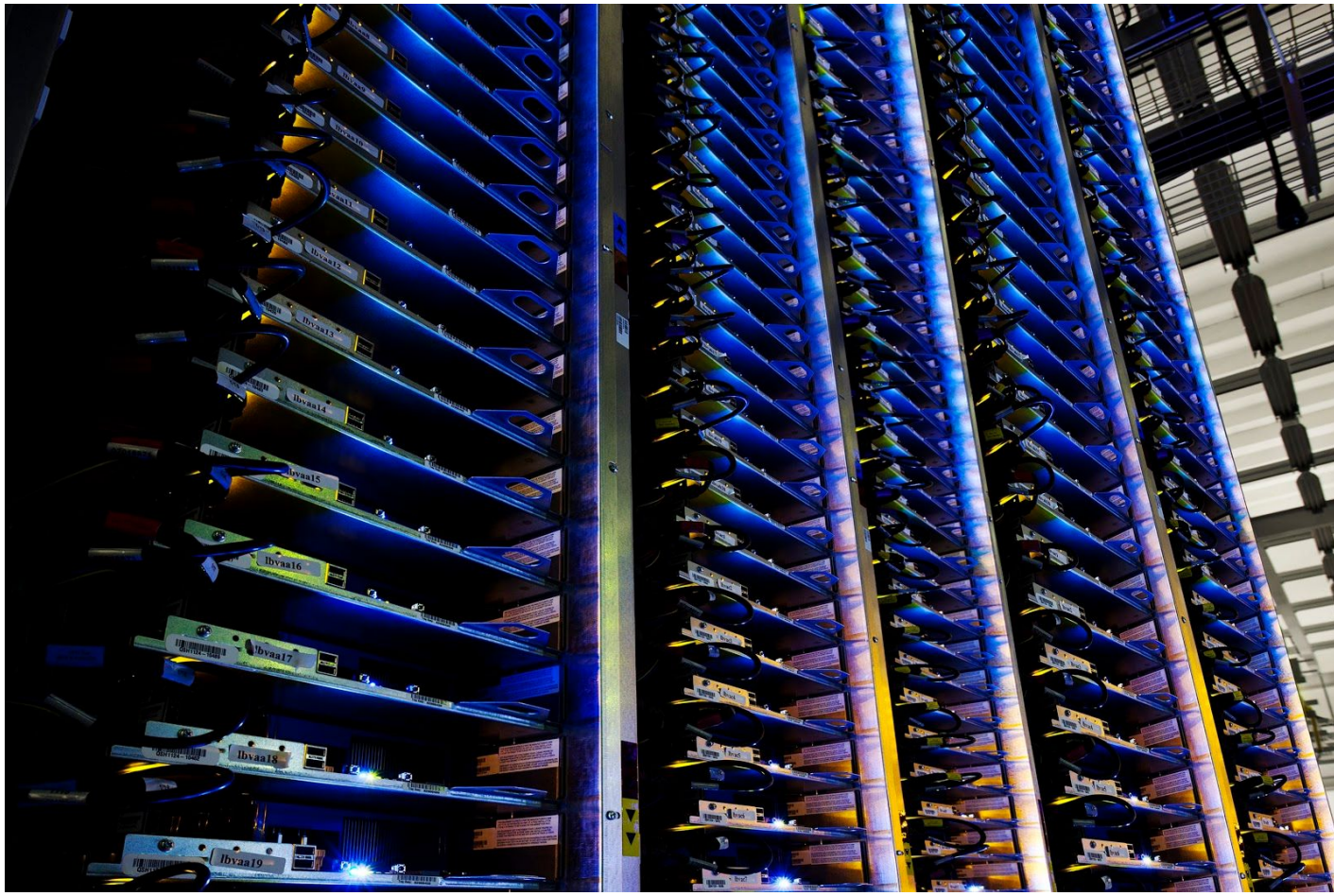
Livre blanc de Google Cloud
Décembre 2020

Google Workspace Guide de mise en œuvre de la protection des données



Google Cloud

Sommaire

Clause de non-responsabilité

Ce guide a pour but d'aider les administrateurs Google Workspace à mieux utiliser et personnaliser les services et les paramètres de Google Workspace afin qu'ils puissent mieux répondre aux règles de protection des données. Ce guide ne constitue en aucun cas une aide juridique. Nous vous recommandons donc de consulter un expert juridique pour obtenir des conseils sur les besoins spécifiques de votre organisation.

Le contenu du présent guide est correct à la date Décembre 2020 et n'a pas été modifié depuis sa rédaction initiale. Les règles et les systèmes de Google peuvent changer par la suite, car nous améliorons continuellement la protection de nos clients.

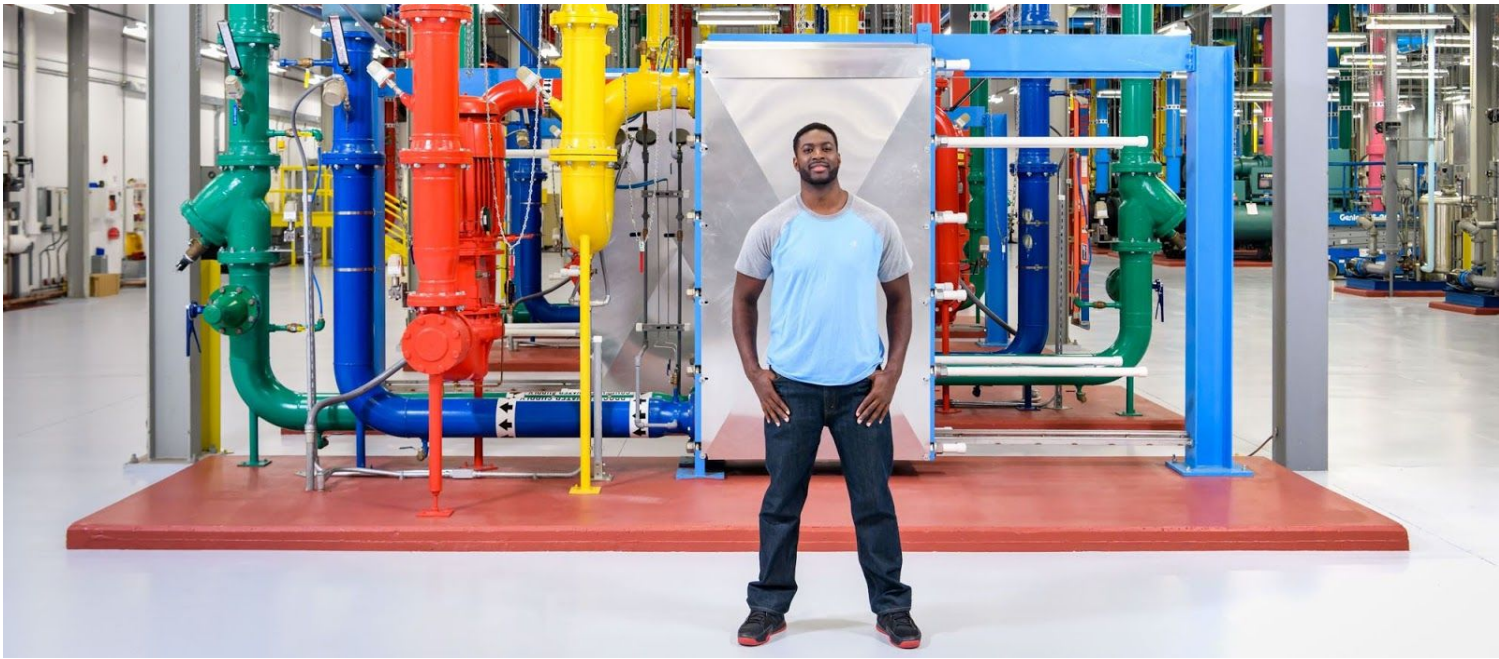
Traitement des données à caractère personnel du Client dans nos services

Comprendre vos obligations en matière de protection des données

Google a à cœur d'aider ses clients à se conformer à toutes leurs obligations en matière de protection des données, ainsi qu'aux exigences du Règlement général sur la protection des données (RGPD). Nous leur proposons donc des produits et des outils pratiques, des certifications et des rapports d'audit, et des services et contrats qui prévoient des mesures efficaces de confidentialité et de sécurité.

Selon l'Avenant relatif au traitement des données de Google Workspace, Google est le sous-traitant des Données à caractère personnel du Client envoyées, stockées ou reçues par votre organisation par le biais des services Google Workspace, et ces données sont traitées en votre nom et selon vos instructions. En tant que client, vous êtes responsable du traitement de vos Données à Caractère Personnel[1], ce qui signifie que vous définissez leurs finalités et leurs modes de traitement.

Nous vous recommandons d'examiner votre contrat Google Workspace, l'Avenant relatif au traitement des données de Google Workspace, ainsi que les conditions applicables aux autres services Google dont disposent vos utilisateurs finaux lorsqu'ils sont connectés aux comptes gérés de leur organisation (par exemple, les autres services que vous avez activés pour votre domaine).



[1] Données client à Caractère Personnel : données à caractère personnel qui font partie des données client.

Nos engagements en matière de confidentialité

Nous formulons ces Engagements Cloud en matière de confidentialité des entreprises pour les produits Google Workspace afin de préciser nos principales responsabilités de protection envers vous lorsque vous utilisez nos solutions d'entreprise. Ces engagements s'appuient sur de solides engagements contractuels mis à votre disposition.

- **Nous vous laissons le contrôle de vos données.** Les Données client[2] sont vos données, pas celles de Google. Nous traitons toujours vos données conformément aux accords que vous avez conclus.
- **Nous n'utilisons jamais vos données pour le ciblage d'annonces.** Nous ne traitons pas vos données client ou de service à des fins publicitaires ni pour améliorer les produits Google Ads.
- **Nous faisons preuve de transparence concernant la collecte et l'utilisation des données.** Nous nous engageons à faire preuve de transparence et à respecter les réglementations comme le RGPD et les bonnes pratiques en matière de confidentialité.
- **Nous ne vendons jamais les données client ou de service.** Nous ne vendons ni les données client, ni les données de service[3] à des tiers.
- **Tous nos produits sont conçus en portant une attention particulière à la sécurité et la confidentialité.** Pour appuyer la vie privée de nos clients, nous devons protéger les données que vous nous confiez. Nous intégrons dans nos produits les technologies de sécurité les plus performantes.

Google a conçu Google Workspace selon des normes de confidentialité et de sécurité très strictes, basées sur les bonnes pratiques du secteur[4]. En plus de solides engagements contractuels concernant la propriété, la sécurité et l'utilisation des données, ainsi que la transparence et la responsabilité, nous mettons à votre disposition les outils nécessaires pour répondre aux exigences liées à la conformité et à la création des rapports (pour plus d'informations, voir l'Annexe 1). Nos Principes de confiance clarifient aussi nos engagements en matière de confidentialité et nos procédures de protection et de gestion de vos données dans le cloud.

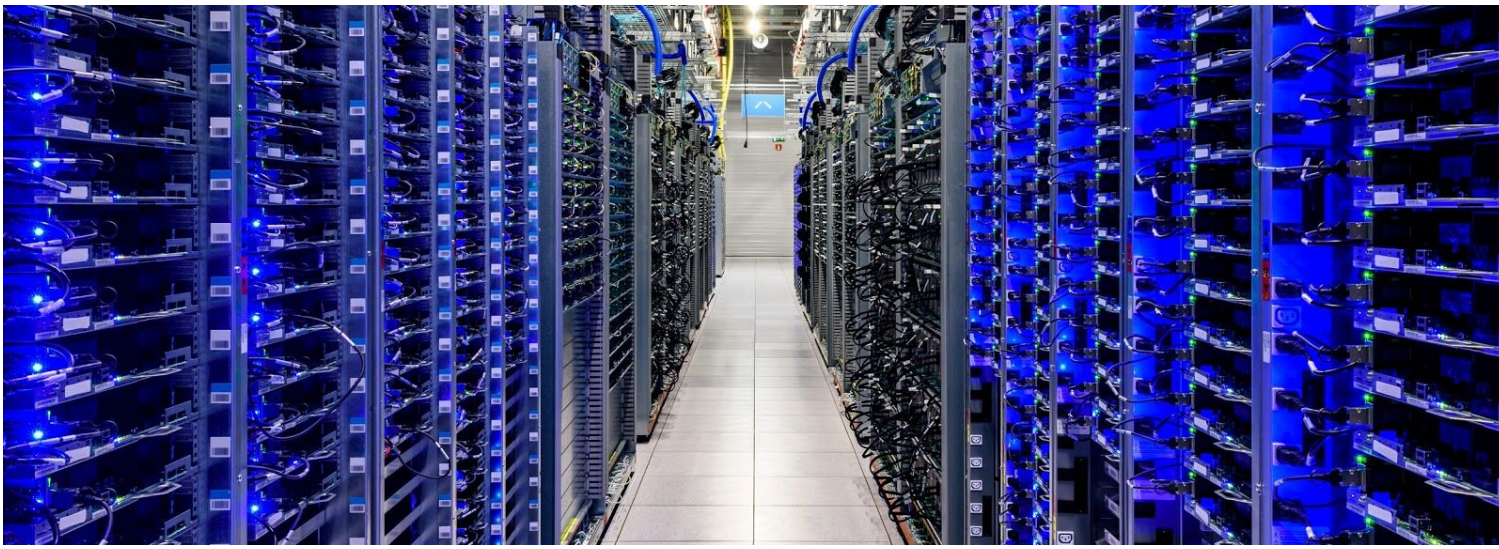
La transparence fait partie de l'ADN de Google. Nous faisons le maximum pour gagner et conserver votre confiance en restant transparents. Chez Google Cloud, nous pensons que la confiance découle de la transparence. Nous voulons que vous sachiez tout de nos engagements et de notre responsabilité

---

[2] Les données client sont les données fournies et créées par vous, votre organisation et vos utilisateurs à Google lorsque vous accédez à Google Workspace et utilisez ces services.
[3] Les données de service correspondent aux informations personnelles que Google collecte ou génère lors du fonctionnement et de l'administration des services Cloud, à l'exception des données client et des données partenaires. Les données de service respectent la Déclaration de confidentialité de Google Cloud.
[4] Reportez-vous à nos certifications ISO/CEI (ISO/CEI 27001, 27017, 27701, 27018) ainsi qu'à notre rapport d'audit SOC 3, disponible en cliquant sur ce lien. Si vous êtes un client existant et que vous souhaitez en savoir plus sur notre sécurité, nous serions ravis de vous présenter un rapport SOC 2 détaillé via le gestionnaire des rapports de conformité. Une liste complète de nos offres de conformité est disponible dans notre Centre de ressources pour la conformité.

partagée concernant la protection et la gestion de vos données dans le cloud. Chez Google Cloud, nous nous efforçons de bâtir un environnement de confiance fondé sur trois piliers : l'assurance de la confidentialité et de la sécurité des données de nos clients, la fiabilité de nos services et l'établissement, ainsi que le respect, des standards les plus élevés en matière de transparence et de sécurité.

Nous sécurisons par ailleurs toutes les données de service. Les données de service correspondent aux informations collectées ou générées par Google lors du fonctionnement et de l'administration de Google Workspace ; elles sont capitales pour assurer la sécurité et la disponibilité de nos services. Les données de service ne comprennent pas les Données client, mais incluent des informations sur les paramètres de sécurité, le fonctionnement, et la facturation. Nous traitons les données de service pour différentes finalités, dont vous trouverez les détails dans l'Avis de confidentialité de Google Cloud publié récemment, par exemple pour suggérer des recommandations visant à optimiser votre utilisation de Google Workspace, et à en améliorer les performances et les fonctionnalités.



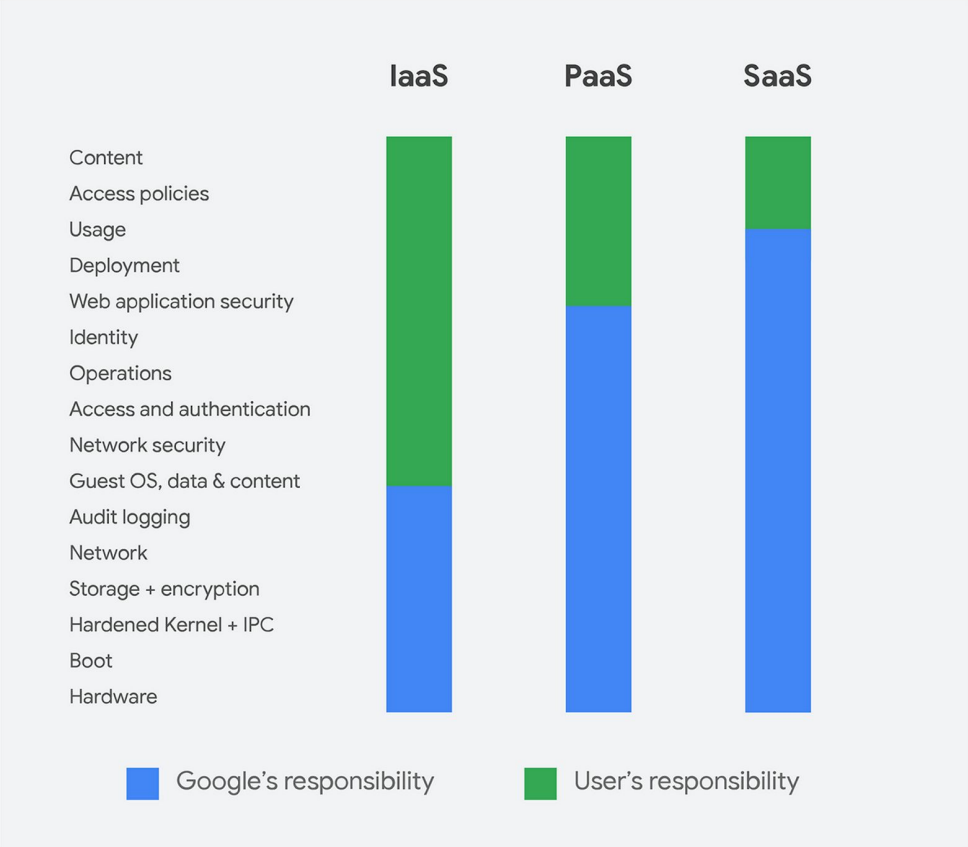
Modèle de responsabilité partagée de Google

La protection des données n'est pas à la seule responsabilité de l'entreprise qui utilise les services Google Workspace, ni de Google qui fournit ces services. La protection des données dans le cloud est au contraire une responsabilité partagée, une collaboration entre le client et le fournisseur de services cloud.

Le modèle de responsabilité partagée de Google offre une représentation visuelle des différentes responsabilités liées à la sécurité qui incombent à la fois au client et à Google. Google Workspace est un logiciel en tant que service (SaaS, Software as a Service) dans lequel le fournisseur de services cloud est responsable de tout, excepté du contenu et des règles d'accès. D'après le modèle SaaS, le fournisseur de services cloud gère les infrastructures physique et virtuelle et la plate-forme tout en fournissant des applications et des services cloud aux clients. Les applications Internet qui sont exécutées directement depuis un navigateur Web ou une application mobile sont des applications SaaS. Grâce à ce modèle, les

clients n'ont pas à se soucier de l'installation, de la mise à jour ou de la compatibilité des applications : ils se chargent simplement de gérer le système et les règles d'accès aux données.

Important : En tant que client Google Workspace, vous êtes tenu de sécuriser le contenu que vous fournissez ou contrôlez (contenu placé dans les services Google Workspace, par exemple), et d'établir un contrôle des accès pour vos utilisateurs.



Vous pouvez consulter le Modèle de responsabilité partagée pour savoir comment sécuriser vos Données client sur Google Workspace. Selon la réglementation sur la protection des données, il vous incombe de protéger les Données client à caractère personnel en votre possession à l'aide de contrôles de sécurité, de surveiller l'accès à ces Données et leur traitement, de vous assurer de leur intégrité et de gérer leur cycle de vie.

Google protège l'infrastructure de Google Workspace tout au long du cycle de vie du traitement des informations. La sécurité est garantie à tous les niveaux : matériel, communications entre les services, gestion des accès interservices, stockage des données, communications Internet et sécurité opérationnelle. Pour plus d'informations à ce sujet, consultez notre Présentation de la sécurité sur l'infrastructure de Google.

Services Google

Dans cette section, nous vous présentons rapidement les divers services Google dont vous allez bénéficier, y compris les services principaux de Google Workspace, les fonctionnalités intégrées, les autres services, les comptes Google gérés par une organisation et le service d'assistance technique.

- **Services principaux de Google Workspace** : services listés et décrits dans le Récapitulatif des services.
- **Fonctionnalités intégrées** : fonctionnalités intégrées dans les services principaux de Google Workspace et qui sont automatiquement disponibles pour tous les utilisateurs Google Workspace.
- **Commentaires/Retours** : les retours sur les suggestions de corrections grammaticales et orthographiques et les commentaires au sein du produit sont régis par les Règles de confidentialité de Google.
- **Autres services** : vendus séparément de l'offre Google Workspace. Généralement, il s'agit de services Google pouvant être utilisés avec un compte Google géré par une organisation. Une liste non exhaustive est disponible sur cette page.
- **Compte Google géré par une organisation** : nécessaire pour profiter d'un compte Google Workspace (différent d'un compte Google personnel) qui est géré par un administrateur.
- **Services d'assistance technique** : les administrateurs Google Workspace peuvent contacter Google pour bénéficier d'une assistance technique par téléphone, e-mail ou chat.

Services principaux de Google Workspace

Les Services principaux de Google Workspace sont listés et décrits dans le Récapitulatif des services des Conditions d'utilisation de Google Workspace (par exemple, Gmail, Docs, Sheets et Slides). Il s'agit des services fournis aux clients Google Workspace en vertu de votre contrat Google Workspace[5].

L'Avenant relatif au traitement des données de Google Workspace, le cas échéant[6], régit la manière dont Google traite les Données client des Services principaux. Les Données client sont les données fournies par les organisations et leurs utilisateurs à Google pour être traitées dans les Services principaux de Google Workspace, y compris les Données à caractère personnel du client (telles que définies dans l'Avenant relatif au traitement des données). Les clients peuvent accepter l'Avenant relatif au traitement des données depuis la console d'administration Google s'ils sont établis en dehors de l'Europe et pensent que l'Avenant répond à leurs besoins en matière de conformité.

[5] G Suite for Education est fourni aux établissements scolaires selon un contrat G Suite for Education distinct et, le cas échéant, selon l'Avenant relatif au traitement des données.
[6] Si le RGPD s'applique au traitement de vos données par Google (par exemple, si vous êtes situé dans l'Union européenne ou si vous êtes établi en dehors de l'UE, mais proposez des biens/services à des personnes résidant dans l'UE), votre contrat avec Google doit contenir des conditions précisant comment les données sont traitées.

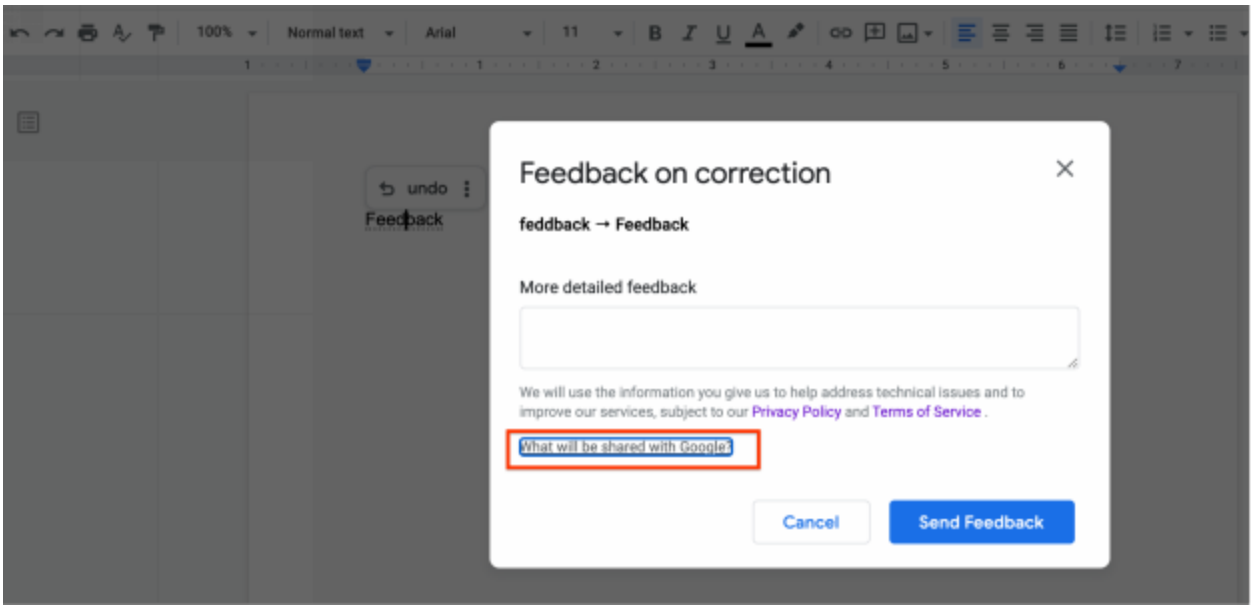
Fonctionnalités intégrées aux Services principaux de Google Workspace

Les Services principaux comprennent plusieurs fonctionnalités telles que le correcteur d'orthographe et de grammaire, Explorer, l'intégration de la géolocalisation d'agenda et Traduction. Ces fonctionnalités sont intégrées aux Services principaux de Google Workspace, et tous les utilisateurs Google Workspace en disposent automatiquement. Google est un sous-traitant des Données à Caractère Personnel utilisées par les fonctionnalités intégrées aux Services principaux de Google Workspace. Ces fonctionnalités sont régies par l'Avenant relatif au traitement des données de Google Workspace lorsqu'elles sont utilisées conjointement aux Services principaux de Google Workspace.

Les utilisateurs peuvent désactiver certaines fonctionnalités intégrées (par exemple, la correction automatique et les suggestions orthographiques et grammaticales dans Google Docs et Gmail) ou choisir de ne pas les utiliser (par exemple, "Traduire le document" et "Explorer"). Notez que si vous avez recours à un site tiers après y avoir accédé par le biais de la fonctionnalité "Explorer", vous n'êtes pas protégé par l'Avenant relatif au traitement des données de Google Workspace.

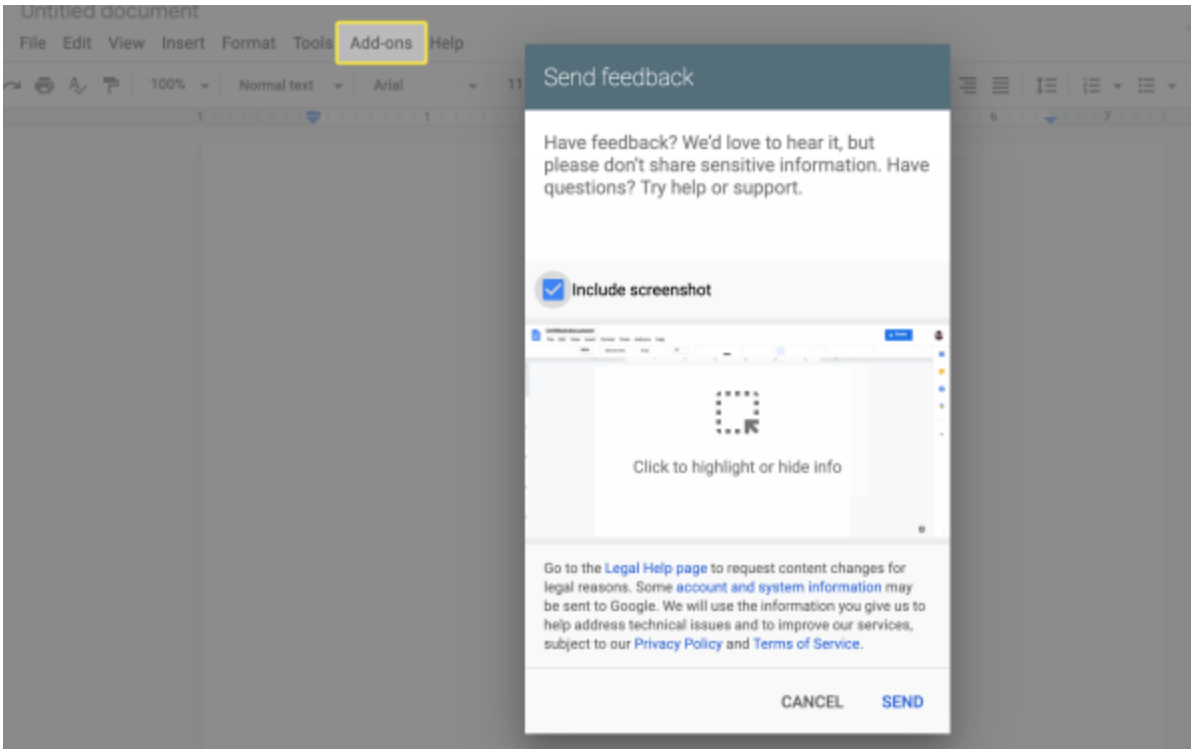
Commentaires/Retours

Les utilisateurs peuvent donner leur avis sur les suggestions orthographiques et les corrections grammaticales (voir l'exemple ci-dessous). Il est important de préciser que les Données client ne sont pas utilisées pour améliorer les services orthographiques et grammaticaux des autres comptes client.



Nous donnons aussi aux utilisateurs la possibilité d'envoyer leurs commentaires dans le produit même. Les utilisateurs peuvent joindre des captures d'écran du problème rencontré, et nous mettons à leur

disposition un outil permettant de masquer les informations sensibles. **Notez que les commentaires transmis par le biais des outils prévus à cet effet seront traités selon les Règles de confidentialité de Google, ce qui est rappelé aux utilisateurs dans chaque champ de saisie de commentaires.** Google agit en tant que “responsable du traitement” des commentaires/retours collectés à partir des corrections grammaticales et orthographiques et au sein des produits.



Autres services

Les Autres services correspondent aux services de Google qui ne sont pas inclus dans l'offre Google Workspace et qui peuvent être utilisés avec un compte Google géré par une organisation. Vous trouverez ici une liste non exhaustive des Autres services. **Ces produits et services n'étant pas inclus dans l'offre Google Workspace, ils ne sont régis ni par l'Avenant relatif au traitement des données de Google Workspace, ni par le contrat Google Workspace**.

Pour une expérience optimale, les utilisateurs de Google Workspace peuvent accéder aux Autres services Google via le Compte Google géré par leur organisation. Comme indiqué sur la page Autres services Google, la plupart des services complémentaires sont régis par les Conditions d'utilisation et les Règles de confidentialité de Google, bien que certains services particuliers soient soumis à des conditions spécifiques. Pour examiner ces modalités, consultez la page Autres services Google et reportez-vous à la section *Services possédant une commande d'activation ou de désactivation individuelle*.

Important : Pour des raisons de conformité, il peut arriver que les administrateurs Google Workspace doivent restreindre l'accès de leurs utilisateurs aux Autres services lorsqu'ils sont connectés à leur compte Google géré par l’organisation.

Les administrateurs peuvent utiliser la console d'administration Google pour *autoriser* ou *empêcher* les utilisateurs connectés à un compte Google géré par leur organisation d'accéder à d'autres services. L'administrateur peut configurer ces paramètres avant de créer des comptes utilisateur. Pour obtenir des instructions, consultez l'article Autres services Google et reportez-vous à la section *Activer ou désactiver des services pour les utilisateurs*. En plus de pouvoir *activer* ou *désactiver* des services Google Workspace et Google depuis la console d'administration, les administrateurs peuvent gérer l'accès aux services Google non répertoriés dépourvus de contrôle individuel (comme Chromecast et Google Surveys). Pour en savoir plus sur l'activation ou la désactivation de ces services, consultez Gérer l'accès aux services qui ne sont pas contrôlés individuellement.

Remarque : Même si un administrateur Google Workspace a désactivé l'accès complet aux Autres services, il est possible que les utilisateurs puissent toujours y accéder et les utiliser sans authentification. Par exemple, si l'administrateur a désactivé YouTube à l'échelle de l'organisation dans la console d'administration, un utilisateur peut toujours y accéder et l'utiliser en étant déconnecté, alors que la connexion à l'application via son compte Google géré par l'organisation échouera. Dans cet exemple, Google ne traitera pas les données liées au compte Google géré de l'utilisateur.

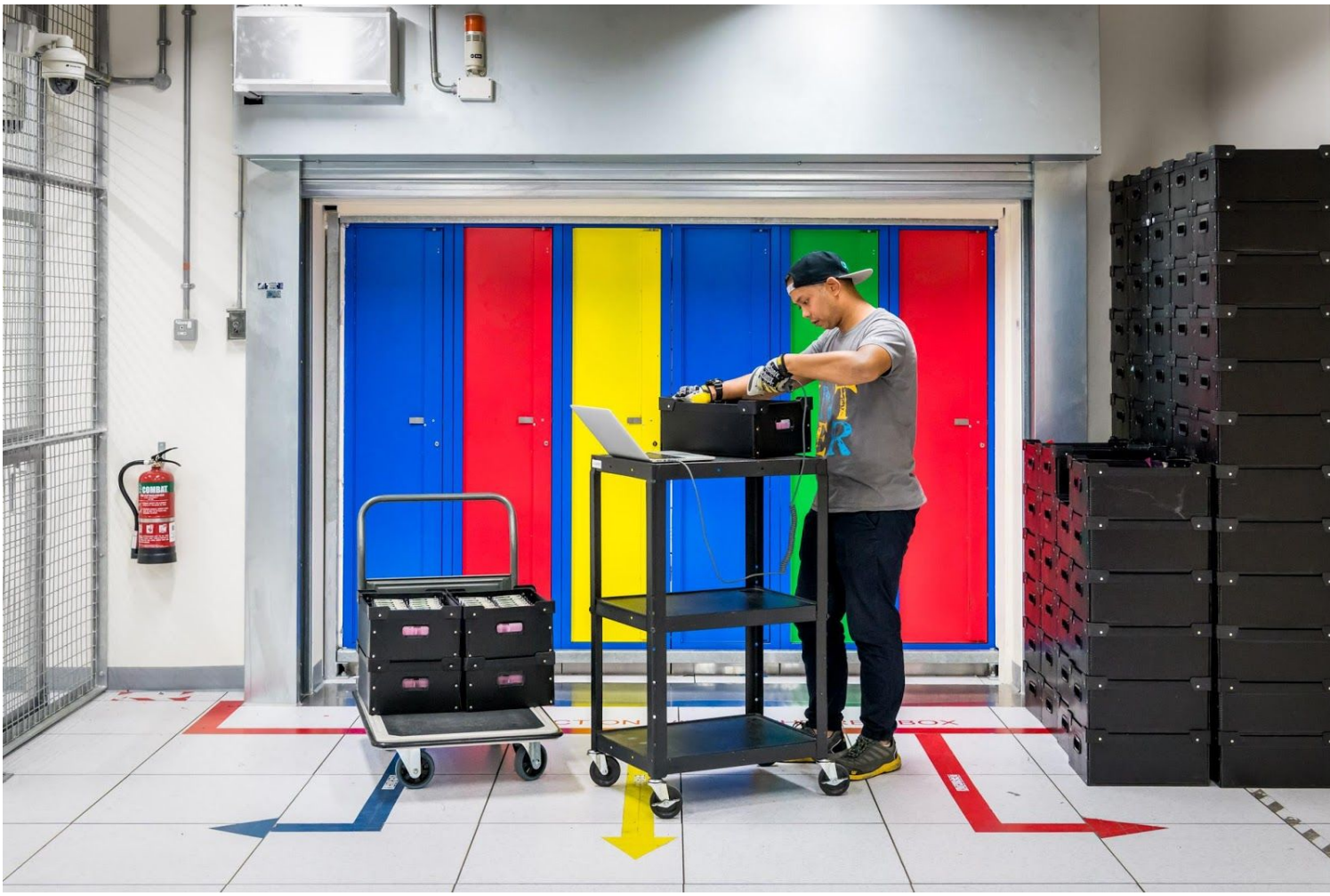
Nous recommandons, le cas échéant, au conseiller juridique ou au délégué à la protection des données (ou équivalent) de votre organisation de réaliser une analyse d'impact concernant le traitement par ces produits des données client à caractère personnel pour déterminer si et comment votre organisation peut remplir ses obligations en tant que responsable du traitement ou sous-traitant des données (selon le cas) pour chacun de ces produits.

Compte Google géré par une organisation

Pour que les utilisateurs de votre organisation puissent profiter de vos services Google Workspace, vous devez configurer un compte pour chacun. Un compte Google géré par une organisation octroie à chaque utilisateur un nom et un mot de passe qui lui permettent de se connecter aux services Google, ainsi qu'une adresse e-mail sur votre domaine et un profil. Les utilisateurs peuvent donner des informations directement, lorsqu'ils fournissent un nom et une photo de profil, ou indirectement, lorsque Google collecte des informations sur le moment, les raisons et le contexte de leur connexion (application/Web, plate-forme et appareil). Quand un utilisateur se connecte à un compte Google que vous venez de créer (géré par votre organisation), il reçoit un avis expliquant comment ses données sont collectées et visualisées par l'administrateur, et précisant que son utilisation des Services principaux de Google Workspace est régie par le contrat Google Workspace de votre organisation. Cet avis mentionne aussi que l'utilisation des Autres services par ce compte Google est régie par les Règles de confidentialité et les Conditions d'utilisation de Google, ainsi que par les Conditions d'utilisation spécifiques des Services applicables. Pour plus d'informations sur la création d'un compte Google géré par une organisation, consultez Options disponibles pour l'ajout de comptes utilisateur.

Services d'assistance technique

Les administrateurs Google Workspace disposent d'une assistance en ligne, téléphonique et par chat. Les données collectées et traitées pour vous fournir des services d'assistance technique lorsque vous utilisez les Services principaux de Google Workspace sont régies par les Instructions relatives aux services d'assistance technique de Google Workspace et la Déclaration de confidentialité de Google Cloud. Google collecte et traite les données dans le but de fournir les services d'assistance décrits dans les Instructions relatives aux services d'assistance technique de Google Workspace et d'assurer leur maintenance. Selon le Contrat Google Workspace (ou les Instructions relatives aux services d'assistance technique de Google Workspace), Google n'est pas tenu de proposer une assistance pour les Autres services.



Bonnes pratiques concernant la confidentialité

Dans cette section, nous avons réuni quelques bonnes pratiques pour vous aider à personnaliser les services Google Workspace afin qu'ils répondent à vos besoins en matière de conformité aux règles de protection des données de votre organisation. Notez qu'il ne s'agit pas d'une liste complète et exhaustive de toutes les pratiques possibles. Nous vous recommandons de consulter un expert juridique ou le délégué à la protection des données de votre organisation pour obtenir des conseils sur les besoins spécifiques de votre organisation, ce guide ne constituant en aucun cas une aide juridique.

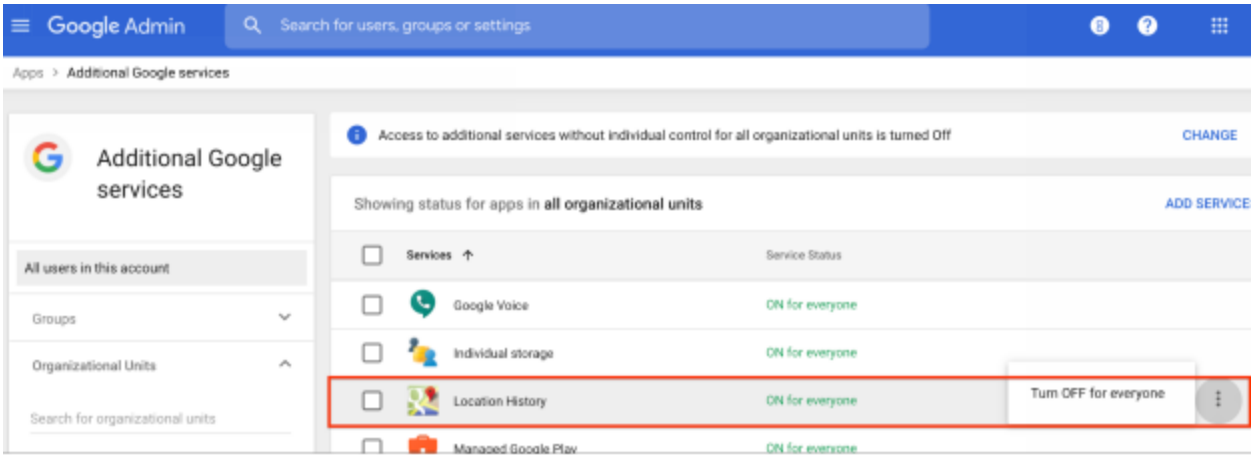
Choisir les Autres services à activer pour vos utilisateurs

Les Autres services ne sont pas inclus dans l'offre Google Workspace, et ne sont couverts ni par l'Avenant relatif au traitement des données de Google Workspace, ni par le contrat Google Workspace. Dans la console d'administration, les Autres services sont activés par défaut. En tant qu'administrateur, vous devez soigneusement choisir les Autres services (par exemple, YouTube, Maps et Blogger) que vous souhaitez activer ou désactiver pour vos utilisateurs, en particulier pour les clients soumis à des limites d'âge ou qui gèrent des données sensibles ou soumises à une réglementation stricte (par exemple, les données financières, médicales et gouvernementales). Pour plus d'informations, consultez la section "Autres services" de ce Guide.

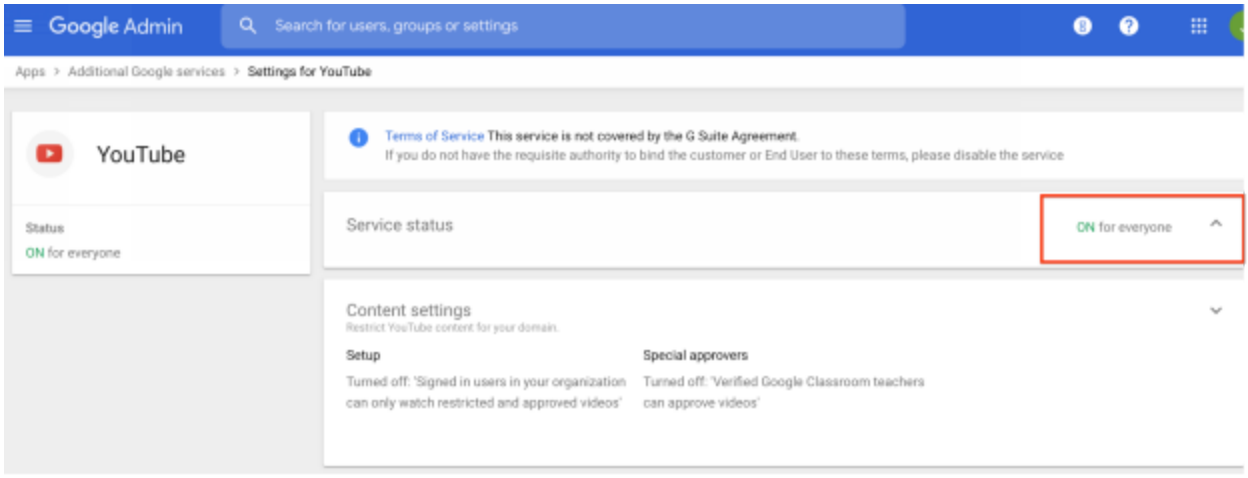
Aider vos utilisateurs à paramétrer les commandes de confidentialité relatives à leur activité

Recommandez à vos utilisateurs d'accepter les commandes relatives à l'activité qui sont conformes aux règles de confidentialité de votre entreprise et qui répondent à leurs besoins personnels. Si vos utilisateurs ne souhaitent pas que Google conserve l'historique de leurs activités et leur offre une expérience personnalisée dans leur compte Google, suggérez-leur de désactiver certains paramètres de la page Commandes relatives à l'activité. Pour plus d'informations, consultez les instructions et les consignes ci-dessous.

- **Historique des positions** : déterminez si vous souhaitez activer ou désactiver l'historique des positions pour le compte Google de vos utilisateurs (géré par votre organisation). Par défaut, l'historique des positions est **désactivé** pour vos utilisateurs. Il ne peut être activé que si vous l'avez activé dans la console d'administration Google **et** que vos utilisateurs l'ont aussi activé. Dans la console d'administration, accédez à *Applications > Autres services Google > Historique des positions*. Demandez à vos utilisateurs d'activer ou de désactiver l'historique des positions en accédant à la page Commandes relatives à l'activité de leur compte Google géré. Pour accéder aux instructions à l'attention des utilisateurs, consultez Gérer l'historique des positions.



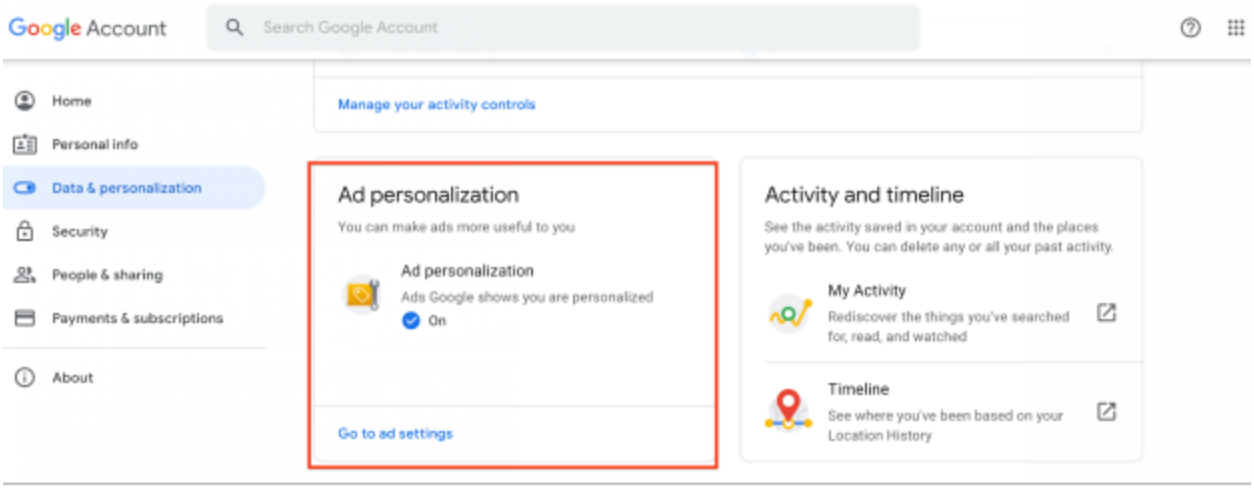
- **Historique YouTube** : déterminez si vous souhaitez activer ou désactiver l'historique YouTube pour vos utilisateurs. Dans la console d'administration, accédez à *Applications > Autres services Google > YouTube*. Si vous activez YouTube dans la console d'administration, chacun de vos utilisateurs peut choisir d'activer ou de désactiver l'**historique YouTube** sur la page Commandes relatives à l'activité. Quand leur historique est désactivé, aucune des vidéos qu'ils regardent n'y apparaît. L'historique n'est pas non plus utilisé pour améliorer les recommandations. Pour accéder aux instructions à l'attention des utilisateurs, consultez Afficher, effacer ou suspendre l'historique des vidéos regardées.



- **Personnalisation des annonces** : les annonces sont personnalisées en fonction des informations que l'utilisateur a ajoutées à son compte Google (géré par votre organisation), des données fournies par les annonceurs partenaires de Google et de nos estimations concernant ses centres d'intérêt. Lorsque la personnalisation des annonces est activée, l'expérience publicitaire est personnalisée pour chaque utilisateur. Vos utilisateurs peuvent toutefois activer ou désactiver ce paramètre depuis la page Commandes relatives à l'activité. Google cesse d'utiliser les informations des utilisateurs qui désactivent ce paramètre pour personnaliser leurs annonces.

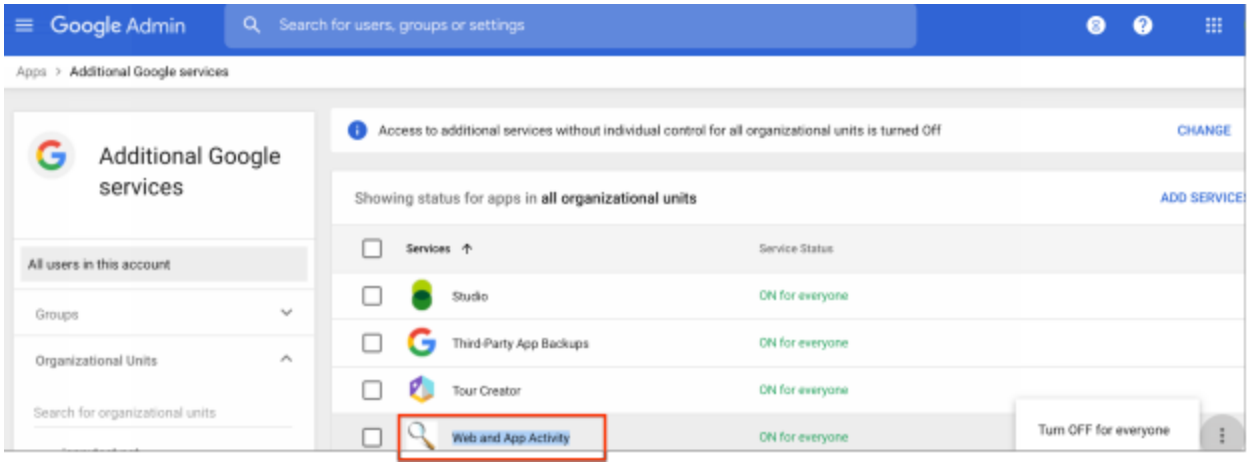
Vous pouvez inviter vos utilisateurs à accéder à la page "Commandes relatives à l'activité" pour activer ou désactiver la personnalisation des annonces.

Remarque : Google Workspace n'utilise pas les Données client à des fins publicitaires. La personnalisation des annonces n'est applicable qu'aux services Google ne faisant pas partie de Google Workspace.



- **Activité sur le Web et dans les applications** : déterminez si vous souhaitez activer ou désactiver le service Activité sur le Web et dans les applications pour vos utilisateurs. Dans le tableau de bord de la console d'administration, accédez à *Applications > Autres services Google > Activité sur le Web et dans les applications*. Par défaut, la commande d'administration Activité sur le Web et dans les applications est activée pour votre organisation, mais le paramètre de personnalisation correspondant est désactivé pour vos utilisateurs finaux. Quand le service Activité sur le Web et dans les applications est **activé** pour l'organisation, les utilisateurs finaux disposent d'une option pour l'activer ou le désactiver. Si l'administrateur **désactive** la commande d'administration Activité sur le Web et dans les applications pour son organisation dans la console d'administration, les utilisateurs finaux ne peuvent pas l'activer par eux-mêmes.

  Si les utilisateurs activent l'option "Activité sur le Web et dans les applications", leurs recherches et leur activité sur un certain nombre d'autres services Google sont enregistrées dans leur compte Google (géré par votre organisation), ce qui leur permet de profiter d'une expérience plus personnalisée. Les utilisateurs peuvent consulter et supprimer leur activité sur le Web et dans les applications depuis la page Commandes relatives à l'activité. Pour accéder aux instructions à l'attention des utilisateurs, consultez Afficher et contrôler l'activité sur le Web et dans les applications.



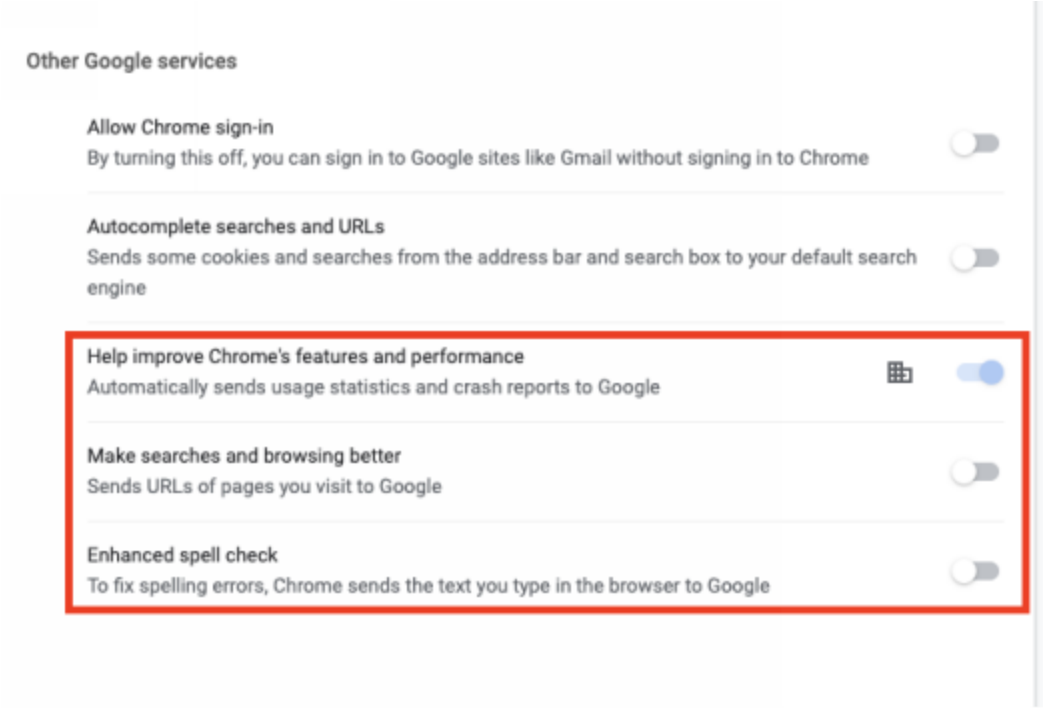
Définir les utilisateurs autorisés à utiliser la synchronisation Chrome et autres paramètres Chrome conseillés

La fonctionnalité de synchronisation Chrome enregistre les favoris, l'historique, les mots de passe et d'autres paramètres de vos utilisateurs de manière sécurisée dans leur compte Google (géré par votre organisation) et leur permet d'y accéder depuis Chrome sur n'importe quel appareil. En tant qu'administrateur, vous pouvez définir quels utilisateurs sont autorisés à utiliser la synchronisation Chrome sur leur compte géré en activant ou désactivant le service pour les utilisateurs concernés. Dans la console d'administration, accédez à *Autres services Google > Synchronisation Google Chrome*. Quand la synchronisation Chrome est activée, les utilisateurs peuvent consulter et mettre à jour les informations synchronisées sur n'importe quel appareil (favoris, historique, mots de passe et d'autres paramètres).

De plus, vos utilisateurs peuvent choisir les fonctionnalités Google qu'ils utilisent dans Chrome, telles que :

- **Contribuer à l'amélioration des fonctionnalités et des performances de Chrome** : l'envoi de rapports d'erreur et de statistiques d'utilisation à Google est activé par défaut, mais l'utilisateur peut désactiver cette option dans les paramètres de Chrome. Les statistiques d'utilisation contiennent des informations telles que les préférences, les clics sur les boutons, les statistiques de performances et l'utilisation de la mémoire. En général, les statistiques d'utilisation de Chrome ne comprennent pas les URL des pages Web ni les données à caractère personnel. Toutefois, si l'utilisateur a activé l'option *Améliorer les recherches et la navigation* dans les paramètres de Chrome, alors les statistiques incluront des informations sur les pages Web visitées par l'utilisateur et sur l'usage qu'il en fait. Si la synchronisation Chrome est activée, Chrome peut aussi combiner les informations sur l'âge et le sexe fournies dans le compte Google de l'utilisateur (géré par votre organisation) avec nos statistiques pour nous aider à développer des produits plus performants pour tous les publics. Ces informations ne permettent pas d'identifier personnellement l'utilisateur et sont utilisées sous forme agrégée uniquement. Les rapports

d'erreur contiennent des informations sur l'état du système collectées au moment du plantage et peuvent contenir des URL de pages Web ou des informations personnelles, en fonction des activités en cours lorsque le rapport d'erreur a été généré. Conseillez à vos utilisateurs d'activer ou de désactiver ce paramètre en fonction de leurs besoins personnels et des règles de votre entreprise (pour accéder aux instructions à l'attention des utilisateurs, consultez Autoriser ou suspendre l'envoi automatique de rapports d'erreur et de plantage).



- **Correcteur orthographique amélioré** : le correcteur orthographique de base utilise un dictionnaire local. Le correcteur orthographique amélioré, quant à lui, est basé sur le cloud et envoie le texte saisi par vos utilisateurs à Google. Par défaut, le correcteur orthographique de base est activé pour vos utilisateurs. S'ils souhaitent activer le correcteur orthographique amélioré, ils doivent accéder au menu Chrome et cliquer sur *Paramètres > Paramètres avancés > Langues*. Lorsque le correcteur orthographique amélioré est activé, Chrome envoie à Google l'intégralité du contenu des zones de texte durant la saisie, ainsi que la langue par défaut du navigateur. Notez que le correcteur orthographique amélioré ne fait pas partie des Services principaux de Google Workspace. Il n'est donc pas régi par le contrat Google Workspace ni par l'Avenant relatif au traitement des données. Les données envoyées à Google par le correcteur orthographique amélioré sont traitées selon les Règles de confidentialité et les Conditions d'utilisation de Google ainsi que les Conditions d'utilisation supplémentaires de Google Chrome et de Chrome OS.

Si votre organisation nécessite un contrôle administrateur plus strict sur les paramètres Chrome et que vous avez besoin de contrôler les données partagées avec Google et les tiers par le biais de Chrome, nous vous recommandons notre solution Chrome Enterprise. Chrome Enterprise permet aux administrateurs de définir des règles de confidentialité pour leur organisation. Par exemple, ils peuvent désactiver la règle Rapports sur les statistiques pour empêcher que des rapports anonymes d'utilisation

et que les statistiques d'erreur pour l'ensemble des utilisateurs de l'organisation ne soient envoyés à Google. Ils peuvent aussi activer ou désactiver les services de correction orthographique améliorée à l'échelle de l'organisation. Pour plus d'informations, consultez Gestion cloud du navigateur Chrome et le Guide de configuration de la sécurité du navigateur Chrome en entreprise.

Appliquer des règles d'accès différentes au sein du domaine

En tant qu'administrateur, vous pouvez créer des unités organisationnelles pour gérer les accès des utilisateurs à différents ensembles de services Google Workspace et de produits complémentaires. Vous pouvez ainsi constituer des groupes séparés pour les utilisateurs qui gèrent des données personnelles ou sensibles. Une fois ces unités organisationnelles créées, vous pouvez activer ou désactiver des services et des produits spécifiques pour chaque groupe d'utilisateurs.

Par exemple, si le département des ressources humaines (RH) doit traiter des données personnelles ou sensibles, il est possible que seuls quelques employés des RH aient réellement besoin d'accéder à ces données. Dans ce cas, vous pouvez configurer une unité organisationnelle RH spécifique pour les utilisateurs travaillant avec des données personnelles ou sensibles dans les Services principaux de Google Workspace, et désactiver certains services ou appliquer des paramètres selon vos besoins.

Recommander aux utilisateurs de garder leurs comptes Google professionnel et personnel séparés

Il est recommandé aux utilisateurs de garder leurs comptes Google professionnel et personnel séparés. En tant qu'administrateur, vous devriez suggérer à vos utilisateurs de ne pas se connecter simultanément à plusieurs comptes Google dans un même navigateur Chrome. Cela permet de diminuer le risque d'erreur humaine conduisant au stockage accidentel de Données client dans le compte personnel d'un utilisateur, ou à l'application des paramètres de confidentialité d'un compte Google personnel à un compte Google géré par l'organisation.

Si votre organisation requiert un contrôle plus strict, vous pouvez empêcher les utilisateurs de se connecter aux services Google avec des comptes autres que ceux que vous leur fournissez. Par exemple, vous pouvez les empêcher d'accéder à leurs comptes Gmail personnels ou à des comptes Google gérés par une organisation appartenant à un autre domaine. Pour obtenir des instructions, consultez Bloquer l'accès aux comptes personnels grand public[7].

En tant qu'administrateur, vous pouvez également gérer les applications professionnelles et les données d'un appareil Android de manière sécurisée, tout en laissant à l'utilisateur le contrôle de ses applications et de ses données personnelles. Vous pouvez configurer un profil professionnel[8] sur un appareil Android

[7] Vous devez inscrire à la gestion cloud du navigateur Chrome les navigateurs pour lesquels vous voulez définir des règles de groupe.
[8] La configuration d'un profil professionnel requiert la gestion avancée des appareils mobiles. Découvrez comment Configurer la gestion avancée des appareils mobiles.

afin de séparer les données et applications professionnelles des données et applications personnelles. Découvrez comment configurer un profil professionnel et ajouter des applications professionnelles à la liste blanche pour les appareils Android.

Passer en revue les recommandations sur l'état de la sécurité

Pour renforcer la sécurité des données de votre organisation, passez en revue les recommandations disponibles sur la page "État de sécurité" dans la console d'administration. Vous pouvez aussi vous reporter à la Checklist de sécurité pour les moyennes et grandes entreprises dans le centre d'aide pour les administrateurs de Google Workspace.

Les administrateurs disposent par ailleurs de nombreux outils de sécurité performants, et peuvent personnaliser leurs propres paramètres de sécurité pour répondre aux besoins de l'entreprise. Par exemple, le centre d'alerte de Google Workspace fournit des alertes et des insights de sécurité exploitables concernant votre domaine, afin de protéger votre organisation des dernières menaces, comme l'hameçonnage et les activités suspectes d'un appareil. L'outil d'investigation de sécurité vous permet d'identifier et de trier les problèmes de confidentialité et de sécurité survenant sur votre domaine, et de prendre les mesures adéquates. Les administrateurs peuvent également automatiser les actions de l'outil d'investigation en créant des règles d'activité afin de détecter et de résoudre les problèmes plus rapidement et efficacement. De plus, Google Vault vous permet d'archiver, de conserver, de rechercher et d'exporter les données pour répondre aux besoins de conservation des données et d'e-discovery de votre organisation. Ces outils de sécurité et bien d'autres sont disponibles et décrits sur la page Sécurité de Google Workspace.

Examiner l'utilisation d'applications tierces au sein de votre organisation

Certains Services principaux de Google Workspace peuvent permettre à un utilisateur de partager des Données client à Caractère Personnel avec un tiers (ou une application tierce), selon les paramètres de votre domaine. De ce fait, il incombe aux clients de mettre en place des mesures appropriées et conformes pour ces tiers (ou applications tierces) préalablement au partage ou à la transmission de Données à Caractère Personnel. Votre organisation est tenue de déterminer s'il est nécessaire ou non de mettre en œuvre d'autres conditions de protection des données avant de partager des données personnelles ou sensibles avec un tiers lors de l'utilisation des services Google Workspace ou d'applications intégrées.

En tant qu'administrateur, vous disposez de trois options pour gérer Google Workspace Marketplace. Vous pouvez interdire l'installation de toutes les applications, autoriser uniquement les applications sur liste blanche ou tout autoriser. Par défaut, les utilisateurs de Google Workspace peuvent installer n'importe quelle application disponible sur Google Workspace Marketplace. Nous vous recommandons de vérifier les règles de l'entreprise et de n'ajouter à la liste blanche que les seules applications tierces qui peuvent accéder aux champs d'application d'API dans les services Google Workspace.

Grâce au contrôle d'accès des applications, vous pouvez déterminer quelles applications tierces et quelles applications appartenant à votre domaine peuvent accéder aux données sensibles de Google Workspace. Utilisez le contrôle d'accès des applications pour :

- limiter ou non l'accès à la plupart des services Google Workspace ;
- autoriser des applications spécifiques à accéder aux services Google Workspace restreints ;
- approuver toutes les applications appartenant au domaine.

L'accès aux Données client est activé par défaut pour les applications Marketplace installées. Nous vous recommandons de vérifier les règles de l'entreprise et de limiter ou de restreindre l'accès aux Données client de Google Workspace si nécessaire.

Surveiller l'activité du compte

Grâce aux rapports et aux journaux d'audit de la console d'administration, vous pouvez facilement examiner les risques de sécurité potentiels, analyser le niveau de collaboration des utilisateurs, savoir qui se connecte et quand, passer en revue l'activité des administrateurs, et bien plus encore. Pour contrôler les journaux, les administrateurs peuvent configurer des notifications pour recevoir des alertes lorsque Google détecte certaines activités, comme les tentatives de connexion suspectes, la suspension de comptes utilisateur par un administrateur, l'ajout et la suppression de comptes utilisateur, la réactivation de comptes utilisateur suspendus, les changements de mot de passe effectués par un administrateur, l'attribution d'un droit d'administrateur à un utilisateur et la révocation de ce même droit. Les administrateurs peuvent également choisir de consulter les rapports et les journaux d'audit à intervalles réguliers pour déterminer les risques potentiels de sécurité. Ils ont ainsi accès à des informations de sécurité clés : des tendances dans les rapports Sélection, le niveau d'exposition global aux violations des données dans les rapports de sécurité, les fichiers créés dans les rapports sur les applications, l'activité des comptes dans les rapports sur les comptes, et les journaux d'audit.

Si les journaux d'audit de la console d'administration donnent des informations sur les actions effectuées par les membres de votre organisation, Access Transparency[9] fournit des journaux sur les actions effectuées par les équipes Google. Les journaux Access Transparency comprennent des informations concernant les ressources consultées et les actions effectuées, ainsi que l'heure et le motif de l'action (par exemple, le numéro de dossier associé à une demande auprès du service client).

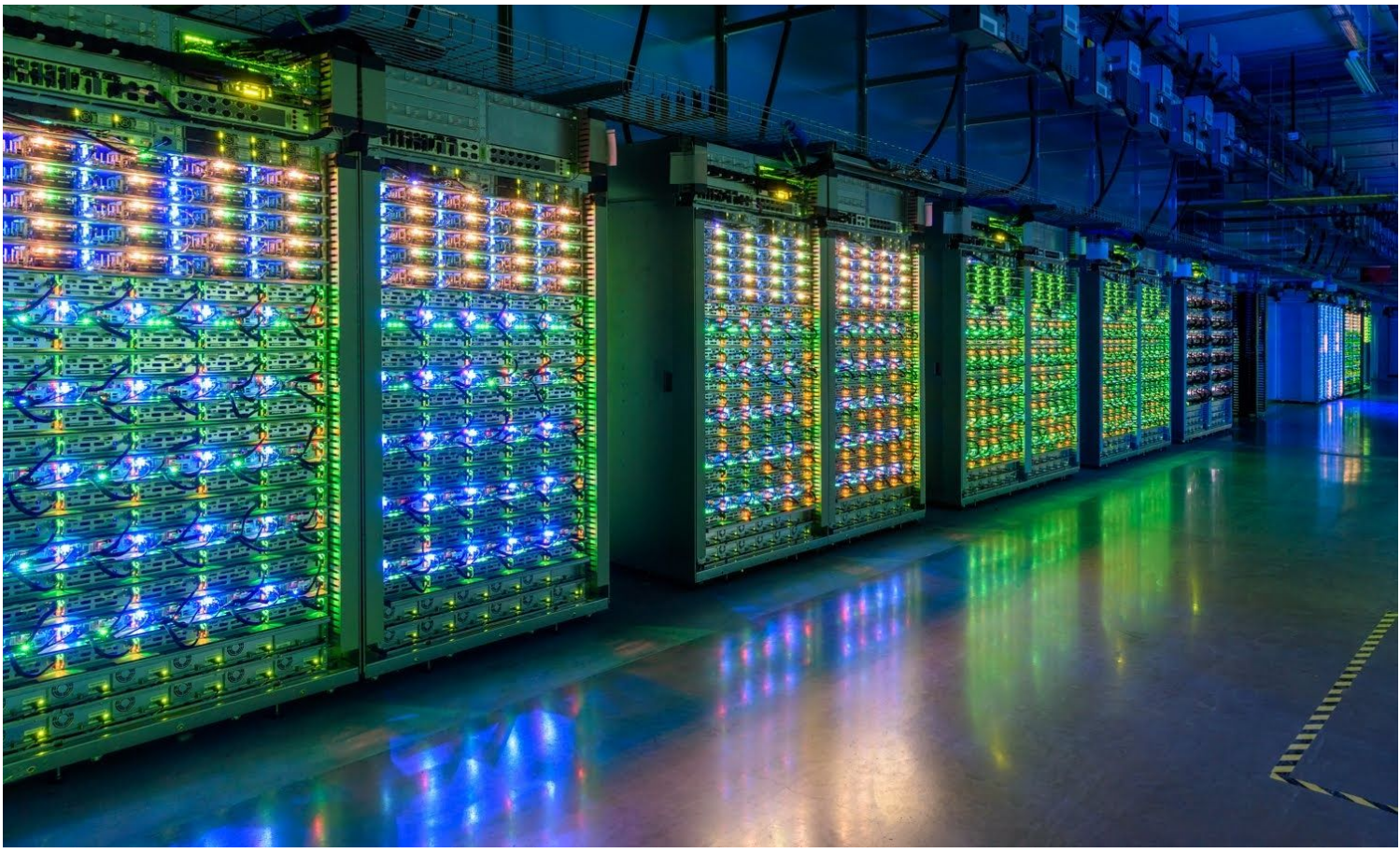
Définir des règles de confidentialité pour les noms et chemins d'accès des fichiers

Pour limiter le partage de Données client à Caractère Personnel, nous vous recommandons, comme mesure de sécurité supplémentaire, de définir des règles visant à empêcher les utilisateurs de fournir

[9] Cette fonctionnalité est disponible uniquement avec Google Workspace Enterprise Plus et G Suite Enterprise for Education.

des informations personnelles sensibles lorsqu'ils nomment des salons Google Chat, des invitations Meet, ou des fichiers dans les Services principaux de Google Workspace (par exemple, Docs, Sheets, Slides, Forms, Drive et Gmail). Voici quelques exemples de Données client sensibles ou à caractère personnel : nom de famille complet, adresse e-mail, adresse postale, numéro de téléphone ou identifiants de compte uniques (par exemple, l'identifiant d'un client, d'un projet ou le nom d'un écran).

Vous pouvez également profiter des fonctionnalités de protection contre la perte de données (DLP) de Google Workspace pour inspecter, classer et anonymiser les données sensibles et ainsi réduire leur exposition. Consultez les pages Empêcher la perte de données grâce au système de protection contre la perte de données pour Drive et Analyser le trafic de messagerie avec la protection contre la perte de données. Pour faciliter la configuration, nous fournissons une bibliothèque de détecteurs de contenu prédéfinis. Une fois la stratégie DLP en place, Gmail peut, par exemple, analyser tous les messages sortants afin de détecter des informations sensibles et de prendre automatiquement les mesures nécessaires pour empêcher la fuite de données : mettre en quarantaine l'e-mail pour l'examiner, inviter les utilisateurs à modifier les informations concernées ou bloquer l'envoi de l'e-mail avec notification à l'expéditeur. Grâce à des règles faciles à configurer et à la reconnaissance optique des caractères contenus dans les images, la protection contre la perte de données dans Drive facilite l'audit des fichiers contenant des informations sensibles. Elle permet également aux administrateurs de configurer des règles visant à avertir les utilisateurs et à les empêcher de partager des informations confidentielles avec des personnes extérieures à l'organisation. Pour en savoir plus, consultez notre livre blanc sur la protection contre la perte de données.



Autres ressources

Pour vous aider à respecter les exigences de conformité et de reporting, nous partageons avec vous des instructions et de bonnes pratiques sur la confidentialité, et vous donnons accès à la documentation dont vous avez besoin. Nous soumettons régulièrement nos produits à des contrôles indépendants de sécurité, de confidentialité et de conformité afin d'obtenir des certifications répondant aux normes internationales appropriées. Pour obtenir la liste des normes, réglementations et certifications de Google Workspace, consultez le Centre de ressources pour la conformité.

Pour consulter facilement et à la demande ces ressources essentielles de conformité, accédez à notre Gestionnaire des rapports de conformité, sans frais supplémentaires. Ces ressources comprennent nos derniers certificats ISO/CEI, rapports SOC et auto-évaluations. Pour sélectionner des ressources, vous devrez peut-être vous connecter à votre Google Cloud Platform ou à votre compte Google Workspace.

Pour savoir comment les services de Google Workspace protègent la confidentialité, l'intégrité et la disponibilité des données, ainsi que la vie privée des utilisateurs, consultez les ressources suivantes :

- **Confidentialité sur Google Cloud** – Inclut une liste des "principes de confiance" de Google Cloud
- **Page Sécuritédans Google Workspace** – Page de référence sur la sécurité dans Google Cloud, qui regroupe des liens vers des livres blancs sur la sécurité et d'autres ressources sur la confidentialité, la transparence, l'infrastructure et les produits de sécurité
- **Centre d'aide pour les administrateurs de Google Workspace** – Page d'accueil regroupant des instructions et la documentation technique sur les produits et les fonctionnalités de sécurité Google Workspace
- **Centre de ressources pour le RGPD** – Inclut toutes les informations nécessaires pour assurer votre conformité au RGPD
- **Centre de sécurité** – Inclut des livres blancs, des vidéos, des articles, des articles de blog et de la documentation sur la confidentialité et la sécurité

Annexe 1 : Synthèse des paramètres de confidentialité

Cette synthèse des paramètres de confidentialité vous permet de déterminer facilement ce dont vous avez besoin pour répondre aux différentes réglementations sur la confidentialité applicables à l'utilisation de Google Workspace. Notez qu'il ne s'agit pas d'une liste exhaustive, mais d'une synthèse des principaux paramètres de confidentialité. Nous vous recommandons de consulter un expert juridique pour obtenir des conseils sur les besoins spécifiques de votre organisation, le présent guide ne constituant pas une aide juridique.

Points à prendre en compte pour les responsables du traitement

Paramètres de confidentialité courants	Responsabilité du client	Support fourni par Google Workspace
Comprendre l'organisation et son contexte	L'organisation doit déterminer son rôle en tant que responsable du traitement des informations personnelles et/ou de sous-traitant des informations personnelles pour déterminer les exigences (réglementaires, etc.) à respecter lors du traitement des Données client à Caractère Personnel.	Consultez les rôles et responsabilités lors du traitement de Données client dans la section 5 de l'Avenant relatif au traitement des données de Google Workspace.
Déterminer quand le consentement est requis et l'enregistrer	Le client doit comprendre les exigences légales ou réglementaires prévoyant l'obligation d'obtenir l'autorisation des personnes physiques avant de traiter leurs Données client à Caractère Personnel et d'enregistrer cette autorisation lorsqu'elle est nécessaire.	Google ne fournit pas d'assistance pour obtenir et enregistrer le consentement des utilisateurs pour l'ensemble de vos activités. Lorsqu'un utilisateur se connecte au compte Google que vous avez créé, il reçoit un avis qui explique comment ses données sont collectées et visualisées par l'administrateur.
Définir la base légale et décrire l'objectif	Le client doit comprendre l'ensemble des exigences qui constituent la base légale du traitement de données, par exemple la nécessité d'obtenir le consentement ou non. Le client doit indiquer dans quel but les Données client à Caractère Personnel sont	Google ne fournit pas directement d'assistance pour définir la base légale du traitement pour l'ensemble de vos activités. Pour en savoir plus sur les opérations de traitement exécutées pour vous par Google et les finalités de ce traitement, consultez les Conditions d'utilisation de Google Workspace et l'Avenant relatif au

	traitées.	traitement des données.
Contrats avec les sous-traitants d'informations personnelles	Le client doit s'assurer que ses contrats avec les sous-traitants comprennent des exigences de conformité légale ou réglementaire concernant le traitement et la protection des Données client à Caractère Personnel.	En tant que sous-traitant des données, Google vous aide à vous conformer à vos obligations (en tenant compte de la nature du traitement des Données à caractère personnel du Client et des informations dont dispose Google) conformément à l'Avenant relatif au traitement des données. Pour obtenir des informations supplémentaires, consultez les sections 7.1.4 (assistance pour la sécurité), 9.2.2 (assistance concernant les droits des personnes concernées) et 8.1 (assistance pour l'analyse d'impact relative à la protection des données).
Limitation de la collecte et du traitement des données	Le client doit comprendre les limites applicables à la collecte et au traitement des Données client à Caractère Personnel (par exemple, il doit accepter que la collecte et le traitement des données doivent se limiter à ce qui est nécessaire pour la finalité prévue).	Pour en savoir plus sur les opérations de traitement exécutées pour vous par Google et les finalités de ce traitement, consultez les Conditions d'utilisation de Google Workspace et l'Avenant relatif au traitement des données.
Enregistrements sur les informations personnelles traitées	Le client doit conserver tous les enregistrements nécessaires et exigés liés aux Données client à Caractère Personnel traitées.	Google Workspace fournit des journaux d'audit pour vous informer sur les accès aux données et vous aider à savoir *qui a fait quoi, où et quand.* Sont inclus les journaux des activités d'administration (journal d'audit de la console d'administration), les journaux de sécurité (connexion, SAML et Access Transparency) et les journaux des services et comptes utilisateur (recherche dans le journal des e-mails et journal d'audit de Drive). Pour en savoir plus sur les journaux d'audit, consultez Journaux d'audit disponibles. Les journaux d'audits sont généralement conservés six mois (pour plus de détails, consultez l'article Conservation des données et temps de latence). Vous pouvez personnaliser le contenu des journaux d'audit depuis la console d'administration Google en filtrant par utilisateur, activité, unité organisationnelle ou par date. Vous pouvez également configurer des alertes pour certaines activités.

Règles sur la protection des données de votre organisation et évaluation

Paramètres de confidentialité courants	Responsabilité du client	Support fourni par Google Workspace
Examen indépendant de la sécurité des informations	Le client doit mettre en œuvre un processus d'évaluation des risques liés à la sécurité des informations pour identifier les risques de perte de confidentialité, d'intégrité et de disponibilité. Ce processus peut comprendre des audits internes ou externes ou d'autres mesures permettant d'évaluer la sécurité du traitement. Nous recommandons au client de collecter les informations des évaluations effectuées par toute autre organisation ou tiers dont il dépend pour une partie ou pour l'ensemble du traitement.	Vous êtes responsable de votre utilisation des services et des copies des données Client que vous stockez en dehors des systèmes Google ou des systèmes de sous-traitance de Google. Google se soumet à un nombre croissant d'audits conduits à intervalles réguliers par des tiers indépendants. Pour chacun d'entre eux, un auditeur indépendant examine nos centres de données, notre infrastructure et nos opérations. Des audits réguliers sont effectués pour certifier notre conformité aux normes d'audit ISO/CEI 27001, ISO/CEI 27017, ISO/CEI 27018, ISO/CEI 27701 et SOC 2. Pour obtenir la liste des certifications liées à la conformité, accédez au Centre de ressources pour la conformité de Google Cloud. Selon les termes de votre contrat avec Google en tant que client Google Workspace, Google peut vous donner l'autorisation (ou à un auditeur indépendant désigné par vos soins) d'effectuer des audits (y compris des inspections) pour vérifier que Google se conforme à ses obligations, conformément à la section 7.5 (Examens et audits de conformité) de l'Avenant relatif au traitement des données.
Analyse d'impact relative à la protection des données	Le client doit être informé de l'obligation de procéder à une analyse d'impact relative à la protection des données (quand l'effectuer, éléments à analyser, qui doit la réaliser, etc.).	En tant que sous-traitant de vos données, Google vous aide à garantir le respect de ses obligations liées à l'analyse d'impact relative à la protection des données (en tenant compte de la nature du traitement et des informations dont dispose Google) conformément à la section 8 de l'Avenant

		relatif au traitement des données.
Détermination de la portée du système de gestion de la sécurité des informations	Le client doit intégrer le traitement de Données client à Caractère Personnel et les obligations correspondantes à son programme global de sécurité et de confidentialité. Les règles de développement et de conception du système doivent comprendre des recommandations sur le traitement des informations personnelles de l'organisation, selon les obligations du responsable des informations personnelles et/ou la législation applicable et/ou la réglementation et le type de traitement effectué par l'organisation.	Google ne fournit pas d'assistance pour les processus internes de ses clients. Au moins une fois par an, envisagez de créer des règles de confidentialité assorties de supports de formation à l'intention des utilisateurs et des groupes de protection de la confidentialité dans votre organisation. Google propose divers services professionnels pour informer les utilisateurs sur la sécurité et la confidentialité dans le cloud, y compris le service d'évaluation de la sécurité Google Workspace.
Règles de sécurité des informations	Le client doit inclure la protection des Données client à Caractère Personnel dans ses règles existantes de sécurité des informations, y compris les règles qui permettent d'assurer la conformité avec la législation applicable. Il doit aussi désigner un responsable de la formation sur la protection des Données client à Caractère Personnel.	Google ne fournit pas d'assistance pour les processus internes de ses clients. Vous pouvez envisager de définir, pour l'ensemble de votre organisation, des règles d'évaluation de la sécurité et de la confidentialité ainsi que des règles d'autorisation qui précisent les procédures et les exigences à respecter pour les évaluations de la confidentialité de l'organisation, les paramètres de confidentialité et le contrôle des autorisations.
Considérations sur l'organisation de la sécurité des informations mise en place par le client	Le client doit attribuer, au sein de son organisation, des responsabilités liées à la sécurité et à la protection des Données client à Caractère Personnel. Il peut être amené à créer des rôles spécifiques pour superviser tout ce qui a trait à la confidentialité, par exemple celui de délégué à la protection des données (DPD). Il convient d'assurer la formation et l'encadrement appropriés pour	Google ne fournit pas d'assistance pour les processus internes de ses clients. Nous vous recommandons de charger une ou plusieurs personnes de développer, mettre en œuvre, maintenir et superviser un programme global de confidentialité et de gouvernance, afin de garantir la conformité avec la législation et les réglementations applicables au traitement des informations personnelles.

	accompagner ces rôles.	Vous pouvez désigner votre délégué à la protection des données et votre représentant dans l'UE dans la console d'administration en accédant à **Paramètres du compte > Conformité**. Google a désigné un DPD pour Google LLC et ses filiales, qui est chargé de couvrir tout ce qui concerne le traitement des données et les différentes réglementations sur la confidentialité.
Classification des informations	Le client doit définir explicitement son utilisation des informations personnelles pour établir son modèle de classification des données.	Google ne fournit pas d'assistance pour les processus internes de ses clients. Le modèle de système de classification des données que vous mettez en œuvre doit explicitement tenir compte de votre utilisation des informations personnelles, afin que vous puissiez bien comprendre les types et les catégories spécifiques d'informations personnelles que vous traitez, l'endroit où elles sont stockées et les systèmes par lesquels elles peuvent transiter. Votre modèle de classification des données doit décrire la manière dont vous classez les données selon leur sensibilité et leur caractère identifiable. Les propriétaires des données ont la responsabilité d'établir une classification appropriée en fonction des besoins et des finalités d'accès à ces données, des risques potentiels, du préjudice en cas d'accès non autorisé à ces données et du contexte général associé à ces informations.
Gestion des incidents concernant la sécurité des informations	Le client doit mettre en place des processus qui mettent en évidence les violations de Données client à Caractère Personnel. Il doit comprendre et décrire ses	Nous vous recommandons d'établir pour votre organisation un règlement pour la gestion des incidents, par exemple des procédures pour faciliter et mettre en œuvre des contrôles dans ce domaine ; il est également conseillé de créer des groupes de sécurité pour les équipes et

	responsabilités en cas de violation des données ou d'incident de sécurité touchant des Données client à Caractère Personnel. Ces responsabilités comprennent : informer les parties concernées, communiquer avec les sous-traitants ou d'autres tiers et assumer toute responsabilité interne à son organisation.	les autorités devant intervenir en cas d'incident dans votre organisation. Nous vous recommandons aussi d'élaborer un plan de test, des procédures et des checklists pour la gestion des incidents, ainsi que des exigences et des critères de réussite. Envisagez de définir les catégories d'incidents que votre organisation doit être capable d'identifier et spécifiez les actions correspondantes pour y répondre. Vous pouvez aussi définir les actions spécifiques que le personnel autorisé doit entreprendre en cas d'incident, comme la marche à suivre pour gérer les fuites d'informations, les failles de cybersécurité et les piratages. Tirez également parti des fonctionnalités de Google Workspace pour analyser et mettre en quarantaine le contenu de certains e-mails,bloquer les tentatives d'hameçonnage et appliquer des restrictions aux pièces jointes. Vous pouvez aussi utiliser la protection contre la perte de données pour inspecter, classer et anonymiser les données sensibles et ainsi réduire leur exposition. Consultez Empêcher la perte de données grâce au nouveau système de protection contre la perte de données pour Drive, Analyser le trafic de messagerie avec la protection contre la perte de données et le livre blanc sur la protection contre la perte de données. En tant que client Google, Google vous envoie rapidement une notification en cas d'incident lié aux données et prend sans délai des mesures raisonnables pour minimiser les dommages et sécuriser les données client. Consultez nos engagements dans la section 7.2 (Incidents relatifs aux données) de l'Avenant relatif au traitement des données. Consultez aussi le Processus

		de gestion des incidents liés aux données.
Sauvegarde des informations	Le client doit établir des règles pour répondre aux obligations de sauvegarde, de récupération et de restauration des informations personnelles (dans le cadre d'un règlement général sur les sauvegardes, par exemple) et toute autre obligation (contractuelle et/ ou légale, par exemple) de suppression des informations personnelles conservées à des fins de sauvegarde.	Nous vous recommandons d'élaborer un plan d'urgence qui définit des procédures et des exigences de mise en œuvre de la planification d'urgence pour l'ensemble de votre organisation. Nous vous conseillons également de dédier du personnel et de définir des rôles et des responsabilités stratégiques pour les situations d'urgence, pour l'ensemble de l'organisation. Définissez aussi les opérations du système d'information qui sont essentielles à la mission et aux activités de votre organisation. Définissez des indicateurs cibles pour la durée maximale d'interruption admissible (DMIA) et la perte de données maximale admissible (PDMA) en cas de reprise des opérations essentielles après activation du plan d'urgence. Décrivez les systèmes d'information critiques et les logiciels associés. Indiquez un maximum d'informations de sécurité, et définissez des directives et des exigences pour le stockage de copies de sauvegarde des composants et des données critiques du système. Google détient et exploite dans le monde entier des centres de données qui contribuent à maintenir Internet accessible 24h/24, 7j/7 et à faire bénéficier nos clients de fonctionnalités de redondance et de résilience. Vous pouvez aussi déployer la fonctionnalité supplémentaire Sauvegarde et synchronisation entre vos fichiers locaux et Google Drive.

Protection des données et paramètres de sécurité

Paramètres de confidentialité courants	Responsabilité du client	Support fourni par Google Workspace
Gestion des accès utilisateur (y compris le provisionnement des accès, et la gestion des accès privilégiés)	Le client doit connaître et gérer de manière appropriée ses responsabilités liées au contrôle des accès dans le service qu'il utilise, en se servant des outils à sa disposition.	Nous vous recommandons de définir à l'échelle de votre organisation des règles sur le contrôle des accès aux comptes du système d'information dans le cloud. Il est également conseillé de configurer les paramètres et les procédures selon lesquels votre organisation crée, active, modifie, désactive et supprime les informations des comptes système. La console d'administration Google offre un espace centralisé qui rend les opérations de configuration et de gestion plus efficaces. Vous pouvez protéger votre organisation grâce aux données analytiques sur la sécurité et aux bonnes pratiques de notre Centre de sécurité. Utilisez Cloud Identity and Access Management (IAM) pour attribuer des rôles et des autorisations aux groupes d'administration grâce aux principes du moindre privilège et de la séparation des tâches. Découvrez comment ajouter Cloud Identity à votre compte Google Workspace.
Procédures de connexion sécurisées	Le client doit mettre en place des procédures de connexion sécurisées pour tous les comptes utilisateur qui sont sous son contrôle.	En tant que client Google Workspace, vous pouvez utiliser les fonctionnalités intégrées de Cloud Identity pour gérer les utilisateurs et configurer des options de sécurité comme la validation en deux étapes et les clés de sécurité. La validation en deux étapes vous permet d'ajouter un niveau de sécurité supplémentaire aux comptes Google Workspace en demandant aux utilisateurs de saisir un code de validation en complément de leur nom d'utilisateur et de leur mot de passe pour accéder à leur compte.

		La clé de sécurité est une amélioration de la validation en deux étapes. Clé physique utilisée pour accéder à un compte Google géré par une organisation, elle a été élaborée par Google en collaboration avec l'organisme de normalisation FIDO Alliance. Elle envoie une signature chiffrée plutôt qu'un code. Ainsi, il est impossible de dérober les informations de connexion par hameçonnage. Pour en savoir plus, consultez Utiliser une clé de sécurité pour la validation en deux étapes. Pour découvrir d'autres fonctionnalités d'authentification/d'autorisation des utilisateurs, consultez le livre blanc sur la sécurité et la conformité de Google Cloud.
Journalisation des événements et protection	Le client doit comprendre les fonctionnalités de journalisation des événements fournies par le système et être en mesure de consigner les actions liées aux Données client à Caractère Personnel qu'il juge nécessaires. Une procédure d'examen des journaux d'événements permettant d'identifier les irrégularités et de proposer des mesures correctives doit être mise en place au moyen d'outils automatisés de surveillance et d'alerte fonctionnant en continu. La procédure peut également être manuelle si l'examen doit avoir lieu à intervalles définis et réguliers.	Google Workspace fournit des journaux d'audit pour vous aider à savoir *qui a fait quoi, où et quand.* Sont inclus les journaux des activités d'administration (journal d'audit de la console d'administration), les journaux de sécurité (connexion, SAML et Access Transparency) et les journaux des services et comptes utilisateur (recherche dans le journal des e-mails et journal d'audit de Drive). Pour en savoir plus sur les journaux d'audit, consultez Journaux d'audit disponibles. Les journaux d'audits sont généralement conservés six mois (pour plus de détails, consultez l'article Conservation des données et temps de latence). Vous pouvez personnaliser le contenu des journaux d'audit depuis la console d'administration Google en filtrant par utilisateur, activité, unité organisationnelle ou par date. Vous pouvez également configurer des alertes pour certaines activités.

Chiffrement	Le client doit définir les données à chiffrer et déterminer si le service qu'il utilise permet de le faire. Il doit recourir au chiffrement au besoin, à l'aide des outils mis à sa disposition.	Les données client de Google Workspace sont chiffrées lorsqu'elles sont en transit, au repos ou stockées sur des supports de sauvegarde. Le chiffrement est un élément essentiel de la stratégie de sécurité de Google Workspace. Il contribue à protéger vos e-mails, vos discussions, vos fichiers Google Drive et toutes les autres données. Pour en savoir plus sur la protection de vos données lorsqu'elles sont au repos, en transit ou stockées sur des supports de sauvegarde, ainsi que sur la gestion des clés de chiffrement, consultez le livre blanc sur le chiffrement dans Google Workspace. En tant qu'administrateur, si votre organisation nécessite un chiffrement supplémentaire des e-mails sortants, vous pouvez créer des règles afin d'exiger que les messages sortants soient signés et chiffrés à l'aide du protocole S/MIME. Vous garantissez ainsi la sécurité, la confidentialité et l'intégrité des Données client à Caractère Personnel.
Enregistrements liés aux pays et aux organisations auxquels les informations personnelles sont susceptibles d'être transmises	Le client doit savoir vers quels pays les Données client à Caractère Personnel sont ou peuvent être transférées, et il doit être en mesure de fournir cette information à qui de droit. Si un tiers ou un sous-traitant se charge de ces transferts, le client doit demander cette information au sous-traitant.	Google détient et exploite des centres de données dans le monde entier afin de maintenir ses produits accessibles 24h/24, 7j/7. Pour plus d'informations, consultez Découvrez où sont implantés nos centres de données. Vous pouvez choisir de stocker vos données à l'emplacement géographique de votre choix (aux États-Unis ou en Europe) en utilisant un règlement relatif à l'emplacement des données. Ce service offre un contrôle précis des emplacements géographiques des espaces de stockage des e-mails, documents et autres contenus Google Workspace. Examinez scrupuleusement nos offres de produits concernés par l'emplacement des

		données et consultez un conseiller juridique pour décider vous-même si ces offres répondent à vos besoins spécifiques (commerciaux et réglementaires).
Enregistrements liés à la divulgation d'informations personnelles à des tiers	Le client doit garder des enregistrements de ses divulgations d'informations personnelles à des tiers, y compris la nature des informations personnelles divulguées, le destinataire et la date. Il peut s'agir, par exemple, de divulgations aux autorités judiciaires. Si un tiers ou un sous-traitant divulgue les données, le client doit s'assurer qu'ils conservent les enregistrements appropriés et les obtenir si nécessaire.	Google et ses sociétés affiliées ont recours à divers *sous-traitants* pour assurer le fonctionnement de leurs services. Pour plus d'informations, consultez la liste des sous-traitants indirects de Google Workspace. Nous vous recommandons, en tant qu'administrateur, d'évaluer l'utilisation des applications tierces. Vous pouvez empêcher les utilisateurs d'utiliser des applications tierces telles que les applications pour Google Drive et les modules complémentaires Google Docs. Nous vous recommandons d'examiner la documentation sur la sécurité fournie par les développeurs tiers, ainsi que les conditions relatives au traitement des données applicables, avant d'utiliser une application tierce avec Google Drive et Google Docs. Si Google reçoit une requête d'un gouvernement au sujet des données d'un client Cloud, sa politique est de demander au gouvernement de déposer sa requête de données directement auprès du client Cloud. Les requêtes que nous recevons sont toutes examinées et évaluées par notre équipe qui vérifie leur conformité aux obligations légales. Lorsqu'il a obligation de divulguer des données, Google notifie rapidement le client avant de procéder à la divulgation, sauf si la loi l'interdit ou qu'une situation d'urgence vitale l'impose. Dans la limite autorisée par la loi ou par les conditions de la requête, Google accédera aux demandes raisonnables du client pour s'opposer à la requête.

		Des informations détaillées sont disponibles dans notre rapport Transparence des informations et notre livre blanc sur les demandes gouvernementales concernant les données des clients Cloud.
Déterminer les droits des personnes concernées et leur en permettre l'exercice (comme l'accès, la rectification, la suppression et la portabilité)	Le client doit connaître les obligations liées aux droits des personnes vis-à-vis du traitement de leurs Données à Caractère Personnel. Ces droits peuvent notamment porter sur l'accès, la rectification, la suppression et la portabilité. Si le client utilise un système tiers, il doit déterminer les parties de ce système (si elles existent) qui fournissent des outils permettant aux personnes d'exercer leurs droits (par exemple, accéder à leurs données). Si le système propose de telles fonctionnalités, le client doit les utiliser en cas de besoin.	La console d'administration Google vous permet, en tant qu'administrateur, de respecter les obligations potentielles liées aux Requêtes de personnes concernées. Google Workspace offre des fonctionnalités permettant aux administrateurs Google Workspace et aux personnes concernées d'accéder aux données client à caractère personnel et de les exporter directement depuis les produits Google. Les administrateurs Google Workspace ont accès à notre outil d'exportation des données pour exporter des données organisationnelles et à Google Vault pour effectuer des recherches et des exportations ciblées, basées sur l'utilisateur. Les personnes concernées (les utilisateurs) peuvent utiliser l'interface Google Takeout pour accéder directement aux données client à caractère personnel pertinentes et les exporter de manière autonome. Pour savoir comment faire, consultez le Guide sur les Requêtes des personnes concernées de Google Workspace.

Rétentionet suppression	L'organisation qui traite les informations personnelles doit vérifier, selon la juridiction concernée, qu'elle détient toujours les informations personnelles après une période donnée.	En tant qu'administrateur, Google effacera les données client concernées des systèmes Google à votre demande. Les administrateurs gèrent les comptes utilisateur depuis la console d'administration Google. Ils peuvent ainsi supprimer un compte ou effacer des données client à caractère personnel des produits et des appareils mobiles. Si votre organisation est tenue de conserver des données pendant un certain temps, vous pouvez configurer Vault pour qu'il conserve les messages et les fichiers, et ce même si les utilisateurs les suppriment et vident la corbeille. Pour en savoir plus sur les paramètres de suppression, reportez-vous au Guide sur les Requêtes des personnes concernées de Google Workspace. Consultez nos engagements sur la suppression des données dans la section 6 (Suppression des données) de l'Avenant relatif au traitement des données. Consultez la Déclaration de confidentialité de Google Cloud concernant la suppression et la conservation des données de service.
Gestion des points de terminaison	Le client doit garantir que l'utilisation d'appareils mobile ne compromet pas les informations personnelles.	En tant qu'administrateur utilisant la gestion des points de terminaison Google, vous pouvez sécuriser les données de votre organisation sur les appareils mobiles, les ordinateurs de bureau, les ordinateurs portables et tout autre point de terminaison de vos utilisateurs. La gestion de base vous permet de mettre en place l'application forcée d'un code secret de base, des rapports relatifs aux mobiles, une protection contre le piratage, l'effacement à distance des données d'un compte, des alertes et des audits pour appareil mobile. La gestion avancée vous offre des fonctionnalités de sécurité et de confidentialité supplémentaires comme l'application forcée d'un mot de passe

		sécurisé, le blocage d'appareils dont la sécurité est compromise, l'approbation des appareils et bien plus encore. Pour obtenir plus d'informations et choisir la version qui vous convient le mieux, consultez la page Comparer les fonctionnalités de gestion des appareils mobiles. Consultez également Configurer la gestion de base des appareils mobiles et Configurer la gestion avancée des appareils mobiles.