Informations sur la sécurité et la confidentialité

• Signaturit est-il conforme au RGPD ?

La sécurité et la confidentialité des données sont les principales priorités de Signaturit. Pour démontrer notre attachement à la sécurité et à la confidentialité, nous avons obtenu la certification ISO 27001 et sommes conformes au RGPD de l'UE. Notre service juridique a analysé les exigences du RGPD et a amélioré nos politiques, procédures, contrats et fonctionnalités de la plateforme pour nous assurer que nous nous conformons au RGPD et que nous permettons la conformité pour nos clients.

• Contrat de sous-traitant des données (DPA)

La relation entre le responsable et le sous-traitant doit être établie au moyen d'un accord de sous-traitant des données, dont le contenu est réglementé et déterminé à l'article 28 du RGPD. Le DPA doit être sous forme écrite ou électronique.

Le DPA susmentionné doit identifier les points clés que tout responsable du traitement doit prendre en compte lors de l'établissement de relations ou de la sous-traitance de services sous traitement des données.

• Nos sous-traitants :

a)
Entité juridique : Amazon Web Services EMEA SARL
Siège social: 38 avenue John F Kennedy, L-1855 Luxembourg
Activité : Services informatiques hébergés
Serveurs : Irlande
Motif du traitement : Utilisation de serveurs pour stockage

b)
Entité juridique : Zendesk, Inc
Siège social : 1019 Market Street, San Francisco, CA 94103, United States
Activité : Support au RESPONSABLE intégré
Serveurs : Irlande
Motif du traitement : Plateforme utilisée pour les tickets d'assistance au RESPONSABLE

c)
Entité juridique : Atlassian Pty Ltd
Siège social : 341 George Street, Sydney, NSW 2000
Activité : Produits de logiciels de suivi, collaboration, communication, gestion de services et développement pour équipes dans organisations
Serveurs : Irlande
Motif du traitement : Gestionnaire de projets

d)

Entité juridique : SendGrid, Inc.
Siège social : 1801 California Street, Suite 500, Denver, CO 80202
Activité : Plateforme de communication digitale
Serveurs : États-Unis
Garanties mises en œuvre : DPA avec clauses contractuelles types conformément à l'article 28 du RGPD
Motif du traitement : Plateforme utilisée pour l'envoi des courriers de la plateforme d'Itering.

e)
Entité juridique : Mailgun Technologies, Inc.
Siège social : 600 North Whisman Road Suite 33, Mountain View, CA 94043
Activité : Plateforme de communication digitale
Serveurs : États-Unis
Garanties mises en œuvre : DPA avec clauses contractuelles types conformément à l'article 28 du RGPD
Motif du traitement : Plateforme que nous utilisons pour analyser et capturer les requêtes réalisées en utilisant le domaine MX itering.com et ainsi capturer les courriers.

f)
Entité juridique : Plivo, Inc.
Siége social : 601 S Congress Ave, STE 220,The Littlefield Building, Austin, TX 78701
Activité : Plateforme de communication et de messagerie pour les entreprises (services SMS et mailing, entre autres).
Serveurs : États-Unis
Garanties mises en œuvre : Contrat de gestionnaire de traitement avec les exigences de l'art. 28 du RGPD, réglementant les transferts internationaux de données au moyen de clauses contractuelles types
Motif du traitement : Plateforme que nous utilisons pour envoyer des codes OTP par SMS, nécessaire pour répondre à certaines demandes de signature.

Le SOUS-TRAITANT du traitement a un contrat de sous-traitant de traitement signé avec les présentes entités.

• Signaturit a obtenu la certification ISO27001 et réalise des audits RGPD tous les deux ans

Signaturit a la certification ISO 27001 sur son Information Security Management System (ISMS) et effectue tous les deux ans une analyse d'impact externe sur la protection des données.

• Le prestataire de services a les mesures techniques et organisationnelles appropriées afin que les informations stockées ne soient pas perdues, endommagées ou corrompues.

L'emplacement du centre de données répond aux exigences de protection de la vie privée pour les données personnelles qui y sont hébergées, conformément au RGPD.

Une fois signée, Signaturit collecte toutes les données personnelles et sous le processus de signature électronique avancée, les données biométriques du graph du signataire (vitesse, accélération, pression), les crypte et les stocke sur les serveurs AWS S3, qui re-crypte les données (sous AES 256). Il existe un double cryptage et Signaturit effectue un backup quotidien du Dataset.

D'autre part, AWS se conforme à toutes les exigences du RGPD et nous avons conclu un DPA avec AWS. Concernant le HSM (Hardware Security Module), nous avons deux modules pour pouvoir avoir un système de sauvegarde/backup. Signaturit suit le principe de responsabilité, en suivant, entre autres, le principe de la confidentialité, a nommé un DPD, effectue une analyse d'impact sur la protection des données tous les deux ans, suive les principes de séparation des tâches et de privilège minimum, etc. (Exigences du RGPD).

En ce qui concerne notre système de gestion de la sécurité de l'information, nous suivons une politique de sauvegarde (backup), une politique de contrôle d'accès, une politique de classification des informations, etc. (sous ISO 27001, exigences de sécurité de l'information).

• Mesures de sécurité adoptées par le prestataire de services pour conserver les données, tels que mises à jour, sauvegardes, audits, mesures de prévention d'incendie, etc.

Signaturit dispose d'un plan de continuité des activités et de reprise après sinistre dans lequel tous les scénarios de sinistre sont pris en compte. En ce sens, il dispose d'une politique de sauvegarde et effectue périodiquement des tests de sauvegarde pour la base de données et les services.

Signaturit est certifié selon la norme ISO 27001 et chaque année des audits sont passés. De même, nous devons passer les audits liés à des services de confiance qualifiés qui incluent des fonctionnalités supplémentaires en termes de sécurité. De même, le DPD vérifie / examine les données, processus et flux dans l'entreprise au moins deux fois par an.

• Les données et processus stockés dans les installations du prestataire de services de confiance ne sont pas accessibles ou utilisés par des tiers et les données sont séparées et non accessibles par d'autres clients.

Aucun client peut accéder ou utiliser les informations (données personnelles ou autres) des bases de données Signaturit. Seul le personnel de confiance (membres PKI) conformément à nos Rôles, responsabilités et autorités politiques de l'organisation peut accéder aux informations sensibles.

Une autre question à garder à l'esprit est que toutes les machines Signaturit sont privées et situées dans une VPC et ne sont pas accessibles depuis Internet. Dans le VPC, nous avons toutes les machines et bases de données, et chaque environnement a une VPC différente avec toutes les ressources nécessaires déployées, sans partage

de ressources et de données entre les environnements. L'accès aux machines et aux bases de données est géré par les groupes de sécurité AWS et les tables de routage. Dans ces ressources, nous limitons les ports ouverts, à ceux qui ne sont nécessaires que pour les services et la base de données.

Nous contrôlons également les ressources auxquelles un service peut accéder avec des rôles IAM uniques par service. Nous suivons la règle du principe du least privilege (PoLP), où les services et les utilisateurs n'ont pas d'autorisations privilégiées. Toutes les machines ont le journal d'audit activé et nous envoyons les journaux à Datadog, où nous les analysons et les surveillons, créant des alarmes pour toute action suspecte. Les journaux sont également stockés dans notre compte d'audit sur AWS, où nous centralisons tous les journaux de sécurité et ne peuvent être modifiés par personne.

• Les données stockées par le prestataire de services ne sont pas consultées ou utilisées par le prestataire de services à des fins autres que celles établies dans le contrat.

Signaturit n'accède ni n'utilise les informations (données personnelles) à des fins autres que celles établies dans le DPA. En ce sens, l'entreprise suit des politiques de sécurité telles que la minimisation, l'anonymisation, le least privilege ou la séparation des fonctions, et toutes les données sont automatiquement cryptées. En ce sens, Signaturit effectue des analyses d'impact tous les deux ans et le DPD vérifie / examine les processus et les flux de données dans l'entreprise au moins deux fois par an.

• Sécurité qui s'applique aux transferts de données.

Signaturit a conclu un DPA avec ses sous-traitants conformément aux clauses contractuelles standard de l'UE du RGPD. En dehors de cela, il dispose d'une politique de sécurité des informations, d'une politique de classification des informations et d'une politique de sécurité des fournisseurs et des partenaires.

• Flexibilité ou comment les services évoluent si nos besoins augmentent ou diminuent.

Signaturit utilise AWS S3, qui est un service de stockage simple qui offre une infrastructure pour stocker des données avec un niveau extrêmement élevé de durabilité, de disponibilité et d'évolutivité. De cette manière, il n'y a aucun problème pour adapter le service aux besoins de l'entreprise et de ses clients et à leurs besoins croissants.

• Options de portabilité à la fin du service ou si les conditions changent.

Signaturit signe toujours un DPA avec ses clients et la manière d'exercer les options de portabilité peut être concrètement précisée.

• **Mettre en place des mesures de continuité des activités pour assurer la continuité en cas d'incident ou de catastrophe affectant vos installations.**

Signaturit dispose d'un plan de continuité des activités et de reprise après sinistre et d'un plan de reprise PKI (Business Continuity Plan). En ce sens, nous mettons en œuvre des tests pour évaluer périodiquement la continuité et la résilience de nos services.

• **Contrôle et suivi**

Les contrôles que nous effectuons chez Signaturit pour la supervision et le suivi des systèmes de production commencent par le développement, les revues de code, les tests unitaires, les tests d'intégration dans un environnement QA, l'intégration dans un environnement QA, les tests fonctionnels dans un environnement QA, l'intégration en pré-production, intégration dans la production et suivi du système de production à travers différents systèmes / fournisseurs. Un modèle de redondance est implémenté dans tous les services. En cas de panne du système, nous avons des équipes réalisant des gardes pour sa restauration. Ainsi que la redondance dans toutes les données (backup) qui garantit l'intégrité des données.

• **Emplacement des documents**

Tous les documents et informations de nos clients sont stockés dans nos serveurs situés dans l'UE et ne sont en aucun cas transférés vers d'autres destinations en dehors de celle-ci. Nous avons actuellement des centres de données disponibles en Irlande et en Allemagne.

• **Processus de sauvegarde**

Signaturit a mis en place un système de sauvegarde et de récupération des données afin qu'en cas de perte ou de destruction, celles-ci puissent être reconstruites et remises à leur état original. La plate-forme est responsable des copies de sauvegarde quotidiennes des données via le service AWS S3, ce qui fait que la disponibilité de ces copies dépasse 99,99%.

• **Accès Firewalls**

La plateforme Amazon Web Services permet la configuration de groupes de sécurité pour limiter l'accès à chacun des ports du serveur. Un groupe de sécurité est un ensemble de règles qui autorisent ou refusent l'entrée ou la sortie des ports d'un serveur conformément aux spécifications.

La plateforme de Signaturit est configurée pour que chacun de nos serveurs soit le plus restrictif possible, établissant des groupes de sécurité avec des règles très

spécifiques pour autoriser l'accès public uniquement à ceux qui sont une condition essentielle au bon fonctionnement du système.

• Communications cryptées

Lors de la navigation sur Internet, les adresses des sites Web que nous visitons sont dirigées par l'acronyme HTTP ou HTTPS.

L'acronyme HTTP signifie « Hypertext Transport Protocol ». C'est un système conçu dans le but de définir et de standardiser la synthèse des transactions qui sont effectuées entre les différents ordinateurs qui composent un réseau. Autrement dit, c'est le protocole en charge de l'arrivée des données. La principale caractéristique de ce protocole est qu'il s'agit d'un système orienté vers des opérations de type « requête-réponse ». Cela signifie que dans la structure il doit y avoir un client et un serveur : le client est celui qui fait les requêtes et le serveur qui y répond.

De même, le protocole HTTPS, qui signifie Hypertext Transfer Protocol Secure. Ce protocole pose une question fondamentale dans l'utilisation d'Internet : la sécurité. Le système HTTPS est basé sur une combinaison de deux protocoles différents : HTTPS et SSL / TLS. Ce système est le plus sûr pour accéder au contenu offert par Internet, car toutes les informations que nous saisissons seront cryptées, ce qui garantit qu'elles ne peuvent être vues par personne d'autre que le client et le serveur. De cette manière, la possibilité que de telles informations puissent être utilisées est annulée, car quiconque essaie de les voir ne trouvera que des données qu'il ne pourra pas déchiffrer.

L'utilisation du protocole HTTPS est indispensable pour toute activité impliquant l'utilisation de données personnelles : des opérations via des entités bancaires en ligne, des achats en ligne, des envois de courriers électroniques et dans toute autre activité pour laquelle nous devons saisir des mots de passe, des numéros de carte bancaire ou autres informations personnelles.

Le protocole HTTPS fournit non seulement le cryptage de la connexion, mais peut également garantir que le Web auquel nous nous connectons est vraiment celui qu'il prétend être. Chez Signaturit, toutes les connexions entre les différents serveurs ou clients (serveur - serveur, serveur - client) se font via des connexions HTTPS, qui assurent le chiffrement des données de bout en bout.

• Principe de responsabilité proactive

Le RGPD, dans son article 24, décrit ce principe comme la nécessité pour le responsable du traitement d'appliquer les mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Les mesures adoptées par Signaturit sont, entre autres :

- Nomination d'un délégué à la protection des données (DPD)

- Protection des données par défaut

- Contrats de sous-traitant des données

- Registre des activités de traitement

- Notification d'une violation de la sécurité des données personnelles à l'autorité de protection des données.

- Analyse de risque

• Analyse d'impact relative à la protection des données

Une analyse d'impact relative à la protection des données (AIPD) est un processus qui aide à identifier et à minimiser les risques de protection des données d'un projet. Toute entreprise doit effectuer une AIPD pour un traitement susceptible d'entraîner un risque élevé pour les individus. L'article 35 du RGPD couvre les analyses d'impact relatives à la protection des données. La AIPD est une nouvelle exigence du RGPD, conformément à la loi :

« Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires ».

En ce sens, Signaturit réalise des AIPD toutes les deux années par des tiers experts dans le domaine. De plus, il mène des audits de sécurité et dispose d'une équipe de sécurité dédiée.

• Notifications de failles de sécurité

Les services de sécurité et juridiques relayeront la violation de données dans les 24 heures suivant la détermination de l'exposition.

• DPD

Signaturit dispose d'une équipe dédiée en charge de la protection des données.

Contact :

DPD dpo@signaturit.com

C. Ávila 29 08005 Barcelone

• Politiques de sécurité

En tant qu'une entreprise certifiée sous la norme ISO 27001, nous avons, entre autres, adopté les politiques de sécurité suivantes :

- *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*