QUELQUES PISTES POUR PROTÉGER VOS DONNÉES

Testez vos connaissances

/

Donnée personnelle

Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. Mais, parce qu'elles concernent des personnes, celles-ci doivent en conserver la maîtrise.

Une personne physique peut être identifiée :

- directement (exemple : nom et prénom) ;
- indirectement (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :

- à partir d'une seule donnée (exemple : nom) ;
- à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre dans telle association) :

Par contre, des coordonnées d'entreprises (par exemple, l'entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un courriel de contact générique « compagnie1@email.fr ») ne sont pas, en principe, des données personnelles.

www.cnil.fr

Le sigle RGPD signifie « Règlement Général sur la Protection des Données » (en anglais « General Data Protection Regulation » ou GDPR). Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne.

Le contexte juridique s'adapte pour suivre les évolutions des technologies et de nos sociétés (usages accrus du numérique, développement du commerce en ligne…).

Ce nouveau règlement européen s'inscrit dans la continuité de la Loi française Informatique et Libertés de 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant.

Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels. Il permet de développer leurs activités numériques au sein de l'UE en se fondant sur la confiance des utilisateurs

Qui est concerné par le RGPD ?

Tout organisme quels que soient sa taille, son pays d'implantation et son activité, peut être concerné.
En effet, le RGPD s'applique à toute organisation, **publique et privée**, **qui traite des données personnelles pour son compte ou non,dès lors** :

- qu'elle **est établie sur le territoire de l'Union européenne**,
- ou que son activité cible directement des **résidents européens**.

Par exemple, une société établie en France, qui exporte l'ensemble de ses produits au Maroc pour ses clients moyen-orientaux doit respecter le RGPD.
De même, une société établie en Chine, proposant un site de e-commerce en français livrant des produits en France doit respecter le RGPD.
Le RGPD **concerne aussi les sous-traitants** qui traitent des données personnelles pour le compte d'autres organismes.
Ainsi, si vous traitez ou collectez des données pour le compte d'une autre entité (entreprise, collectivité, association), vous avez des obligations spécifiques pour garantir la protection des données qui vous sont confiées.

Désactiver les services de localisation d'Android

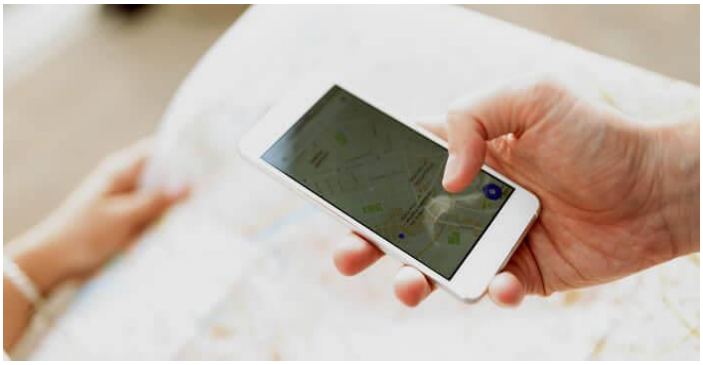
C'est la solution la plus efficace mais aussi la plus radicale puisque vous ne pourrez plus utiliser la puce GPS de votre smartphone Android. Mais est-il bien utile qu'Android connaisse en permanence vos moindres faits et gestes ? La réponse est clairement non.

Et puis n'oubliez pas que certaines applications peuvent se transformer en espions et collecter toutes sortes de **données personnelles**. Une fois récupérées, elles sont généralement transmises à des spécialistes du marketing en ligne pour enrichir votre profil publicitaire.

Voilà pourquoi il est recommandé d'utiliser les services de localisation uniquement lorsque ces derniers présentent une réelle utilité pour vous.

- Ouvrez les paramètres de votre smartphone Android
- Cliquez sur la rubrique localisation ou emplacement
- Appuyez sur le petit interrupteur pour désactiver l'option

Plus aucune application ne pourra avoir accès à vos **données de localisation**. Cela vous permettra de préserver votre vie privée et accessoirement d'améliorer l'autonomie de votre téléphone. Gardez tout de même en tête que cette opération empêchera certaines applications de fonctionner correctement et notamment les assistants virtuels.



APPLE/ iPhone

Votre iPhone enregistre plus de données de localisation que vous ne pensez...

Savez vous que votre iPhone sait où vous travaillez, où vous habitez, et quand et combien de temps vous passez chez vos amis ? Voici comment désactiver cette fonction.

Votre iPhone réunit beaucoup plus de données de localisation vous concernant que vous ne l'imaginiez. Pour l'en empêcher, il faut se pencher sur un réglage qui s'appelle "Lieux fréquents". Alors que vous vaquez à vos occupations quotidiennes, votre iPhone note l'endroit où vous vous trouvez et combien de temps vous y restez. Il repère alors les "lieux fréquents". Il suppose, de manière plutôt précise, que l'endroit où vous vous trouvez la journée est votre lieu de travail et celui où vous vous trouvez la nuit est votre domicile. Quelle que soit l'heure, il traque les endroits où vous vous trouvez : le domicile des amis, les restaurants préférés...

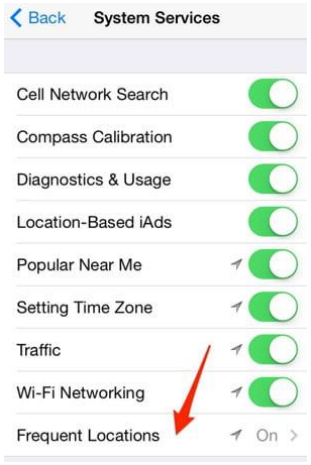
Voici comment voir ce que votre iPhone a identifié comme étant vos lieux fréquents et également de quelle manière désactiver cette fonctionnalité.

1. Dans "Réglages", sélectionnez "Confidentialité".

2 Sélectionnez ensuite "Services de localisation".

3. Descendez jusqu'en bas et sélectionnez "Services système".

4.Finalement, on y est. Sélectionnez "Lieux fréquents".



Voici une liste de ce qu'il estime être nos "lieux fréquents" à chaque fois qu'il enregistre un endroit où nous passons beaucoup de temps. Voyons les endroits qui correspondent à New York.

Pour désactiver cette fonctionnalité de collecte de données de rêve, déplacez ce bouton dans vos réglages.

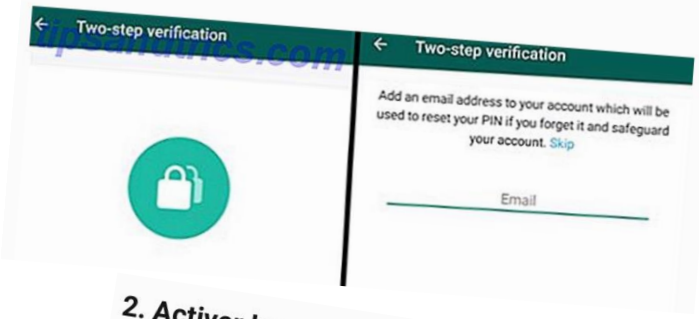
Article de Dylan Love. Traduction par Sylvie Ségui, JDN

Paramétrer son compte whatsapp pour protéger ses données

3. Activer la validation en deux étapes

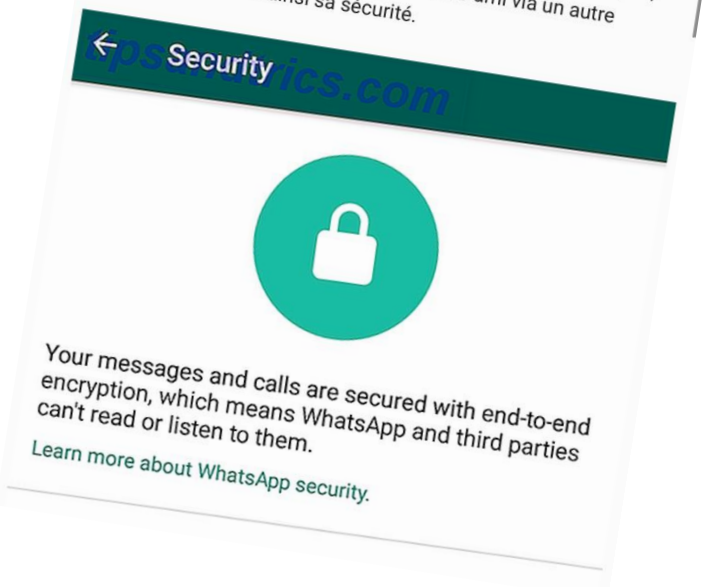
Si un service le supporte, vous devriez utiliser l'authentification à deux facteurs Vous pouvez maintenant activer la validation en deux étapes sur WhatsApp Vous pouvez maintenant activer la validation en deux étapes sur WhatsApp WhatsApp propose désormais une vérification en deux étapes à ses 1, 2 milliard d'utilisateurs dans le monde. Et nous encourageons tout le monde à l'activer dès que possible. Lire la suite (2FA). Cela ajoute un code d'accès périodique à WhatsApp, et garantit également que vos données ne sont pas accessibles par quelqu'un d'autre.

Pour activer 2FA, allez dans **Menu** > **Paramètres** > **Compte** > **Vérification en deux étapes** > **Activer** . Suivez les étapes pour créer un code PIN à six chiffres dont vous pouvez facilement vous souvenir. Surtout, ajoutez votre adresse e-mail pour récupérer ce code au cas où vous l'oublieriez.



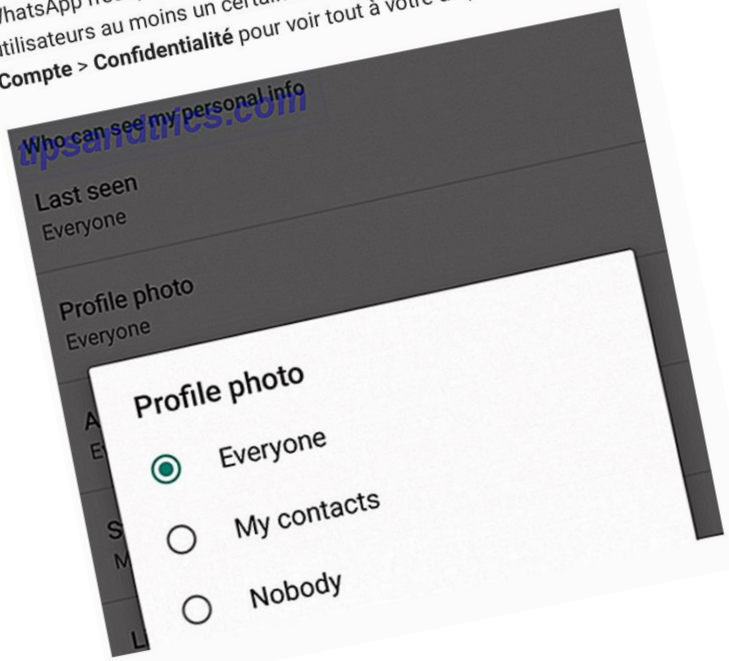
2. Activer les notifications de sécurité

Lorsqu'un nouveau téléphone ou ordinateur portable accède à une conversation existante, un nouveau code de sécurité est généré pour les deux téléphones. Et WhatsApp peut envoyer une notification lorsque le code de sécurité change. De cette façon, vous pouvez vérifier le cryptage avec votre ami via un autre messager, assurant ainsi sa sécurité.



8. Protégez votre vie privée sur WhatsApp

WhatsApp n'est pas le messager le plus privé, mais il donne aux utilisateurs au moins un certain contrôle. Allez dans **Paramètres** > **Compte** > **Confidentialité** pour voir tout à votre disposition.



Vous pouvez contrôler qui peut voir votre photo Last Last, sa photo de profil, son statut et son emplacement en direct. Vous pouvez également désactiver les confirmations de lecture ici, de sorte que les coches bleues sont désactivées.

Il n'y a pas de recommandation ici, vous pouvez choisir ce qui fonctionne le mieux pour vous. Pour en savoir plus, voici tout ce que vous devez savoir sur les paramètres de confidentialité WhatsApp Tout ce que vous devez savoir sur vos paramètres de confidentialité WhatsApp Tout ce que vous devez savoir sur vos paramètres de confidentialité WhatsApp Comme pour tous les outils de communication, la confidentialité est primordiale. Voici comment protéger votre vie privée lors de l'utilisation de WhatsApp. Lire la suite .

Travail &
Données personnelles

Les outils informatiques au travail

L'utilisation des outils informatiques s'est largement développée dans le monde du travail. Une utilisation personnelle de ces outils est tolérée si elle reste raisonnable et n'affecte pas la sécurité des réseaux ou la productivité. C'est à l'employeur de fixer les contours de cette tolérance et d'en informer ses employés.

Le contrôle de l'utilisation d'Internet et de la messagerie : dans quel but ?

L'employeur peut contrôler et limiter l'utilisation d'internet (dispositifs de filtrage de sites, détection de virus...) et de la messagerie (outils de mesure de la fréquence des envois et/ou de la taille des messages, filtres « anti-spam »...)

Ce contrôle a pour objectif :

1. D'assurer la sécurité des réseaux qui pourraient subir des attaques (virus, cheval de troie...)
2. De limiter les risques d'abus d'une utilisation trop personnelle d'internet ou de la messagerie (consultation de sa messagerie personnelle, achats de produits, de voyages, discussions sur les réseaux sociaux...).

Par défaut, les courriels ont un caractère professionnel. L'employeur peut les lire, tout comme il peut prendre connaissance des sites consultés, y compris en dehors de la présence de l'employé.

À noter

Les marque-pages, « favoris » ou « bookmark » du navigateur ne constituent pas un espace personnel ou privé. Ajouter un site internet à ses « favoris » ne limite donc pas le pouvoir de contrôle de l'employeur.

Quelles garanties pour la vie privée ?

Les limites au contrôle de l'employeur

- l'employeur ne peut pas recevoir en copie automatique tous les messages écrits ou reçus par ses employés, c'est excessif,
- les « keyloggers » permettent d'enregistrer à distance toutes les actions accomplies sur un ordinateur. Sauf circonstance exceptionnelle liée à un fort impératif de sécurité, ce mode de surveillance est illicite,
- les logs de connexion ne doivent pas être conservés plus de 6 mois.

- **La protection des courriels personnels :**

Un employé a le droit, même au travail, au respect de sa vie privée et au secret de ses correspondances privées.

Un employeur ne peut pas librement consulter les courriels personnels de ses employés, même s'il a interdit d'utiliser les outils de l'entreprise à des fins personnelles.

Pour qu'ils soient protégés, les messages personnels doivent être identifiés comme tels, par exemple :

- en précisant dans leur objet « Personnel » ou « Privé »,
- en les stockant dans un répertoire intitulé « Personnel » ou « Privé ».

Les courriers ne seront pas considérés comme personnels du simple fait de leur classement dans le répertoire « mes documents » ou dans un dossier identifié par les initiales de l'employé.

Les outils informatiques au travail

Cette protection n'existe plus si une enquête judiciaire est en cours (par exemple, si l'employé est accusé de vol de secrets de l'entreprise) ou si l'employeur a obtenu une décision d'un juge l'autorisant à accéder à ces messages.

En cas de litige, il appartient aux tribunaux d'apprécier la régularité et la proportionnalité de l'accès par l'employeur à la messagerie. L'employeur peut ainsi demander au juge de faire appel à un huissier qui pourra prendre connaissance des messages de l'employé.

- **Les fichiers**

Par défaut, les fichiers ont un caractère professionnel et l'employeur peut y accéder librement.

Lorsque les fichiers sont identifiés comme personnels, l'employeur peut y accéder :

- en présence de l'employé ou après l'avoir appelé,
- en cas de risque ou évènement particulier, qu'il appartient aux juridictions d'apprécier.

- **La communication des mots de passe**

Les identifiants et mots de passe (session Windows, messagerie...) sont confidentiels et ne doivent pas être transmis à l'employeur. Toutefois, si un employé absent détient sur son poste des informations indispensables à la poursuite de l'activité, son employeur peut exiger la communication de ses codes si l'administrateur réseau n'est pas en mesure de fournir l'accès au poste.

L'information des employés

Les instances représentatives du personnel doivent être informées ou consultées avant la mise en œuvre d'un dispositif de contrôle de l'activité.

Chaque employé doit être notamment informé :

- des finalités poursuivies,
- de la base légale du dispositif (obligation issue du code du travail par exemple, ou intérêt légitime de l'employeur),
- des destinataires des données,
- de la durée de conservation des données,
- de son droit d'opposition pour motif légitime,
- de ses droits d'accès et de rectification,
- de la possibilité d'introduire une réclamation auprès de la CNIL.

Cette information peut se faire au moyen d'une charte, annexée ou non au règlement intérieur, d'une note individuelle ou d'une note de service...

Quelle formalité

Si l'employeur a désigné un Délégué à la protection des données (DPO), il doit être associé à la mise en oeuvre des dispositifs de contrôle.

Les différents systèmes de contrôle des outils informatiques doivent être inscrits au registre des activités de traitement tenu par l'employeur.

Quels recours ?

En cas de difficulté, vous pouvez saisir :

- les services de l'inspection du Travail,
- le procureur de la République,
- le service des plaintes de la CNIL, sur les modalités de mise en œuvre d'un dispositif de contrôle de l'activité.

Textes de référence

- **Le code civil :**
  Article 9 (protection de l'intimité de la vie privée)
- **Le code du travail :**
  Article L. 1121-1 (droits et libertés dans l'entreprise)
  Article L. 1222-3 et L. 1222-4 (information des employés)
  Article L. 2323-47 (information/consultation du comité d'entreprise)
- **Le code pénal :**
  Articles 226-1 et suivants (protection de la vie privée)
- Le Règlement européen sur la protection des données personnelles (RGPD)

Pour plus d'informations, consultez la rubrique « Besoin d'aide » sur **www.cnil.fr**. Vous pouvez également appeler la permanence juridique de la CNIL au **01 53 73 22 22**, les lundi, mardi, jeudi et vendredi de 10h à 12h et de 14h à 16h.

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Édition 2018 cnil.fr