Información sobre Seguridad y Privacidad

- **Signaturit cumple con el RGPD y LOPDGDD**

La seguridad y la privacidad de los datos son las principales prioridades de Signaturit. Para demostrar nuestra dedicación a la seguridad y la privacidad, hemos obtenido la certificación ISO 27001 y cumplimos con el RGPD de la UE. Nuestro equipo legal ha analizado los requisitos del RGPD y mejorado nuestras políticas, procedimientos, contratos y características de la plataforma para garantizar que cumplimos con el RGPD y permitir el cumplimiento por parte de nuestros clientes.

- **Contrato de Encargado de Tratamiento**

La relación entre el Responsable y el Encargado del Tratamiento debe establecerse mediante un Contrato de Encargado de Tratamiento de Datos ("DPA"), cuyo contenido se regula y determina en el artículo 28 del RGPD. Debe realizarse por escrito o en formato electrónico.

El mencionado DPA deberá identificar los puntos clave que todo responsable del tratamiento debe tener en cuenta a la hora de establecer relaciones o contratar servicios que impliquen un tratamiento de datos personales por parte del proveedor.

- **Nuestros Subencargados de Tratamiento:**

a)
Entidad legal: Amazon Web Services EMEA SARL
Domicilio social: 38 avenue John F Kennedy, L-1855 Luxemburg
Actividad: Cloud computing services
Servidores: Irlanda
Razón del tratamiento: Uso de servidores para almacenamiento

b)
Entidad legal: Zendesk, Inc
Domicilio social: 1019 Market Street, San Francisco, CA 94103, United States
Actividad: Soporte al RESPONSABLE integrado
Servidores: Irlanda

Razón del tratamiento: Plataforma utilizada para los tickets de atención al RESPONSABLE.

c)

Entidad legal: Atlassian Pty Ltd

Domicilio social: 341 George Street, Sydney, NSW 2000

Actividad: productos de software de seguimiento, colaboración, comunicación, gestión de servicios y desarrollo para equipos en organizaciones

Servidores: Irlanda

Razón del tratamiento: Gestor de proyectos.

d)

Entidad legal: SendGrid, Inc.

Domicilio social: 1801 California Street, Suite 500, Denver, CO 80202

Actividad: Plataforma de comunicación digital

Servidores: Estados Unidos.

Garantías adecuadas: Contrato encargado del tratamiento con los requisitos del art. 28 del RGPD, regulando las transferencias internacionales de datos mediante
Cláusulas Contractuales Tipo.

Razón del tratamiento: Plataforma utilizada para remitir los correos de la plataforma de Signaturit.

e)

Entidad Legal: Mailgun Technologies, Inc.

Domicilio social: 600 North Whisman Road Suite 33, Mountain View, CA 94043

Actividad: Plataforma de comunicación digital

Servidores: Estados Unidos.

Garantías adecuadas: Contrato encargado del tratamiento con los requisitos del art. 28 del RGPD, regulando las transferencias internacionales de datos mediante
Cláusulas Contractuales Tipo.

Razón del tratamiento: plataforma que utilizamos para parsear y capturar la peticiones que se realizan usando el dominio MX signaturit.com y así poder capturar los correos.

f)

Entidad Legal: Plivo Inc.

Domicilio social: 601 S Congress Ave, STE 220,The Littlefield Building, Austin, TX 78701

Actividad: Plataforma de comunicación y mensajería para empresas (servicios de SMS y mailing, entre otros).
Servidores: Estados Unidos
Garantías adecuadas: Contrato de encargado de tratamiento con los requisitos del art. 28 del RGPD, regulando las transferencias internacionales de datos mediante Cláusulas Contractuales Tipo.
Razón del tratamiento: plataforma que utilizamos para enviar códigos OTP mediante SMS, necesarios para completar determinadas peticiones de firma.

- **Signaturit ha obtenido la certificación ISO27001 y realiza auditorías de RGPD bienalmente**

Signaturit cuenta con la certificación ISO27001 respecto de su Sistema de Gestión de Seguridad de la Información y cada dos años realiza una Evaluación de Impacto de Protección de Datos externa, mediante auditores especialistas y ajenos a la empresa.

- **El prestador de servicios cuenta e implementa las medidas técnicas y organizativas adecuadas para que la información que se almacena no se pierda, dañe o corrompa.**

Sí, la ubicación del centro de datos cumple con los requisitos de protección de la privacidad correspondientes a los datos personales que se alojan allí, de acuerdo con el RGPD.

Una vez que el documento se firma dentro de la plataforma, Signaturit recopila todos los datos personales y, dentro del proceso de firma electrónica avanzada, los datos biométricos relativos al grafo del firmante (aceleración, velocidad, presión), los cifra y los almacena en los servidores AWS S3, que vuelve a cifrar los datos (AES 256). En este sentido existe un doble cifrado y Signaturit realiza una copia de seguridad del Dataset a diario.

Por otro lado, AWS cumple con todos los requisitos de GDPR y existe un DPA entre las partes. En cuanto al HSM (Hardware Security Module) contamos con dos módulos para poder tener un sistema de respaldo. Signaturit cumple con el principio de responsabilidad siguiendo, entre otros, el principio de privacidad por diseño, ha designado un DPO, conduce una Evaluación de Impacto de Protección de Datos cada dos años, siguiendo los principios de segregación de funciones y privilegio mínimo, etc. (Requisitos GDPR).

Asimismo, y dentro de los términos de nuestro Sistema de Gestión de Seguridad de la Información, seguimos una Política de Respaldo, una Política de Control de Acceso, una Política de Clasificación de la Información, etc. (ISO 27001, Requisitos de Seguridad de la Información).

- **Medios de seguridad adoptados por el proveedor para preservar datos, como actualizaciones, copias de seguridad, auditorías, medidas contra incendios, etc.**

Signaturit cuenta con un Plan de Continuidad del Negocio y Recuperación de Desastres donde se contemplan todos los escenarios de desastres. En este sentido, cuenta con una Política de Backup y realiza pruebas de backup para Base de Datos y servicios periódicamente con el objetivo de asegurar la disponibilidad de la información.

Asimismo, Signaturit está certificada bajo la norma ISO 27001 y realiza auditorías cada año en esta materia y todas las auditorías relacionadas con los Servicios de confianza cualificados que incluyen características adicionales en términos de seguridad. Asimismo se realizan superan DPIA externos cada dos años y el Oficial de Protección de Datos de la empresa verifica/revisa los datos, procesos y flujos en la empresa al menos dos veces al año.

- **Los datos y procesos almacenados en las instalaciones del prestador de servicios no son accesibles ni utilizados por terceros y se ofrecen garantías de que los datos están separados y no son accesibles por parte de otros clientes.**

Ningún cliente puede acceder o utilizar ninguna información (datos personales u otros) de las bases de datos de Signaturit. Solo el personal de confianza (miembros de PKI) podrá tener acceso a la información sensible de acuerdo con nuestros roles, responsabilidades y autoridades de la política de la organización.

Otra cuestión a tener en cuenta es que todas las máquinas de Signaturit son privadas y están ubicadas dentro de una VPC y no se puede acceder a ellas desde Internet. Dentro de la VPC tenemos todas las máquinas y bases de datos, y cada entorno tiene una VPC diferente con todos los recursos necesarios desplegados, sin compartir recursos y datos entre entornos. El acceso a las máquinas y las bases de datos lo administran los grupos de seguridad y las tablas de rutas de AWS. A partir de estos recursos limitamos los puertos abiertos, los que solo son necesarios para los servicios y la base de datos.

También controlamos los recursos a los que puede acceder un servicio con roles de IAM únicos por servicio. Seguimos la regla del Principio de Privilegio Mínimo (PoLP), donde los servicios y los usuarios no tienen permisos privilegiados. Todas las máquinas tienen habilitado el log de auditoría y enviamos los logs a Datadog, donde los analizamos y monitoreamos, creando alarmas para cualquier acción sospechosa. Los registros también se almacenan en nuestra cuenta de auditoría en AWS, donde centralizamos todos los registros de seguridad y nadie puede modificarlos.

- **Los datos almacenados por el proveedor de servicios no son accedidos ni utilizados por el proveedor de servicios para fines distintos a los establecidos en el DPA.**

Signaturit no accede ni utiliza información (datos personales) para fines distintos a los establecidos en el DPA. En este sentido, la empresa sigue políticas de seguridad como minimización, anonimización, privilegio mínimo o separación de funciones y además todos los datos se encriptan automáticamente. En este sentido, Signaturit cuenta cada dos años con una DPIA externa y el Delegado de Protección de Datos de la empresa verifica/revisa los procesos y flujos de datos en la empresa al menos dos veces al año.

- **Seguridad que aplican en las transferencias de datos.**

Signaturit ha celebrado un DPA con sus subencargados del tratamiento de acuerdo con las cláusulas contractuales estándar de la UE de GDPR. Aparte de esto, tiene una Política de Seguridad de la Información, una Política de Clasificación de la Información y una Política de Seguridad de Proveedores y Colaboradores Socios.

- **Flexibilidad o cómo escalan los servicios si nuestras necesidades aumentan o disminuyen.**

Signaturit utiliza AWS S3, que es un servicio de almacenamiento simple que ofrece una infraestructura para almacenar datos con un nivel extremadamente alto de durabilidad, disponibilidad y escalabilidad. De esta forma no tenemos inconvenientes a la hora de adaptar el servicio a las necesidades de la empresa y sus clientes y sus crecientes necesidades.

- **Opciones de portabilidad cuando finaliza el servicio o si se cambian las condiciones.**

Signaturit firma siempre un Contrato de Tratamiento de Datos con sus clientes y se puede concretar específicamente la forma de ejercitar las opciones de portabilidad.

- **Implementa medidas de continuidad comercial para garantizar la continuidad en caso de un incidente o desastre que afecte sus instalaciones.**

Signaturit cuenta con un Plan de Continuidad de Negocios y Recuperación ante Desastres y un Plan de Recuperación de la PKI. En este sentido, implementamos pruebas para asegurar la continuidad y la capacidad de recuperación de nuestros servicios periódicamente.

- **Control y seguimiento**

Los controles que realizamos en Signaturit para la supervisión y seguimiento de los sistemas de producción comienzan con el desarrollo, revisiones de código, pruebas unitarias, prueba de integración en ambiente QA, integración en ambiente QA, pruebas funcionales en ambiente QA, integración en preproducción, integración en producción y seguimiento del sistema de producción a través de diferentes sistemas/proveedores. Se implementa un patrón de redundancia en todos los servicios. En caso de caída del sistema, contamos con equipos realizando guardias para su restauración. Así como redundancia en todos los datos (backup) que asegura la integridad de los datos.

- **Ubicación de los documentos**

Todos los documentos e información de nuestros clientes se almacenan en nuestros servidores ubicados dentro de la UE y en ningún caso se transfieren a otros destinos fuera de ella. Actualmente tenemos centros de datos disponibles en Irlanda y Alemania.

- **Procesos de backup**

Signaturit ha establecido un sistema de respaldo y recuperación de datos para que, en caso de pérdida o destrucción, se pueda reconstruir y devolver a su estado original. La plataforma se encarga de realizar copias de seguridad diarias de los datos a través del servicio AWS S3, haciendo que la disponibilidad de estas copias supere el 99,99%.

- **Firewalls**

La plataforma Amazon Web Services permite la configuración de grupos de seguridad para limitar el acceso a cada uno de los puertos del servidor. Un grupo de seguridad es un conjunto de reglas que permiten o niegan la entrada o salida a los puertos de un servidor según especificaciones.

La plataforma de Signaturit está configurada para que cada uno de nuestros servidores sea lo más restrictivo posible, estableciendo grupos de seguridad con reglas muy específicas para permitir el acceso público solo a aquellos que resultan imprescindibles para el correcto funcionamiento del sistema.

- **Comunicaciones encriptadas**

Al navegar por Internet, las direcciones de los sitios web que visitamos están encabezadas por las siglas HTTP o HTTPS. El acrónimo HTTP significa "Protocolo de transporte de hipertexto". Es un sistema diseñado con el propósito de definir y estandarizar la síntesis de las transacciones que se llevan a cabo entre los diferentes equipos que componen una red. Es decir, es el protocolo encargado de que los datos lleguen y lo haga bien. La característica principal de este protocolo es que es un sistema orientado a operaciones de tipo "solicitud-respuesta". Esto significa que en la

estructura debe haber un cliente y un servidor: el cliente es el que hace las solicitudes y el servidor quien las responde.

En la misma línea está el protocolo HTTPS, cuyas siglas significan Hypertext Transfer Protocol Secure. Este protocolo plantea una cuestión fundamental en el uso de Internet: la seguridad. El sistema HTTPS se basa en una combinación de dos protocolos diferentes: HTTPS y SSL / TLS. Este sistema es el más seguro para acceder a los contenidos que ofrece Internet, ya que cualquier información que ingresemos estará encriptada, lo que garantiza que no puede ser vista por nadie más que el cliente y el servidor. De esta forma se cancela la posibilidad de que se pueda utilizar dicha información, ya que quien intente verla solo encontrará datos que no podrá descifrar.

El uso del protocolo HTTPS es fundamental para cualquier actividad que implique el uso de datos personales: operaciones a través de entidades de banca online, compras online, envío de correos electrónicos y en cualquier otra actividad para la que debamos introducir contraseñas, números de tarjetas de crédito u otra información personal.

El protocolo HTTPS no solo proporciona cifrado de conexiones, sino que también puede garantizar que la web a la que nos conectamos es realmente la que dice ser. En Signaturit, todas las conexiones entre los diferentes servidores o clientes (servidor - servidor, servidor - cliente) se realizan a través de conexiones HTTPS, que aseguran el cifrado de datos de extremo a extremo.

- **Principio de responsabilidad proactiva**

El RGPD, en su artículo 24, describe este principio como la necesidad de que el responsable del tratamiento aplique las medidas técnicas y organizativas adecuadas para garantizar y poder demostrar que el tratamiento es conforme al Reglamento. Las medidas adoptadas por Signaturit son, entre otras:

- Nombramiento de un Delegado de Protección de Datos
- Protección de datos por diseño y por defecto
- Acuerdos de procesamiento de datos
- Registro de actividades de tratamiento
- Notificación de una violación de la seguridad de los datos personales a la autoridad de protección de datos.
- Evaluaciones de impacto en materia de protección de datos

- **Evaluaciones de Impacto de Protección de Datos**

Una Evaluación de Impacto de Protección de Datos (EIPD) es un proceso para identificar y minimizar los riesgos del tratamiento de datos. Cualquier empresa que realice un tratamiento de datos que pueda implicar un alto riesgo para las personas (sujetos interesados), debe realizar una EIPD. El artículo 35 del RGPD regula las evaluaciones de impacto de la protección de datos. La EIPD es un nuevo requisito bajo el RGPD como parte del principio de "protección por diseño". De acuerdo con la ley:

"*Cuando un tipo de procesamiento, en particular utilizando nuevas tecnologías, y teniendo en cuenta la naturaleza, alcance, contexto y propósitos del procesamiento, pueda resultar en un alto riesgo para los derechos y libertades de las personas físicas, el controlador deberá, antes al tratamiento, realizar una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales".*

En este sentido, Signaturit lleva a cabo EIPD bienales a cargo de terceros expertos en la materia. Además, realiza auditorías de seguridad y tiene un equipo de seguridad dedicado.

- **Notificaciones de brechas de seguridad**

Los equipos de seguridad y legal notificarán a quien corresponda el acaecimiento de una violación de datos dentro de las 24 horas posteriores a la determinación de que se ha producido la exposición.

- **Delegado de Protección de Datos**

Signaturit cuenta con un equipo dedicado a cargo de la protección de datos.

Contacto:
Delegado de Protección de Datos dpo@signaturit.com
C. Ávila 29 08005 Barcelona

- **Políticas de seguridad**

Como empresa certificada bajo la norma ISO 27001, hemos adoptado las siguientes políticas de seguridad, entre otras:

- *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*