Privacy and Security Information

- **Does Signaturit comply with the GDPR?**

Data security and privacy are top priorities for Signaturit. To demonstrate our dedication to security and privacy, we have obtained ISO 27001 certification and we are in full compliance with the EU GDPR. Our legal team has analyzed the requirements of the GDPR and enhanced our policies, procedures, contracts and platform features to ensure we comply with the GDPR and enable compliance for our customers.

- **Data Processing Agreement**

The relationship between the Controller and the Processor must be established through a Data Processing Agreement (DPA), whose content is regulated and determined in article 28 of the GDPR. Such DPA must be done in writing or in electronic format.

The aforementioned DPA must identify the key points that all data controllers shallt bear in mind when establishing relationships or hiring services that imply the processing of data.

- **Signaturit's sub-processors:**

a)
Legal entity: Amazon Web Services EMEA SARL
Registered address: 38 avenue John F Kennedy, L-1855 Luxemburg
Business activity: Cloud computing services
Servers: Ireland
Purpose of the engagement: Use of data servers in Ireland for storage purposes.

b)
Legal entity: Zendesk, Inc
Registered address: 1019 Market Street, San Francisco, CA 94103, United States
Business activity: Integrated Customer Support
Servers: Ireland
Purpose of the engagement: Platform used for tickets related to customer support. Only used if support is needed.

c)
Legal entity: Atlassian Pty Ltd
Registered address: 341 George Street, Sydney, NSW 2000
Business activity: tracking, collaboration, communication, service management, and development software products for teams in organizations
Servers: Ireland
Purpose of the engagement: Project Management. In case of support of the Data Controller, there is a chance data from the Data Controller will be processed in the platform.

d)
Legal Entity: SendGrid, Inc.
Registered address: 1801 California Street, Suite 500, Denver, CO 80202

Business activity: Digital communication platform.
Servers: United States.
Implemented guarantees: Data Processing Agreement with the requirements of art. 28 of the RGPD, regulating international data transfers through Standard Contractual Clauses.
Purpose of the processing: Platform used to send all emails of Signaturit's platform.

e)
Legal entity: Mailgun Technologies, Inc.
Registered address: 600 North Whisman Road Suite 33, Mountain View, CA 94043
Business activity: Digital communication platform
Servers: United States.
Implemented guarantees: Data Processing Agreement with the requirements of art. 28 of the RGPD, regulating international data transfers through Standard Contractual Clauses.
Purpose of the processing: Platform that we use to parse and capture the petitions that are made using the MX signaturit.com domain and thus capture the emails.

f)
Legal entity: Plivo Inc.
Activity: B2B communication and messaging platform (provision of SMS and mailing services)
Servers: United States
Implemented guarantees: DPA in compliance with the requirements of article 28 of the GDPR regarding international transfer of personal data under standard contractual clauses.
Purpose of engagement: platform we use to send OTP codes through SMS which are necessary to finish certain signature petitions.

- **Signaturit has the ISO27001 certification and conducts GDPR audits every two years.**

Signaturit has the certification ISO27001 regarding its International Security Management System and every two years conducts an external Data Protection Impact Assessment with independent expert auditors.

- **The services provider implements the appropriate technical and organizational measures so that the information that is stored is not lost damage or corrupted. The location of the data center meets the privacy protection requirements appropriate to the personal data that is hosted therine, according to the GDPR.**

Once the document is signed within Signaturit's platform, Signaturit collects all personal data and -within the advanced electronic signature process- also collects the biometric data associated to the signer's graph (acceleration, speed, pressure). All data is encrypted and stored in Signaturit's AWS S3 servers which encrypts the data again (AES 256). In this sense there is a double encryption and Signaturit makes a Dataset backup in a daily basis.

On the other hand, AWS is compliant with all GDPR requirements and has executed a DPA with Signaturit. Regarding the HSM (Hardware Security Module) we have two modules in order to have a backup system. Signaturit complies with the accountability principle and following, among others, the principle of privacy by design it has designated a DPO, it conducts a Data Protection Impact Assessment every two years, and follows the principles of segregation of duties and least privilege (GDPR Requirements).

Apart from that and in terms of our Information Security Management System, we follow a Backup Policy, Control Access Policy, an Information Classification Policy, etc. (ISO 27001, Information Security Requirements).

- **Security means taken by the vendor to preserve data, such as updates, backups, audits, fire measures, etc.**

Signaturit has a Business Continuity and Disaster Recovery Plan where all disaster scenarios are contemplated. In this sense, has a Backup Policy and do backup test for Database and services periodically.

Signaturit is certified under ISO 27001 every year are pass audits on this matter and all audits related to Qualified Trusted Services which include extra features in terms of security and pass externals DPIA every two years and the Data Protection Officer of the company checks/reviews the data processes and flows in the company at least two times per year.

- **Data and processes stored in the facilities of the services provider are not accessed or used by third parties. The services provider offers guarantees that the data is separated and is not accessible by other customers.**

No customer can access or use any information (personal data or other) from databases of Signaturit. Only trusted personnel (PKI members) can access to sensitive information according to our Roles, Responsibilities and Authorities of the Organization Policy.

Another matter to take into account is that all the machines in Signaturit are private and placed inside a VPC and can't be reached from the internet. Inside the VPC we have all the machines and databases, and each environment has a different VPC with all the necessary resources deployed, without sharing resources and data between environments.

The access to the machines and databases is managed by the AWS security groups and route tables. In these resources we limit the open ports, to the ones that are only necessary for the provision of the services and database. We also control the resources that a service can access with unique IAM roles per service. We follow the Principle of Least Privilege (PoLP) rule, where the services and users do nots have privileged permissions.

All the machines have the audit log enabled and we send the logs to Datadog, where we parse and monitor them, creating alarms for any suspicious actions. The logs are also stored in our audit account in AWS, where we centralize all the security logs, and no one can modify them.

- **Data stored by the services provider are not accessed or used by the service provider for purposes other than those established in the DPA.**

Signaturit does not access or use information (personal data) for different purposes than those established in the Data Processing Agreement, which are necessary to provide the service. In this sense, the company follows security policies like minimisation, anonymization, least privilege or separation of duties and besides all data is automatically encrypted as stated above.

In this sense, Signaturit conducts impact assessments every two years and the Data Protection Officer of the company checks/reviews the data processes and flows in the company at least two times per year.

- **Security is enforced in data transfers.**

Signaturit has executed a Data Processing Agreement with its sub-processors according to GDPR EU Standard Contractual Clauses. Apart from this, it counts with an Information Security Policy, an

Information Classification Policy and a Supplier and Partner Collaborator Security Policy.

- **Flexibility or how they scale up their services if our needs increase or decrease.**

Signaturit uses AWS S3 which is a simple storage service that offers an infrastructure to store data with an extremely high level of durability, availability and scalability. In this way, there is no inconvenient to adapt the service to the needs of the company and its customers

- **Portability options when the service ends or if conditions are changed.**

Signaturit always sign a Data Processing Agreement with its customers and there can be specified concretely the way to exercise the portability options.

- **Implementing business continuity measures to ensure continuity in the event of an incident or disaster affecting the services provider's facilities.**

Signaturit has a Business Continuity and Disaster Recovery Plan and a Recovery Plan of the PKI. In this sense, we implement tests to assess the continuity and the capacity to recovery of our services on a periodic basis.

- **Control and monitoring**

The controls we carry out at Signaturit for the supervision and monitoring of production systems begin with development, code reviews, unit tests, integration test in QA environment, integration in QA environment, functional tests in QA environment, integration in pre-production, integration in production and monitoring of the production system through different systems/suppliers. A redundancy pattern is implemented in all services. In case of a system crash, we have teams carrying out guards for its restoration. As well as redundancy in all data (backup) that ensures the integrity of the data.

- **Location of documents**

All documents and information of our clients is stored in servers located within the EU and in no case they are transferred to other destinations outside of it. We currently have data centers available in Ireland and Germany.

- **Backup procedures**

Signaturit has established a data backup and recovery system so that, in the event of loss or destruction, it can be rebuilt and returned to its original state. The platform is responsible for making daily backup copies of the data through the AWS S3 service, making the availability of these copies greater than 99.99%.

- **Access Firewalls**

The Amazon Web Services platform allows the configuration of security groups to limit the access to each of the server ports. A security group is a set of rules that allow or deny entry or exit to the ports of a the server according to specifications.

Signaturit's platform is configured so that each of our servers is as restrictive as possible, establishing security groups with very specific rules to allow public access only to those that are an essential requirement for the proper functioning of the system.

- **Encrypted communications**

When browsing the Internet, the addresses of the websites we visit are headed by the HTTP or HTTPS acronym. The acronym HTTP stands for “Hyper Text Transport Protocol”. It is a system designed with the purpose of defining and standardizing the synthesis of the transactions that are carried out between the different computers that make up a network. That is to say, the protocol is in charge of making sure that the data arrives and does it well. The main characteristic of this protocol is that it is a "request-response" type operation-oriented system. This means that in the structure there must be a client and a server: the client is the one who makes the requests and the server who answers it.

Along the same lines is the HTTPS protocol, whose acronym stands for Hypertext Transfer Protocol Secure. This protocol raises a fundamental issue in the use of the Internet: security. The HTTPS system is based on a combination of two different protocols: HTTPS and SSL / TLS. This system is the safest to access the contents offered by the Internet, since any information that we enter will be encrypted, which guarantees that it cannot be seen by anyone but the client and the server. In this way, the possibility that said information can be used is inexistent, since whoever tries to see it will only find data that they will not be able to decipher.

The use of the HTTPS protocol is essential for any activity that involves the use of personal data: operations through online banking entities, online purchases, sending emails and in any other activity for which we must enter passwords, credit card numbers or other personal information.

The HTTPS protocol not only provides encryption of connections but can also ensure that the web we connect to is really the one it claims to be. At Signaturit, all the connections between the different servers or clients (server - server, server - client) are made through HTTPS connections, which ensure end-to-end data encryption.

- **Accountability principle**

The GDPR, in its article 24, describes this principle as the need for the controller to apply appropriate technical and organizational measures in order to guarantee and be able to demonstrate that the processing is done in accordance with the Regulation. The measures adopted by Signaturit are, among others:

- Appointment of a Data Protection Officer
- Data protection by design and by default
- Execution of Data Processing Agreements
- Record of processing activities
- Notification of a breach of personal data security to the data protection authority
- Risk analysis

- **Data Protection Impact Assessment (DPIA)**

A Data Protection Impact Assessment (DPIA) is a process to help the processor to identify and minimise the data protection risks of a project. Any company performing a processing that is likely to result in a high risk to individuals shall conduct a DPIA. Article 35 of the GDPR covers Data Protection Impact Assessments. The DPIA is a new requirement under the GDPR as part of the “protection by design” principle. According to the law:

“Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data”.

In this sense, Signaturit carries out DPIAs each two years by third-party experts in the field. In addition, it conducts security audits and has a dedicated security team.

- **Data Breach Notification**

The Security and Legal teams will notify the data breach to the relevant parties within 24 hours of determining that the exposure has occurred.

- **Data Protection Officer**

Signaturit has a dedicated team in charge of Data Protection.

Contact: Data Protection Officer dpo@signaturit.com

c. Avila 29 08005 Barcelona

- **Security Policies**

As a company certified under the ISO 27001 standard, we have adopted the following security policies, among others:

- Backup Policy
- Business Continuity and Disaster Recovery Plan
- Recovery Plan of the PKI
- Incident Management Procedure
- Incident Response Plan
- Disposal and Destruction Policy
- Information Security Policy
- Information Classification Policy
- Access Control Policy
- Risk Assessment and Risk Methodology
- Supplier and Partner/Collaborator Security Policy