadlines, and in no case more than two working days after receipt of the request, and must be submitted to the Data Controller together with any information that

may be relevant to its resolution.

Security

Concerning technical and organisational security measures, the Data Processor shall implement mechanisms for:

- Ensuring the permanent confidentiality, integrity, availability and resilience of the processing systems and services.
- Restoring availability and access to personal data in a timely manner, in the event of a physical or technical incident.
- Verifying, evaluating and assessing, on a regular basis, the effectiveness of the technical and organisational measures implemented to ensure the security of the processing.
- Pseudonymising and encrypting personal data, where appropriate.

In particular, the Parties have agreed on a list of measures to be implemented by the Processor, set out in **Appendix A** to this Data Processing Agreement.

If the Controller, subsequent to the formalisation of the Contract, requires the Processor to adopt or maintain security measures different from those agreed in this Annex II, or if they are required by any future regulation, and this significantly affects the costs of providing the Services, the Processor and the Controller shall agree on appropriate contractual measures to address the effect that such changes may have on the price of the Services.

Subcontracting

The Controller grants a general authorisation for the Processor to subcontract part of the Services to third-party entities or subcontractors (the "Sub-processor"). The Processor shall inform the Controller of the processing operations to be subcontracted and clearly and unambiguously identify the subcontracting company and its contact details. The subcontracting may be carried out if the Controller does not express its opposition within 15 days.

The Processor shall apply due diligence to choose only those sub-processors that provide sufficient guarantees to implement appropriate technical, physical and administrative measures so that the subcontracted processing operations are in compliance with the requirements of the Federal Act on the Protection of Personal Data held by Private Parties and the protection of the rights of data subjects subject to the processing is ensured.

The Sub-processor, who shall also have the status of data processor, shall also be obliged to

comply with the obligations imposed on the Processor and the instructions issued by the Controller, as set out in this Data Processing Agreement. It is incumbent upon the Processor to regulate the new relationship in a contract signed by the Processor and the Sub-Processor, so that the Sub-Processor is subject to the same conditions (instructions, obligations, security measures...) and with the same formal requirements as the initial Processor, as regards the proper processing of personal data and the guarantee of the rights of the data subjects. In the event of non-compliance by the Sub-Processor, the Processor shall remain fully liable to the Controller with regard to compliance with the obligations included in this Data Processing Agreement.

The list of the Sub-Processors authorised by the Controller is attached to this Data Processing Agreement as Appendix B.

International data transfers

The Processor may carry out international transfers of personal data to authorised subcontractors outside the national territory of Mexico that provide sufficient guarantees in terms of physical, technical and administrative measures.

Liability

The Processor shall be held responsible for the processing in the event that he/she uses the data subject to this Data Processing Agreement for other purposes, communicates them or uses them in breach of the stipulations of this Data Processing Agreement, and shall be liable for any infringements that he/she may have personally incurred.

Each Party shall indemnify the other Party against claims, damages, actions and expenses arising from claims that the Party is obliged to pay under a final judgment or award rendered by a competent court, or under an agreement reached between a Party and third party claimants, resulting from non-compliance or defective compliance with the applicable law.

APPENDIX A.- SAFETY MEASURES

Our infrastructure is mainly Cloud-based, we use several providers, for greater fault tolerance, and is constantly being improved.

Our application has a distributed architecture, which allows us to have separate front, api and other services necessary for the operation of the application. In addition, it allows us better scalability of the service, as we can control separately which part of the infrastructure needs to support more load.

On the other hand, we have a virtualised development environment that allows our team to make all changes in parallel and controlled by the GIT version control system, which assures the integrity of the system. As well as a continuous integration flow with Gitlab.

Development methodologies

- SOLID
- DDD (Domain Driven Design)
- Unitary Tests
- Hexagonal Architecture .
- Multiple authentication
- CI/CD with Gitlab.

Programming languages

- Backend
    - Symfony 4
    - PHP 7.x.x
    - MySQL / MariaDB.
    - Redis. or SQS (or Beanstalk)
    - S3
    - SQS
- Frontend
    - VueJS
    - Tailwind
    - Library of proprietary logic components.
- Apps
    - VueJS
    - Capacitor
    - Typescript
- Sockets
    - NodeJS
    - Express
    - Typescript
    - SocketIO.

Infrastructure

The following infrastructure technologies are available to process all the information:

- Debian 10
- Docker
- K8S
- AWS
- Google Cloud
- OVH Cloud
- Proxmox
- HAProxy
- Cloudflare

Our systems department will be responsible for ensuring that the servers have the necessary software for the correct functioning of the application.

Providers

- OVH Cloud
- So You Start
- AWS
- Google Cloud
- Cloudflare
- Dockerhub

Database Servier

- Relational (sql): for relational databases, we will use MaríaDB - Database must have a utf8 coding.
- We have a user with the following permissions:
    - Scheme (Create objects): Yes (create, modify and delete tables).
    - Writing (SUDI Select, Update, Delete e Insert): yes.
    - Reading (SELECT): yes.

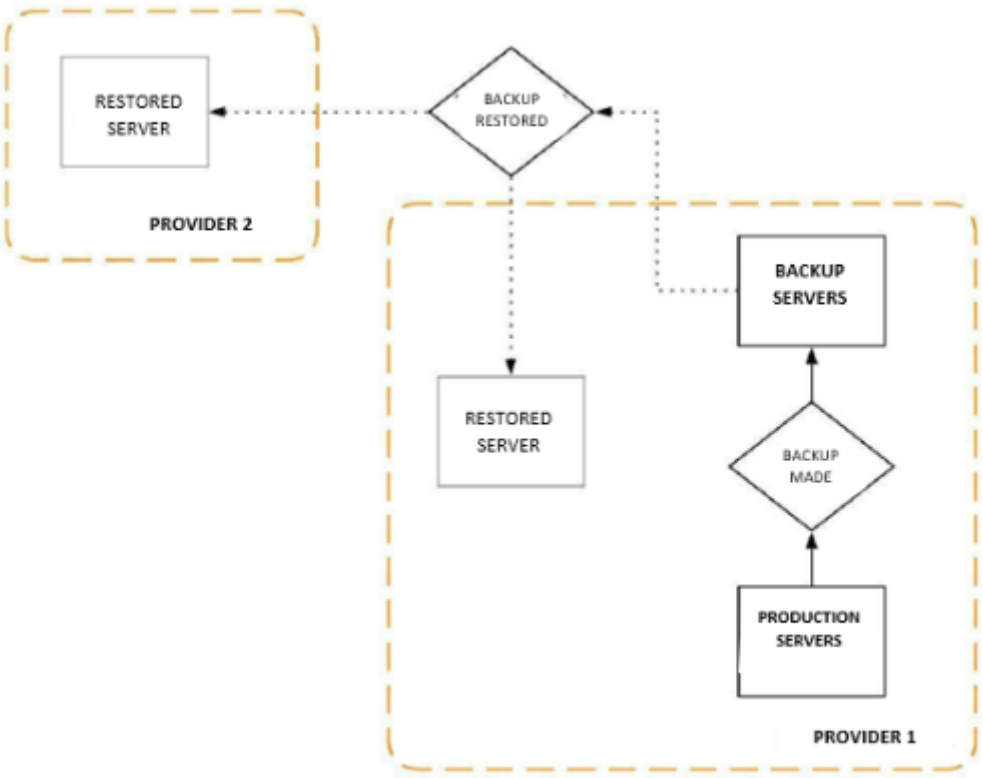
Backups are performed weekly full and daily incremental backups. From our database server we keep a copy of the copies on a monthly, weekly and daily basis, stored on our slave server. In addition, hourly copies are also made of our main server database.

We keep copies of all web server content, and copies of critical service configuration files.

We use a backup server in France which is redundant in Poland to ensure the availability of backups in case of disaster.

The administrator of the information systems or IT department or the one acting in its stead is the designated manager who will draw up a procedure for testing the backups and testing the restoration of the backups on a monthly basis.

In the event of recovery of a copy, the following procedure shall be followed:



Infrastructure security measures
Datacenter

Our servers are contracted to OVH, number one in Europe and third in the world in web hosting, which has more than 150,000 physical servers. OVH's success lies in the total control it exercises over the hosting chain, including the production of its servers. OVH is known for the special attention it pays to the selection of the components of its machines, demanding the highest quality.

Each server is systematically subjected to a series of tests to verify its technical conformity and its good behaviour under all circumstances. As soon as the machine leaves production,

it is installed and connected in the OVH datacentres. A robot then checks that the hardware is as ordered by the customer and that its performance meets the specifications.

The check points are as follows:

- processors: compliance, load test, temperature;
- RAM memory: size, memtest;
- BIOS: BIOS version, virtualisation;
- disks: speed, SMART test, firmware version, etc.

We also have contracted services on AWS. AWS have been pioneering cloud computing since 2006, creating a cloud infrastructure that allows you to create securely and innovate faster. Their data centres are designed to protect against natural and man-made hazards. They implement controls, develop automated systems and undergo third-party audits to confirm security and compliance.

Data centres are designed to anticipate and tolerate errors while maintaining service levels. In the event of an error, automated processes divert traffic away from the affected area. Core applications are deployed on an N+1 standard, so that in the event of a failure in one data centre, there is sufficient capacity to be able to load balance traffic between the other sites.

AWS monitors and performs preventive maintenance on electrical and mechanical equipment to maintain the constant operation of the systems installed in AWS data centres. Equipment maintenance procedures are performed by qualified persons and are carried out in accordance with a documented maintenance schedule.

Protection against attacks

Our servers use the anti-DDoS infrastructure deployed by OVH to protect servers 24 hours a day against any type of DDoS attack, regardless of its duration and scale.

The objective of a DDoS attack is to bring down a server, a service or an infrastructure by sending multiple simultaneous requests from multiple points on the network.

The intensity of this ‘crossfire’ destabilises the service, or worse, disables it. This infrastructure allows:

- analysing all packets in real time and at high speed,
- to suck incoming traffic from the server,
- mitigate, i.e. identify all illegitimate IP packets, but let legitimate IP packets through.

Security

Sesame is very conscious of security, data processing and data leakage. That is why we work every day to improve security, maintaining clear objectives in this area. For this reason, we will now go into more detail about the different aspects we deal with in terms of security, both in the application and in the infrastructure:

Cloud providers: Sesame uses different cloud providers to provide the highest possible availability and scalability for the application. All our providers have at least the following security certifications:

- ISO/IEC 27001, 27017 and 27018
- PCI DSS Level 1
- GDPR Compliance with EU Regulation 2016/679 on General Data Protection.
- SSAE 18 of Type 2: SOC 1, SOC 2 and SOC 3

Access to these providers is only granted to employees with a very high level of accreditation in the company, almost always by an area or systems manager.

Servers: Access to servers is restricted to employees with a high level of accreditation. Access to the servers will use a 2048-bit RSA encrypted key pair and will include a nominal user password which allows for logging of user access as well as detailed movement of changes or alterations to the machines for possible auditing at a later date.

Third party tools: Sesame uses third party security tools such as Tenable.io which inventories all our machines and domains we use and periodically launches vulnerability and intrusion audits. Therefore every week our experts have new reports which indicate possible security breaches that according to Tenable's AI algorithm will be patched with the recommended order of priority.

Access to the application: Access to the platform will always be through our CDN and DNS provider CloudFlare which has an integrated state-of-the-art WAF capable of detecting and mitigating attacks that target the application directly.

Patching policy

All services, and the infrastructure that supports them, accessible from the Internet, whether they are for internal company use or for our clients, follow a policy of agile security updates. These services are patched as soon as we become aware of a bug or important vulnerability. In the case of non-critical updates, patching is scheduled monthly or quarterly depending on our needs and the application.

Internal services (printers, local user network equipment, telephone switchboards, etc.) have a policy of regular scheduled updates (every six months, every year, etc.) according to needs and carried out by the company's IT department.

We also have a virus alert system, ClamAV.

APPENDIX B- SUBPROCESSORS LIST

OVH

Usage: This applies to the required use of the platform. This provider applies worldwide except for countries in the Americas (except the USA and Canada).

Sub-processor's name: OVH SAS

Current Processing Location: France and Germany

Link to the security policy of the sub-processor:
https://us.ovhcloud.com/personal-data-protection/security/

Amazon Web Services

Usage: This applies to the required use of the platform. This provider applies worldwide except for countries in the Americas (excluding the USA and Canada).

Sub-processor's name: Amazon Web Services

Current Processing Location: France and Germany

Link to the security policy of the sub-processor:
https://aws.amazon.com/compliance/?nc1=h_ls

Mailchimp

Usage: This applies to the required use of the platform. This provider applies worldwide.

Sub-processor's name: The Rocket Science Group (Mailchimp)

Current Processing Location: United States

Link to the security policy of the sub-processor: https://mailchimp.com/gdpr/

International transfer for the purposes of the GDPR: The subprocessor is a signatory to the EU-U.S. Data Privacy Framework.

Signaturit

Usage: This applies to the use of the electronic signature feature (only if this is enabled, this is used). This provider applies worldwide.

Sub-processor's name: Signaturit Solutions S.L

Current Processing Location: Spain

Link to the security policy of the sub-processor:
https://www.signaturit.com/privacy-policy/

OPEAN AI

Usage: This applies in case of hiring and using SESAME AI.

Sub-processor's name: OPEAN AI
Current Processing Location: United Stated
International transfer for the purposes of the GDPR: According to the privacy policy of the Subprocessor

Link to the security policy of the sub-processor: https://openai.com/policies/privacy-policy/

AUREN

Usage: This applies in case of hiring and using the Payroll Management tool.

Sub-processor's name: AUREN LEGAL SP, S.L.P

Current Processing Location: Spain

Link to the security policy of the sub-processor:
https://auren.com/es/en/privacy-policy/

IPXON

Usage: This applies to the required use of the platform. This provider applies for countries in the Americas (except the USA and Canada).

Sub-processor's name: CONEXUM INC (IPXON Networks)

Current Processing Location: Brazil (Only for Customers registered in countries in the Americas except USA and Canada)
Link to the security policy of the sub-processor: https://www.ipxon.com/es-br/privacidad

SWAN

Usage: This provider applies in case of hiring and using Expense Management and Salary in Advance.
Sub-processor's name: SWAN SAS
Current Processing Location: France
Link to the security policy of the sub-processor: https://www.swan.io/privacy-policy