RESILIENCE

Politique de confidentialité

Document d'information (sans acceptation)

Date de publication : 11 novembre 2026

En vigueur au 18 novembre 2026

Éditeur : RESILIENCE, SARL, RCS 1 494 970, Nouméa, Nouvelle-Calédonie

Pour consulter en ligne : voc.nc/politique-confidentialite

Empreinte SHA-256 du texte archivé : b04d5e1e49b10c5c2dab539cffaaeb6336be84685987f082e6131fc370ebd2af

Politique de confidentialité

En vigueur au 18 novembre 2026.

Responsable du traitement

Le service voc.nc est édité par RESILIENCE (SARL, RCS 1 494 970, siège à Nouméa, Nouvelle-Calédonie). Pour l'ensemble des traitements décrits ci-dessous, le responsable de traitement au sens du RGPD est :

- RESILIENCE - service voc.nc
- Délégué à la protection des données (DPO) : dpo@voc.nc
- Courrier général : contact@rsl.nc

voc.nc est exclusivement destiné à une clientèle professionnelle (ci-après « l'Organisation »). L'Organisation, qui conduit ses enquêtes sur voc.nc, est responsable de traitement vis-à-vis des personnes concernées, décrites à la fiche T-02. voc.nc agit en qualité de sous-traitant au sens de l'article 28 du RGPD ; les conditions de cette sous-traitance sont formalisées dans le DPA.

Notre philosophie : zéro numéro en base, zéro cookie sur l'enquête publique

voc.nc a été conçu pour que la vie privée des personnes sondées ne repose pas sur la discipline d'exploitation, mais sur une architecture technique irréversible :

- Les références communiquées par nos clients professionnels ne sont jamais persistées dans nos bases de données. Elles transitent uniquement en mémoire vive le temps d'exécuter les traitements de voc.nc, sont restituées immédiatement à l'Organisation sous forme d'un fichier récapitulatif téléchargeable pendant 24 heures, puis sont définitivement effacées.
- voc.nc dépose au plus deux cookies, décrits dans la politique cookies : le cookie de session __Host-voc_nc_session, sur les écrans de l'espace client, y compris avant la connexion, et sur les pages des rapports partagés protégés par un code d'accès ; le cookie __Host-voc_nc_appareil, seulement si l'utilisateur demande à la connexion que son code de double authentification ne lui soit plus demandé sur ce navigateur. À part cela, ne dépose aucun cookie ou traceur.

Empreinte SHA-256 du texte archivé : b04d5e1e49b10c5c2dab539cffaaeb6336be84685987f082e6131fc370ebd2af

Traitements effectués

T-01 - Authentification des clients professionnels

Nous traitons votre email professionnel, un mot de passe stocké sous forme hachée (algorithme standard), le nom de votre entreprise et les autres informations que vous déclarez sur elle. L'adresse e-mail de contact de votre organisation est affichée aux personnes sondées pour l'exercice de leurs droits et reçoit les avis de voc.nc (CGU, article 14).

Nous conservons aussi les clés d'API que votre organisation crée pour accéder au service par programme (CGU, article 2.1) : leur nom, leur portée, le compte qui les a créées, une empreinte de la clé et ses six derniers caractères, et la date de leur dernière utilisation, arrondie à cinq minutes - jamais la clé elle-même.

Pour les comptes dont la double authentification est activée (elle est obligatoire pour tout utilisateur avant un geste qui engage des données, et dès la connexion quand votre organisation détient des données), nous conservons aussi le secret qui sert à vérifier les codes de votre application d'authentification, chiffré, et une empreinte de chacun de vos codes de récupération - jamais les codes eux-mêmes.

Si vous demandez, à la connexion, que votre code ne vous soit plus demandé sur un navigateur, nous conservons pour cet appareil de confiance une empreinte de l'identifiant déposé dans ce navigateur, sa date de création, d'expiration (30 jours) et de dernière utilisation, la signature technique que ce navigateur transmet à ce moment (chaîne « user-agent ») et le libellé qui en est tiré - système et navigateur, par exemple « Windows · Chrome » -, seul affiché, pour que vous reconnaissiez l'appareil à révoquer sur la page Sécurité ; jamais l'adresse IP.

Un appareil expiré n'ouvre plus rien ; sa trace est supprimée au plus tard le lendemain de son expiration, trente jours après sa déclaration - et plus tôt si vous le révoquez, si vous changez de mot de passe, si vous désactivez ou reconfigurez la double authentification, ou avec votre compte.

Si vous n'avez plus accès à votre application d'authentification, vous pouvez recevoir un code à usage unique par e-mail, valable 10 minutes : nous n'en conservons qu'une empreinte et l'heure d'envoi, effacées à votre connexion suivante ; la double authentification est alors réinitialisée et vous la configurez à nouveau - jusque-là, chaque connexion vous demande un tel code.

Si vous perdez aussi l'accès à votre boîte e-mail, notre support peut, après avoir vérifié votre identité, désactiver la double authentification de votre compte ; votre mot de passe est alors remplacé, vos sessions ouvertes sont fermées et vous recevez un lien pour en choisir un nouveau.

Nous conservons une trace de chaque déblocage : le compte concerné, la personne du support qui l'a fait, la date et le motif, qui indique qui a demandé le déblocage et comment l'identité a été vérifiée - il peut donc nommer un autre administrateur de votre organisation. Cette trace est supprimée avec votre compte.

Empreinte SHA-256 du texte archivé : b04d5e1e49b10c5c2dab539cffaaeb6336be84685987f082e6131fc370ebd2af

Quand vous acceptez les CGU et le DPA au nom de votre organisation, ou les CGU pour votre propre compte en prenant connaissance du DPA, nous en conservons une trace : le document et sa version, la date et l'heure de l'acceptation, la version du texte de la case cochée, le rôle de votre compte, votre adresse e-mail et la date de sa confirmation, ainsi que la dénomination, la forme juridique et la référence légale de l'organisation ce jour-là.

Quand un administrateur invite un utilisateur, nous conservons l'adresse e-mail invitée, le rôle proposé, le compte qui invite, une empreinte du lien envoyé et son échéance, 72 heures après l'envoi. L'invitation est supprimée quand elle est acceptée ou annulée, quand celui qui l'a envoyée n'est plus administrateur de l'organisation, et au plus tard le lendemain du trentième jour qui suit son échéance.

Nous tenons aussi un journal des membres de votre organisation : invitations envoyées, annulées et acceptées, changements de rôle et retraits, avec la date, le compte qui agit, le compte concerné le cas échéant et les rôles avant et après - désignés par leur identifiant, sans adresse e-mail. Ce journal est conservé vingt-quatre mois, et supprimé plus tôt avec les données de l'Organisation.

Quand nous notifions une nouvelle version de ces documents, nous conservons, pour chaque envoi, le document, sa version, la date d'envoi et l'adresse du destinataire ; pour l'adresse de contact de l'organisation, une empreinte de cette adresse seulement. Aucune adresse IP n'est conservée au titre de ces traces.

Base légale

exécution du contrat (art. 6.1.b RGPD) et obligation comptable.

pour les traces d'acceptation et de notification, l'intérêt légitime de RESILIENCE à pouvoir prouver la conclusion du contrat et l'information de l'Organisation (art. 6.1.f RGPD).

Durée de conservation

Ces données sont conservées pendant la durée du contrat de votre organisation. Chaque utilisateur peut supprimer son propre compte à tout moment depuis son espace, sauf le dernier administrateur d'une organisation qui a d'autres utilisateurs ; la suppression est immédiate et ne porte pas sur les données de l'Organisation. Un administrateur peut aussi retirer un autre utilisateur : son compte est alors supprimé de la même façon.

Quand l'Organisation n'a plus d'utilisateur, ses clés d'API sont révoquées et elle en est informée à son adresse e-mail de contact. Ses formulaires continuent de recevoir des réponses par les liens déjà émis et ses rapports partagés restent consultables jusqu'à leur date d'expiration, s'ils en ont une. Sans demande à contact@voc.nc dans les douze mois, son contrat prend fin.

Le contrat prend fin aussi si aucun administrateur n'accepte expressément, au nom de l'Organisation, une nouvelle version des CGU ou du DPA dans les douze mois qui suivent le premier avis qui l'annonce, et dans les autres cas prévus à l'article 8 des CGU. À la fin du contrat, l'ensemble de ses données est supprimé sous 30 jours ; elle peut en demander l'export pendant ce délai.

L'Organisation peut aussi demander à dpo@voc.nc la suppression de l'ensemble de ses données à tout moment : elle est exécutée sous 30 jours et met fin au contrat. Les copies de sauvegarde sont écrasées à leur rotation.

Empreinte SHA-256 du texte archivé : b04d5e1e49b10c5c2dab539cffaaeb6336be84685987f082e6131fc370ebd2af

Par exception, les traces d'acceptation et de notification décrites ci-dessus ne sont supprimées ni avec le compte qui les a produites, ni avec les données de l'Organisation. Elles sont conservées pendant la durée du contrat et cinq ans après sa fin, pour la constatation, l'exercice ou la défense de droits en justice ; pendant ce délai, elles ne sont pas effacées sur demande, même en cas d'opposition (art. 17.3.e et 21.1 RGPD).

Les pièces que la loi impose de conserver (comptabilité) le sont pour la durée légale applicable - à ce jour, seul le temps d'audit prévu à l'article 10 du DPA peut être facturé.

Les durées propres à l'appareil de confiance, au code envoyé par e-mail, à la trace d'un déblocage, aux invitations et au journal des membres sont indiquées avec leur description, plus haut.

T-02 - Génération de liens de réponse à usage unique

Personnes concernées : les personnes à qui l'Organisation destine un lien de réponse et celles qui répondent par ce lien (personnes sondées), quelle que soit leur relation avec elle (client, usager, membre de son personnel ou autre) ; les personnes que désigne, directement ou non, le contenu d'un formulaire ou d'une réponse, qu'elles appartiennent ou non au personnel de l'Organisation (une note peut porter sur une personne qu'un formulaire désigne, un texte libre peut nommer quiconque).

Cas d'utilisation principal de voc.nc : pour chaque destinataire fourni par l'Organisation, nous générons un lien de réponse à usage unique, porteur d'un jeton opaque (aléatoire, sans lien mathématique avec la référence destinataire) qui permet à ce destinataire d'accéder au formulaire d'enquête une seule fois.

Nous conservons : le jeton d'accès, un identifiant d'enquête unique, les horodatages techniques d'émission, de réponse et d'expiration du lien - rattachés au jeton et non à une personne identifiée côté voc.nc -, et les réponses saisies par la personne sondée (valeurs choisies sur l'échelle de la question, réponses oui/non, choix parmi les options proposées, textes libres).

La référence fournie par l'Organisation transite en mémoire le temps de la génération et n'est jamais conservée : elle est restituée immédiatement dans un fichier récapitulatif téléchargeable pendant 24 heures. L'Organisation génère ces liens depuis son espace ou par l'API (CGU, article 2.1) ; par l'API, la référence lui est rendue dans la réponse à son appel et n'est pas davantage conservée.

Sur un formulaire que l'Organisation a déclaré anonyme, la réponse est enregistrée dissociée du jeton qui l'a portée ; elle porte la date de fin du formulaire, jamais le jour où elle a été donnée ; son contenu n'est pas modifié - un commentaire libre qui identifie son auteur reste tel quel. Ces réponses restent des données à caractère personnel. L'Organisation sait si votre lien a servi, jamais ce que vous avez répondu. Rien ne lui est restitué avant la date de fin du formulaire, ni ensuite si le formulaire a reçu moins de cinq réponses au total - ces réponses sont alors supprimées trois mois après la date de fin ; à partir de cinq réponses, tout lui est restitué, réponses une à une et textes libres compris, sans lien avec une personne et dans un ordre qui ne suit pas celui des réponses (CGU, article 9.1 ; page Formulaires anonymes).

Empreinte SHA-256 du texte archivé : b04d5e1e49b10c5c2dab539cffaaeb6336be84685987f082e6131fc370ebd2af

Finalité

permettre à l'Organisation de recueillir et de mesurer l'avis des personnes sondées, par des enquêtes ciblées, ponctuelles ou récurrentes.

Base légale

celle déclarée par l'Organisation, responsable du traitement (intérêt légitime ou exécution du contrat) ; voc.nc agit comme sous-traitant (art. 28 RGPD) et ne détermine pas cette base légale. L'Organisation la déclare dans son formulaire, et l'information qui en découle est affichée à la personne sondée sur la page de réponse.

Durée de conservation

Les réponses sont conservées jusqu'à la suppression de l'ensemble des données de l'Organisation (voir T-01). Un lien de réponse est valable trois mois à compter de son émission, ou jusqu'à la date de fin du formulaire si elle est plus proche.

24 mois après l'échéance d'un lien, la réponse qu'il a portée en est dissociée - son horodatage réduit au jour, ses textes libres effacés - et le lien est supprimé, qu'il ait servi ou non ; cette dissociation ne supprime pas la réponse. Les journaux de diffusion sont supprimés 24 mois après leur création.

Par exception, les réponses d'un formulaire anonyme clos avec moins de cinq réponses sont supprimées trois mois après sa date de fin.

Un formulaire qui n'a pas encore été distribué peut être supprimé ; une fois distribué, il ne peut plus qu'être archivé, ce qui ne supprime aucune réponse.

Chaque utilisateur peut supprimer son propre compte à tout moment depuis son espace, sauf le dernier administrateur d'une organisation qui a d'autres utilisateurs ; la suppression est immédiate et ne porte pas sur les données de l'Organisation. La fin du contrat et la suppression des données de l'Organisation sont décrites en T-01.

T-03 - Mesure d'audience agrégée (cookieless)

Mesure d'audience sans cookie ni empreinte de navigateur (fingerprinting), réalisée par un outil hébergé et exploité par RESILIENCE en France (Union européenne). Aucun suivi d'une visite d'un jour sur l'autre.

- Périmètre : l'ensemble des pages du service, y compris l'espace client et le formulaire d'enquête public /r/:token.

Données traitées

URL consultée, temps passé sur la page et part de la page parcourue, type de navigateur et de système d'exploitation, référent, pays inféré. Les identifiants figurant dans les adresses des pages (liens de réponse, rapports partagés) sont masqués avant transmission à la mesure d'audience.

Empreinte SHA-256 du texte archivé : b04d5e1e49b10c5c2dab539cffaaeb6336be84685987f082e6131fc370ebd2af

L'adresse IP n'est pas conservée : elle sert à inférer le pays et à calculer, avec le type de navigateur et de système d'exploitation et un sel renouvelé chaque jour, un identifiant de visiteur haché - donnée pseudonymisée, non anonyme ; les statistiques qui en découlent sont restituées sous forme agrégée.

Base légale

· intérêt légitime (art. 6.1.f RGPD) - amélioration du service.

Durée de conservation

· les données détaillées, identifiant de visiteur haché compris, sont conservées 25 mois au plus à compter de leur collecte, puis supprimées. Seuls des totaux mensuels anonymes sont gardés au-delà, sans limitation de durée.

Destinataires

· Hébergeur : Hostinger (sous-traitant), en France (Union européenne), sur la même infrastructure que voc.nc. Aucun tiers n'y accède.

Journalisation des erreurs techniques

Traitement de sécurité commun à tout le service : les erreurs techniques du service sont journalisées par un outil hébergé et exploité par RESILIENCE en France, aux seules fins de sécurité et de continuité du service (intérêt légitime, art. 6.1.f RGPD).

Chaque erreur garde son message, où sont masqués les adresses e-mail, les jetons connus et les numéros au format international. Si elle survient pendant une requête, elle garde aussi l'adresse demandée, le navigateur et l'appareil utilisés (type, système, langue) et l'identifiant de la requête, qui la relie aux journaux du serveur. Sont exclus par configuration : adresse IP, cookies, corps de requête, paramètres de jobs, jetons figurant dans les URL, chaînes de requête et référents.

Durée de conservation

90 jours. Aucun tiers n'y accède.

Journaux du serveur

Traitement de sécurité commun à tout le service : le serveur journalise les requêtes adressées à l'ensemble des pages du service et à l'API - méthode, adresse de la page demandée (les jetons de lien y sont masqués), horodatage, statut et adresse IP - ainsi que les paramètres reçus et, en cas d'erreur, le message qui la décrit, lequel peut reprendre une valeur reçue.

Dans les paramètres sont masqués les mots de passe, codes, jetons et autres secrets, les adresses e-mail, les numéros de téléphone, les références des destinataires et le nom de campagne (saisis à l'import ou transmis par l'API), les réponses aux enquêtes, le message d'une demande d'exercice des droits et la preuve du contrôle anti-robot ; l'en-tête qui transmet la clé d'API n'est jamais journalisé. Le formulaire d'enquête public /r/:token fait exception : aucune adresse IP n'y est journalisée.

Empreinte SHA-256 du texte archivé : b04d5e1e49b10c5c2dab539cffaaeb6336be84685987f082e6131fc370ebd2af

Ces journaux sont effacés au plus tard 180 jours après leur écriture, sauf extrait conservé pour traiter un incident de sécurité, jusqu'à la clôture de celui-ci ; aucun tiers n'y accède.

Les compteurs qui appliquent les limites de débit sont effacés à la fin de leur période de comptage : deux minutes au plus pour ceux de l'API (par clé d'API et par adresse IP), une heure au plus pour ceux que tiennent les autres pages par adresse IP, par compte utilisateur (renvoi du lien de confirmation, avis « adresse déjà utilisée » envoyés au titulaire d'un compte) ou par lien de réponse ou de rapport partagé.

Une clé d'API ou un lien n'y figure jamais en clair : seulement son empreinte ou, pour une clé d'API, le numéro qui la désigne.

Après des échecs de connexion répétés, l'adresse IP et l'adresse e-mail saisie (sous forme d'empreinte) sont bloquées temporairement : compteur et blocage sont conservés une heure au plus pour l'adresse IP, quinze minutes au plus pour l'adresse e-mail.

Chaque compte utilisateur tient en outre le nombre de ses échecs de connexion (mot de passe ou code de double authentification erronés) : ce nombre est conservé sur le compte jusqu'à la connexion réussie suivante ou jusqu'à son déverrouillage ; après des échecs répétés, le compte est verrouillé temporairement, sauf déverrouillage par le lien envoyé à son titulaire.

Finalité

sécurité et continuité du service (intérêt légitime, art. 6.1.f RGPD).

Durées de conservation - récapitulatif

- Réponses aux enquêtes : conservées jusqu'à la suppression de l'ensemble des données de l'Organisation ; dissociées du lien 24 mois après son échéance (horodatage réduit au jour, textes libres effacés), sans être supprimées ; celles d'un formulaire anonyme clos avec moins de cinq réponses sont supprimées trois mois après sa date de fin.
- Liens de réponse : valables trois mois, supprimés 24 mois après leur échéance, qu'ils aient servi ou non ; journaux de diffusion : supprimés 24 mois après leur création.
- Suppression d'un formulaire : un formulaire qui n'a pas encore été distribué peut être supprimé ; une fois distribué, il ne peut plus qu'être archivé, ce qui ne supprime aucune réponse.
- Suppression du compte : chaque utilisateur peut supprimer son propre compte à tout moment depuis son espace, sauf le dernier administrateur d'une organisation qui a d'autres utilisateurs ; la suppression est immédiate et ne porte pas sur les données de l'Organisation.
- Délais de douze mois : une organisation sans utilisateur a douze mois pour demander à contact@voc.nc qu'un utilisateur lui soit rattaché ; une organisation qui n'accepte pas une nouvelle version des CGU ou du DPA a douze mois, depuis le premier avis, pour la faire accepter expressément par un administrateur. À défaut, son contrat prend fin.

Empreinte SHA-256 du texte archivé : b04d5e1e49b10c5c2dab539cffaaeb6336be84685987f082e6131fc370ebd2af

- Fin du contrat : quelle qu'en soit la cause, l'ensemble des données de l'Organisation est supprimé sous 30 jours ; elle peut en demander l'export pendant ce délai. Sa suppression peut aussi être demandée à tout moment à dpo@voc.nc : elle est exécutée sous 30 jours et met fin au contrat.
- Mesure d'audience : 25 mois au plus à compter de leur collecte pour les données détaillées, identifiant de visiteur pseudonymisé compris, puis suppression ; au-delà, seuls des totaux mensuels anonymes sont gardés, sans limitation de durée.
- Journaux d'erreurs techniques : 90 jours.
- Journaux du serveur : 180 jours au plus après leur écriture, hors extrait conservé pour un incident de sécurité ; compteurs de débit : deux minutes au plus pour l'API, une heure au plus pour les autres, par adresse IP, par compte utilisateur ou par lien ; blocage après échecs de connexion : une heure au plus pour l'adresse IP, quinze minutes au plus pour l'adresse e-mail (sous forme d'empreinte) ; échecs de connexion d'un compte : comptés jusqu'à la connexion réussie suivante ou au déverrouillage.
- Traces d'acceptation des CGU et du DPA et de notification de leurs nouvelles versions : durée du contrat et cinq ans après sa fin, y compris après la suppression du compte qui les a produites et celle des données de l'Organisation (voir T-01).
- Données du compte client, clés d'API comprises : durée du contrat, puis suppression sous 30 jours avec l'ensemble des données de l'Organisation (voir T-01). Chaque compte utilisateur se supprime immédiatement, par son titulaire depuis son espace (sauf le dernier administrateur d'une organisation qui a d'autres utilisateurs) ou par un administrateur qui le retire. Le journal des déblocages de la double authentification suit le compte : il est supprimé avec lui.
- Invitations d'un utilisateur : jusqu'à leur acceptation ou leur annulation, au plus tard le lendemain du trentième jour qui suit leur échéance de 72 heures ; journal des membres : vingt-quatre mois, ou moins s'il est supprimé avec les données de l'Organisation (voir T-01).
- Double authentification : appareil de confiance, trente jours après sa déclaration, trace supprimée au plus tard le lendemain de son expiration, ou plus tôt dans les cas décrits en T-01 ; code envoyé par e-mail, empreinte et heure d'envoi effacées à la connexion suivante.

Hébergement et localisation des données

Les données du service voc.nc - base de données, fichiers et journaux applicatifs - sont hébergées en France, chez Hostinger, sur un serveur opéré par RESILIENCE ; les copies de sauvegarde de l'hébergeur sont conservées aux Pays-Bas. La France et les Pays-Bas appartiennent à l'Union européenne.

Hors ces copies, un seul flux de données personnelles quitte ce serveur : l'acheminement des emails par Google Workspace, transfert vers les États-Unis encadré par les clauses contractuelles types de la Commission européenne.

Empreinte SHA-256 du texte archivé : b04d5e1e49b10c5c2dab539cffaaeb6336be84685987f082e6131fc370ebd2af

Sous-traitants

Dans le cadre de l'exploitation du service, nous faisons appel aux sous-traitants suivants :

- Hostinger, hébergeur du serveur qui exécute voc.nc. Finalité : hébergement de l'application, de sa base de données et de ses sauvegardes. Localisation : France, copies de sauvegarde aux Pays-Bas (Union européenne).
- Google Workspace (RESILIENCE). Finalité : hébergement mail. Transfert UE ? États-Unis encadré par les clauses contractuelles types de la Commission européenne.

La liste à jour est également maintenue dans notre DPA (article 6).

Vos droits (articles 13 à 22 du RGPD)

Vous disposez des droits suivants sur les données personnelles vous concernant :

- Droit d'accès (art. 15) et droit à la rectification (art. 16).
- Droit à l'effacement (art. 17), sous réserve des obligations légales de conservation et de la conservation des traces d'acceptation et de notification (T-01).
- Droit à la limitation du traitement (art. 18).
- Droit à la portabilité (art. 20) pour les données que vous nous avez fournies.
- Droit d'opposition (art. 21), sous la même réserve pour les traces d'acceptation et de notification (T-01).

Pour exercer l'un de ces droits, rendez-vous sur notre formulaire d'exercice des droits ou écrivez directement à dpo@voc.nc. Nous accusons réception sous 72 heures ouvrées et répondons sous un mois (RGPD art. 12), prolongeable à trois mois pour les demandes complexes avec information préalable. Un effacement demandé est exécuté sous 30 jours.

Limite technique. voc.nc ne conserve pas la référence qui relie un lien de réponse à une personne : une demande d'accès émanant directement d'une personne sondée, non relayée par l'Organisation, ne peut pas aboutir techniquement de notre côté. Nous la redirigeons alors vers l'Organisation, responsable du traitement. Nous lui transmettons de même la demande d'une personne que désigne un formulaire ou une réponse.

Réclamation auprès de la CNIL

Si vous estimez, après nous avoir contactés, que vos droits n'ont pas été respectés, vous pouvez adresser une réclamation à la Commission nationale de l'informatique et des libertés (CNIL), autorité de contrôle compétente pour la Nouvelle-Calédonie et la Polynésie française :

- CNIL - 3 Place de Fontenoy - TSA 80715 - 75334 PARIS CEDEX 07 - France
- Téléphone : +33 1 53 73 22 22

Empreinte SHA-256 du texte archivé : b04d5e1e49b10c5c2dab539cffaaeb6336be84685987f082e6131fc370ebd2af

· Formulaire de plainte en ligne : cnil.fr/plaintes (https://www.cnil.fr/plaintes)

Modifications

La présente politique peut être amendée pour refléter une évolution du service, un nouveau sous-traitant ou une précision réglementaire. Toute modification substantielle fait l'objet d'une mise à jour de la date en tête du document et, le cas échéant, d'une notification par email aux Organisations concernées.

Empreinte SHA-256 du texte archivé : b04d5e1e49b10c5c2dab539cffaaeb6336be84685987f082e6131fc370ebd2af