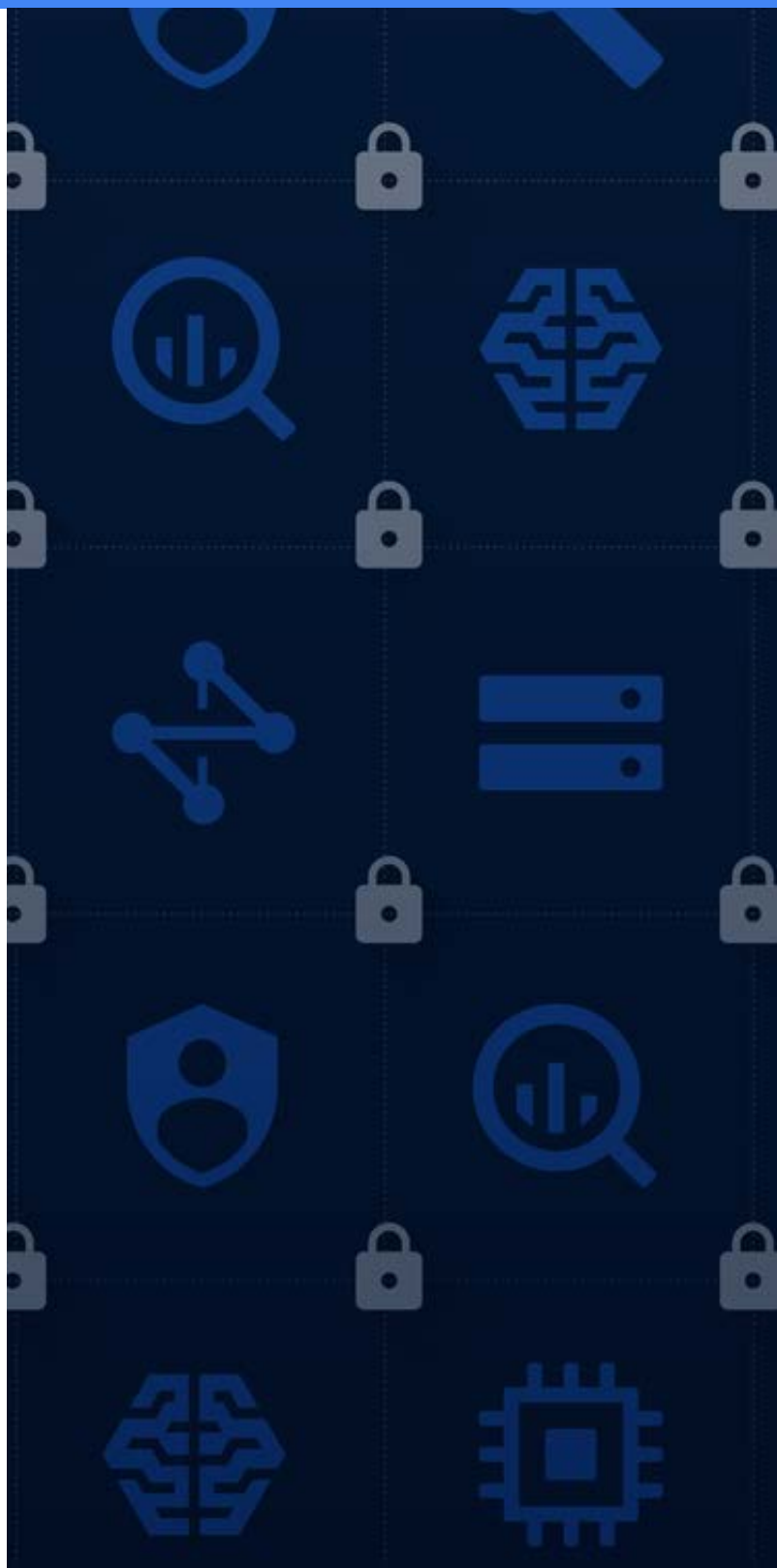
Google Cloud

Règlement Général sur la Protection des Données (RGPD)



INTRODUCTION

Règlement Général sur la Protection des Données (RGPD)

Le 25 mai 2018, la loi européenne relative à la protection des données la plus importante de ces 20 dernières années entrera en vigueur. Le EU General Data Protection Regulation (RGPD) remplace la 1995 EU Data Protection Directive. Le RGPD renforce les droits des individus concernant leurs données personnelles. Il vise à uniformiser les lois sur la protection des données au sein de l'Union européenne, quel que soit le pays où les données sont traitées.

Vous pouvez compter sur notre engagement à respecter le RGPD sur l'ensemble des services G Suite[1] et Google Cloud Platform. Nous avons également à cœur d'aider nos clients à se conformer aux exigences du RGPD en leur offrant une protection efficace en matière de confidentialité et de sécurité que nous avons intégré à nos services et contrats au fil des ans.

[1] G Suite inclut G Suite for Business et G Suite pour l'éducation.

CE QUE VOUS POUVEZ FAIRE

Quelles sont vos responsabilités en tant que client G Suite ou GCP ?

Les clients G Suite et Google Cloud Platform sont généralement responsables du contrôle des données personnelles qu'ils fournissent à Google dans le cadre de leur utilisation des services. Les responsables du contrôle des données définissent les finalités des données personnelles et leurs modes de traitement. Le prestataire de traitement, quant à lui, se charge des opérations au nom du responsable. Google est un prestataire de traitement qui traite les données personnelles au nom des responsables du contrôle des données lorsqu'ils utilisent G Suite ou Google Cloud Platform.

Les responsables du contrôle des données sont chargés de mettre en place des mesures techniques et organisationnelles adéquates pour garantir et prouver que les données sont traitées conformément au RGPD. Leurs obligations touchent aux principes de légalité, d'équité, de transparence, de restriction des finalités, de minimisation et d'exactitude des données ainsi que de respect des droits des personnes concernées à l'égard de leurs données.

Si vous êtes responsable du contrôle des données, vous trouverez des conseils relatifs à vos responsabilités dans le cadre du RGPD en consultant régulièrement la rubrique correspondante[2] du site Web de votre autorité de protection des données nationale ou principale (le cas échéant).

Vous pouvez également lire les publications d'associations agissant dans le domaine de la confidentialité des données, telles que l'**International Association of Privacy Professionals (IAPP).**
Nous vous recommandons également d'obtenir des conseils juridiques concernant votre statut et vos obligations dans le cadre du RGPD, car seul un avocat peut vous fournir des informations spécifiques à votre situation. N'oubliez pas que le contenu de ce site Web n'a pas pour but de fournir des conseils juridiques et ne saurait être considéré comme tel.

Par où commencer?

En tant que client actuel ou futur de Google Cloud, vous pouvez dès maintenant commencer à vous préparer au RGPD. Suivez ces conseils :

- Familiarisez-vous avec les dispositions du **RGDP,** en particulier celles qui diffèrent de vos obligations actuelles en matière de protection des données.
- Créez un inventaire à jour des données personnelles que vous gérez. Vous pouvez utiliser certains de nos outils, tels que **Data Loss Prevention API** pour identifier et classer les données.
- Examinez vos contrôles, règles et procédures actuels pour déterminer s'ils sont conformes au RGPD, puis établissez un plan pour répondre aux exigences du règlement qui ne sont pas satisfaites.
- Réfléchissez à la manière dont vous pouvez tirer parti des fonctionnalités de protection des données actuelles sur Google Cloud pour mettre en place votre charte de régulation. Étudiez les **ressources** d'audit et de certifications indépendants de G Suite ou Google Cloud Platform pour vous y aider.
- Consultez les conseils en matière de régulation lorsqu'ils sont mis à disposition, et faites appel à un avocat pour obtenir des informations juridiques applicables à votre activité.

[2] Nous vous recommandons de faire appel à un conseiller juridique pour connaître votre autorité nationale ou principale de protection des données.

CE QUE NOUS FAISONS

G Suite et Google Cloud Platform : engagements relatifs au RGPD

Entre autres obligations, les responsables du contrôle des données doivent uniquement faire appel à des prestataires de traitement de données en mesure de fournir des garanties suffisantes quant à leur mise en œuvre des mesures techniques et organisationnelles nécessaires au respect du RGPD. Nous vous recommandons de prendre en compte les éléments suivants lors de votre évaluation des services G Suite et Google Cloud Platform.

EXPERTISE, FIABILITÉ ET RESSOURCES

Expertise relative à la protection des données

Google emploie des professionnels de la sécurité et de la confidentialité, dont certains des plus grands experts mondiaux en sécurité des informations, des applications et des réseaux. Leur objectif : gérer les systèmes de défense de l'entreprise, développer des processus d'examen de la sécurité, concevoir l'infrastructure de sécurité, et mettre en œuvre les règles de sécurité de Google.

Google emploie également de nombreux avocats, experts en conformité vis-à-vis des réglementations et spécialistes de politiques publiques qui veillent à garantir la conformité de l'entreprise en matière de confidentialité et de sécurité. Ces équipes interagissent avec les clients, les parties prenantes du secteur et les autorités de contrôle pour concevoir nos services **G Suite** *et* **Google Cloud Platform** *de façon à répondre aux besoins des entreprises en matière de conformité.*

ENGAGEMENTS RELATIFS À LA PROTECTION DES DONNÉES

Accords sur le traitement des données

Nos conditions relatives au traitement des données pour G Suite et Google Cloud Platform définissent clairement nos engagements envers les clients en matière de confidentialité. Nous les faisons régulièrement évoluer en fonction des commentaires de nos clients et des organismes de régulation. Nous les mettrons à jour pour assurer leur conformité avec les modifications induites par le RGPD.

Traitement conforme aux instructions

Toutes les données saisies par un client et ses utilisateurs dans nos systèmes seront traitées conformément aux instructions du client, telles qu'elles sont décrites dans nos accords sur le traitement des données.

Respect de la confidentialité par les employés

Tous les employés Google sont tenus de signer un accord de confidentialité. Ils doivent également suivre des formations relatives à la confidentialité et à la vie privée, ainsi que la formation ***Code de conduite****. Le code de conduite Google traite particulièrement des responsabilités et du comportement attendu des employés en matière de protection des informations.*

UTILISATION DE PRESTATAIRES

Les entreprises du groupe Google effectuent directement la majorité des activités de traitement des données nécessaires pour fournir les services G Suite et Google Cloud Platform. Cependant, nous employons également des fournisseurs tiers pour nous aider à offrir ces services. Chacun d'entre eux est soumis à une procédure de sélection rigoureuse pour veiller à ce qu'il dispose de l'expertise technique requise et soit en mesure de fournir le niveau de sécurité et de confidentialité adéquat. Vous pouvez consulter les informations sur les prestataires du groupe Google gérant les services G Suite et Google Cloud Platform, ainsi que sur les prestataires tiers y participant.

SÉCURITÉ DES SERVICES

Selon le RGPD, le responsable du contrôle des données et le prestataire du traitement doivent mettre en œuvre les mesures techniques et organisationnelles nécessaires pour garantir un niveau de protection adapté au risque encouru. Google gère une infrastructure mondiale conçue pour garantir un niveau de sécurité de pointe pendant l'intégralité du cycle de vie du traitement des informations. Cette infrastructure est conçue pour garantir la sécurité et la confidentialité de nos services à tous niveaux : déploiement, stockage des données avec boucliers de confidentialité de l'utilisateur final, communications entre les services et avec les clients par Internet, opérations effectuées par les administrateurs. Les services G Suite et Google Cloud Platform sont exécutés sur cette infrastructure.

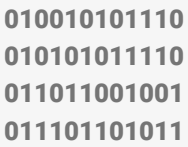
Nous avons conçu la sécurité de notre infrastructure en couches qui se superposent : sécurité physique des centres de données, protections de nos matériels et logiciels, processus utilisés pour soutenir la sécurité opérationnelle. Cette protection en couches crée une sécurité de base solide pour toutes nos activités. Pour en savoir plus sur notre sécurité et son infrastructure, lisez notre livre blanc Google Infrastructure Security Design Overview

Disponibilité, intégrité et résilience

Nous concevons les composants de notre plate-forme de manière à garantir un niveau de redondance élevé. Nos centres de données sont répartis dans différents endroits pour minimiser les conséquences de dysfonctionnements potentiels au niveau régional sur les produits internationaux, pouvant être dus à des catastrophes naturelles ou des pannes locales. Dans le cas d'une panne matérielle, logicielle ou de réseau, les services sont automatiquement et instantanément permutés vers d'autres sites pour que les opérations se poursuivent sans interruption. Notre infrastructure à haute redondance aide les clients à se prémunir contre la perte de données.

Test

Nous menons des tests de reprise après sinistre chaque année afin de créer un cadre commun pour les équipes dédiées aux infrastructures et aux applications. Nous testons ainsi les plans de communication, les scénarios de basculement, la transition opérationnelle et d'autres interventions d'urgence. Toutes les équipes participant à l'exercice de reprise après sinistre développent des plans de test et des revues "post-mortem", qui décrivent les résultats et les enseignements tirés des tests.



Chiffrement

Nous utilisons le chiffrement pour protéger les données lors de leur transfert et de leur stockage. Les données transférées vers G Suite sont protégées par un protocole HTTPS, activé par défaut pour tous les utilisateurs. Les services G Suite et Cloud Platform procèdent automatiquement au chiffrement des données client au repos. Une ou plusieurs méthodes de chiffrement sont utilisées. Pour découvrir des informations détaillées sur le chiffrement des données, **consultez notre livre blanc sur le chiffrement**.

Contrôles d'accès

Les niveaux et droits d'accès accordés aux employés Google dépendent de leur poste et de leur rôle. Les employés ont accès au minimum d'informations et uniquement à celles qui sont indispensables à l'exercice de leur fonction, à la hauteur des responsabilités qui leur ont été confiées. Les demandes d'accès supplémentaires suivent une procédure formelle impliquant un formulaire de demande et d'approbation géré par un propriétaire des données ou du système, un manager ou un autre responsable, tel que l'exigent nos règles de sécurité.

Gestion des failles

Nous recherchons des failles dans le système à l'aide d'un ensemble d'outils disponibles sur le marché et conçus en interne, de tests d'intrusion intensifs automatisés et manuels, de procédures d'assurance qualité, d'examens de la sécurité logicielle et d'audits externes. Nous nous appuyons également sur la plus vaste communauté de recherche en sécurité et apprécions son aide au niveau de l'identification de failles dans G Suite, Google Cloud Platform et les autres produits Google. Notre Vulnerability Reward Program incite les chercheurs à signaler les problèmes de conception et de mise en œuvre pouvant présenter un risque pour les données des clients.

Sécurité du produit : G Suite

Les clients G Suite peuvent utiliser les fonctionnalités et les configurations du produit pour assurer une protection supplémentaire de leurs données personnelles contre le traitement non autorisé ou illégal :

- *La validation en deux étapes réduit de manière significative le risque d'accès non autorisé en demandant aux utilisateurs une autre preuve de leur identité à l'étape de connexion. La mise en œuvre des clés de sécurité offre un niveau de sécurité supplémentaire aux comptes utilisateur en nécessitant la saisie d'une clé physique.*
- *Le suivi des connexions suspectes permet de détecter les activités douteuses à l'aide des grandes capacités du machine learning.*
- *La sécurité renforcée des e-mails signe et chiffre les e-mails à l'aide de la méthode S/MIME (Secure/ Multipurpose Internet Mail Extensions).*
- *La protection contre la perte de données garantit la sécurité de vos informations sensibles au sein de Gmail et de Drive contre le partage non autorisé. Pour en savoir plus, consultez notre livre blanc sur la protection contre la perte de données.*
- *La gestion des droits relatifs à l'information dans Drive vous permet de désactiver le téléchargement, l'impression et la copie de fichiers depuis le menu de partage avancé, et de définir des dates d'expiration pour l'accès aux fichiers.*
- *La gestion des appareils mobiles offre une surveillance continue du système et vous prévient en cas d'activité suspecte enregistrée sur l'appareil.*

Pour en savoir plus, accédez au site.

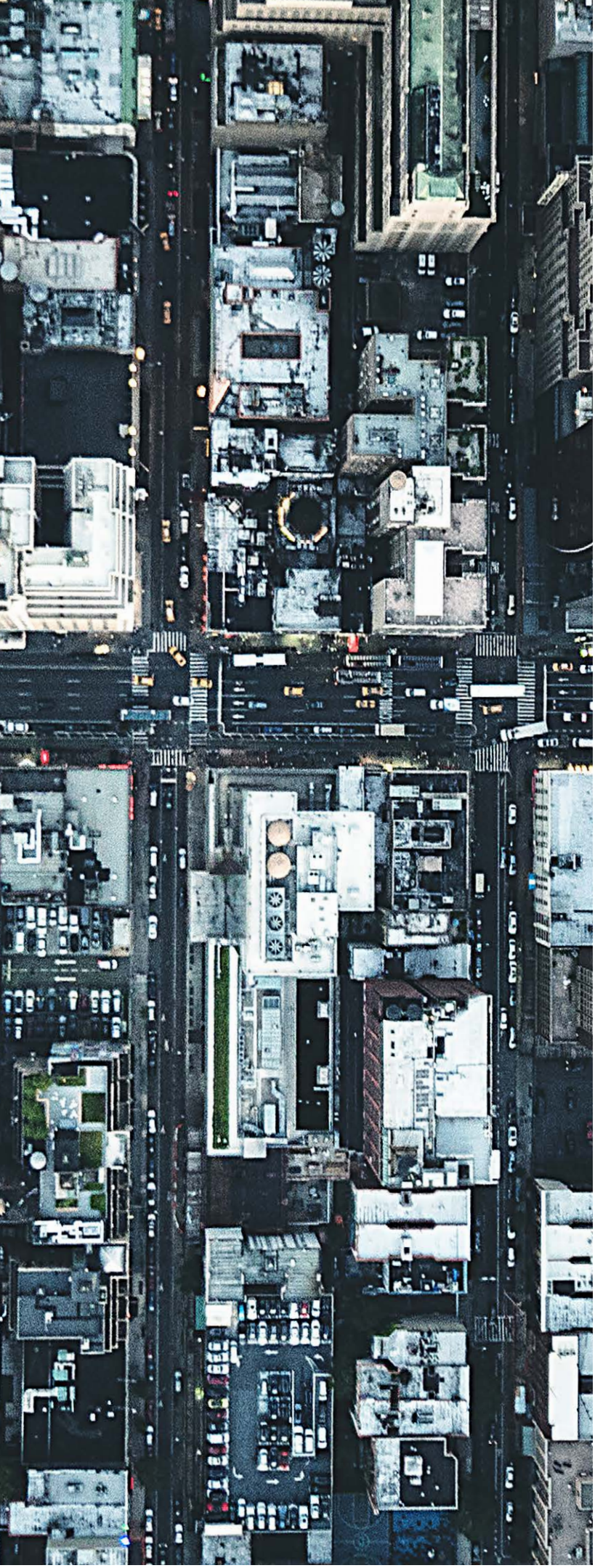
Sécurité produit : GCP

Les clients GCP peuvent utiliser les fonctionnalités et les configurations du produit pour mieux protéger leurs données personnelles contre le traitement non autorisé ou illégal :

- *La validation en deux étapes réduit fortement le risque qu'un tiers accède sans autorisation à des données en demandant aux utilisateurs une preuve supplémentaire de leur identité à l'étape de connexion. La mise en œuvre des clés de sécurité offre un niveau de sécurité supplémentaire aux comptes utilisateur en nécessitant la saisie d'une clé physique.*
- *La gestion de l'authentification et des accès Google Cloud (Cloud IAM) vous permet de créer et de gérer précisément les permissions d'accès et de modification pour les ressources de Google Cloud Platform.*
- *L'API Cloud Data Loss Prevention permet d'identifier et de surveiller le traitement de catégories spéciales de données personnelles afin de mettre en œuvre des contrôles adéquats.*
- *Stackdriver Logging et Stackdriver Monitoring intègrent des systèmes de connexion, de surveillance, d'alerte et de détection d'anomalies à Google Cloud Platform.*
- *Cloud Identity-Aware Proxy (Cloud IAP) contrôle les accès aux applications cloud exécutées sur Google Cloud Platform.*

Cloud Security Scanner recherche et détecte des failles courantes dans les applications Google App Engine.

Pour en savoir plus, accédez au site.



RENVOI ET SUPPRESSION DE DONNÉES

Les administrateurs peuvent exporter les données d'un client à l'aide de la fonctionnalité des ***services G Suite*** *ou Google Cloud Platform à tout moment pendant la durée de validité du contrat. Nous avons intégré des engagements pour l'exportation de données dans nos conditions relatives au traitement des données depuis plusieurs années. De plus, nous améliorons en permanence la stabilité des fonctionnalités d'exportation de données des services G Suite et Google Cloud Platform (consultez la documentation Google Cloud Platform pour en savoir plus).*

Vous pouvez également supprimer les données d'un client à l'aide de la fonctionnalité des services G Suite ou Google Cloud Platform à tout moment. Si vous nous donnez pour instruction de supprimer définitivement des données (comme par exemple, lorsque vous supprimez un e-mail qui ne peut pas être récupéré dans la corbeille), nous supprimons les données du client de tous nos systèmes dans un délai de 180 jours maximum, à moins que nous ne soyons tenus de les conserver.

AIDE POUR LE RESPONSABLE DU CONTRÔLE DES DONNÉES

Droits des personnes concernées

Les responsables du contrôle des données peuvent utiliser les consoles d'administration et les fonctionnalités des services G Suite et Google Cloud Platform pour accéder aux données que leurs utilisateurs et eux-mêmes saisissent dans nos systèmes, les rectifier, limiter leur traitement ou les supprimer. Ces fonctionnalités leur permettent de remplir leurs obligations de répondre aux demandes des personnes concernées cherchant à exercer leurs droits en vertu du RGPD.

Canal de communication relatif à la protection des données

Les clients G Suite et Google Cloud Platform disposent d'un canal de communication où peuvent être dirigées leurs questions relatives à la protection des données.

Notifications d'incident

Dans le cadre de nos services G Suite et Google Cloud Platform, nous proposons des engagements contractuels concernant la notification d'incident depuis de nombreuses années. Nous continuerons à vous informer rapidement des incidents impliquant les données de vos clients, tel que stipulé dans les conditions de notre contrat sur les incidents relatifs aux données.

TRANSFERTS DE DONNÉES INTERNATIONAUX

Le RGPD propose plusieurs mécanismes facilitant les transferts de données personnelles en dehors de l'UE. Ces mécanismes ont pour but d'apporter un niveau de protection adapté ou d'assurer la mise en œuvre de garanties appropriées lorsque des données personnelles sont transférées dans un autre pays.

Les garanties adéquates peuvent être décrites dans des clauses contractuelles types. Le niveau de protection adapté peut être confirmé par des décisions d'adéquation, telles que celles appuyant les boucliers de confidentialité UE-États-Unis.

Nous nous engageons contractuellement à maintenir un mécanisme facilitant les transferts de données personnelles en dehors de l'UE, tel qu'il est requis par la directive de protection des données. Nous offrirons un engagement équivalent conformément au RGPD.

La certification Google s'inscrivant dans le cadre défini par le bouclier de protection des données UE-États-Unis et Suisse-États-Unis comprend ***G Suite et Google Cloud Platform****. Les autorités européennes de protection des données nous ont également confirmé que nos clauses contractuelles types sont conformes. Cela signifie que nos engagements contractuels actuels pour G Suite et Google Cloud Platform sont entièrement conformes à la directive de protection des données, et permettent d'encadrer légalement les transferts de données personnelles de l'UE vers le reste du monde.*

NORMES ET CERTIFICATIONS

Nos clients et régulateurs attendent des vérifications indépendantes afin de contrôler nos dispositifs de sécurité, de confidentialité et de conformité. Pour offrir cette garantie, nous soumettons régulièrement nos services G Suite et Google Cloud Platform à des audits tiers.

ISO 27001 (gestion de la sécurité des informations) ISO 27001 est l'une des normes de sécurité indépendantes les plus courantes et reconnues à travers le monde. Google a obtenu cette certification pour les systèmes, les applications, les personnes, la technologie, les processus et les centres de données qui constituent notre infrastructure commune partagée, ainsi que pour les produits G Suite et Google Cloud Platform.

ISO 27017 (sécurité dans le cloud) ISO 27017 est une norme internationale sur les bonnes pratiques de contrôle de la sécurité des informations. Elle repose sur la norme ISO/IEC 27002 qui est spécifiquement adaptée aux services cloud. Nos services G Suite et Google Cloud Platform ont été certifiés conformes à la norme ISO 27017.

ISO 27018 (confidentialité dans le cloud) ISO 27018 est une norme internationale sur les bonnes pratiques relatives à la protection des informations personnelles dans les services cloud publics. Nos services G Suite et Google Cloud Platform ont été certifiés conformes à la norme ISO 27018.

SSAE16/ISAE 3402 (SOC 2/3) Les audits SOC 2 (Service Organization Controls, Contrôle d'organisation des services) et SOC 3 de l'AICPA (American Institute of Certified Public Accountants) encadrent les "principes et critères de confiance" vis-à-vis de la sécurité, de la disponibilité des services, de l'intégrité du traitement des données et de la confidentialité. Google Cloud Platform et G Suite sont conformes aux normes des audits SOC 2 et SOC 3.

QUESTIONS FRÉQUENTES

" QU'EST-CE QUE LE RGPD ? "

Le Règlement général sur la protection des données est une nouvelle loi européenne sur la confidentialité qui remplace la Directive 95/46/CE sur la protection des données du 24 octobre 1995.

" QUAND LE RGPD ENTRE-T-IL EN VIGUEUR ? "

Le RGPD entrera en application dans l'ensemble des États membres de l'Union européenne le 25 mai 2018.

" LE RGPD IMPOSE-T-IL DE STOCKER LES DONNÉES PERSONNELLES DANS L'UE ? "

Non. Comme la Directive 95/46/CE sur la protection des données, le RGPD définit des conditions concernant le transfert de données personnelles en dehors de l'Union européenne. Elles peuvent être respectées par le biais de mécanismes tels que des clauses contractuelles types.

" LE RGPD ACCORDE-T-IL AUX CLIENTS LE DROIT D'EFFECTUER UN AUDIT DE GOOGLE CLOUD ? "

Conformément au RGPD, des droits d'audit doivent être accordés aux responsables du contrôle de données dans les contrats les liant aux prestataires de traitement de données. Par conséquent, nos conditions relatives au traitement des données incluront ces droits d'audit au bénéfice de nos clients.

" QUEL RÔLE JOUENT LES NORMES ISO 27001, ISO 27017, ISO 27018 ET SOC 2/3 DANS LE CADRE DE LA CONFORMITÉ AVEC LE RGPD ? "

Nos certifications ISO indépendantes et nos rapports d'audit SOC 2/3 peuvent être utilisés par les clients pour évaluer les risques et vérifier que les mesures techniques et organisationnelles nécessaires sont prises.

" QUELLES AUTRES INFORMATIONS SUR LE RGPD POUVONS-NOUS FOURNIR ? "

Consultez le site Web **"Les entreprises et leurs données" de Google.**