

# Politique de confidentialité - ToqueHub Mobile

Dernière mise à jour : 30 juillet 2026

Cette politique de confidentialité explique comment l'application mobile ToqueHub traite les données lorsque vous l'utilisez sur iOS ou Android.

ToqueHub Mobile est une application professionnelle destinée aux cuisines, restaurants, cuisines centrales, traiteurs, hôtels, établissements médico-sociaux, collectivités et autres organisations utilisant une instance ToqueHub locale ou self-hosted.

ToqueHub Mobile est conçu selon un principe local-first : l'application fonctionne avec le serveur ToqueHub choisi par l'utilisateur ou par l'administrateur de son établissement. Par défaut, ToqueHub Mobile n'envoie pas les données métier vers un serveur central ToqueHub.

## 1. Responsable du traitement

Pour les données traitées dans le cadre de l'utilisation réelle de ToqueHub, le responsable du traitement est généralement l'organisation qui installe, configure et exploite son serveur ToqueHub : restaurant, entreprise, collectivité, établissement ou administrateur self-hosted.

L'éditeur de ToqueHub Mobile fournit l'application et le logiciel open source, mais ne contrôle pas par défaut les données stockées ou synchronisées sur les instances locales/self-hosted exploitées par les utilisateurs.

Si vous utilisez ToqueHub dans votre établissement, adressez en priorité vos demandes relatives à vos données à l'administrateur ToqueHub ou au responsable de votre organisation.

## 2. Données pouvant être traitées

Selon les modules utilisés, ToqueHub Mobile peut traiter les catégories de données suivantes :

- données de compte et de session : identifiant utilisateur, rôle, droits, jetons d'authentification, serveur sélectionné ;
- données d'établissement : nom de l'organisation, site, cuisine, équipements, zones, emplacements ;
- données HACCP : relevés de température, contrôles, actions correctives, plans de nettoyage, validations, historiques, rapports journaliers ;
- données de traçabilité : produits, lots, dates, DLC/DDM, réceptions, productions, photos d'étiquettes, informations fournisseurs ;
- données de production et stocks : tâches de production, mouvements, produits, unités, inventaires, documents d'achat ou bons de livraison ;
- données médias : photos prises avec l'appareil photo ou importées depuis la bibliothèque lorsque l'utilisateur choisit de les ajouter ;
- données techniques locales : préférences de l'application, configuration d'imprimante, statut de synchronisation, files d'attente offline, journaux techniques nécessaires au diagnostic ;
- données de localisation approximative ou ville choisie : utilisées pour afficher la météo locale sur le tableau de bord, lorsque la fonctionnalité est activée ;
- données de notification : préférences de notification et, selon la configuration, jeton de notification push nécessaire à l'envoi d'alertes.

Toutes ces données ne sont pas forcément utilisées dans chaque installation. Les données réellement traitées dépendent des modules activés, des permissions accordées, de la configuration du serveur et de l'usage de l'établissement.

### 3. Données que ToqueHub Mobile ne collecte pas par défaut

ToqueHub Mobile ne collecte pas par défaut :

- de données publicitaires ;
- d'identifiants destinés au suivi publicitaire ;
- de données destinées au profilage marketing ;
- de contacts du carnet d'adresses ;
- de données de paiement dans l'application mobile ;
- de données de santé au sens médical, sauf si un établissement saisit volontairement des informations dans des champs libres, ce qui est déconseillé si ces informations ne sont pas nécessaires.

ToqueHub Mobile n'utilise pas les données de l'application pour suivre l'utilisateur entre des apps ou sites tiers.

### 4. Finalités du traitement

Les données sont traitées pour les finalités suivantes :

- permettre la connexion à une instance ToqueHub locale ou self-hosted ;
- enregistrer les contrôles HACCP et les opérations métier de cuisine ;
- assurer la traçabilité des produits, lots, réceptions et productions ;
- permettre le fonctionnement offline et la synchronisation différée ;
- générer des historiques, rapports, preuves de contrôle et documents internes ;
- configurer et utiliser les imprimantes compatibles ;
- afficher des informations utiles au tableau de bord, comme la météo locale ou l'état de synchronisation ;
- envoyer des rappels ou alertes liés aux contrôles ou capteurs, si les notifications sont activées ;
- sécuriser l'accès à l'application et au serveur choisi ;
- diagnostiquer les incidents techniques liés à l'utilisation de l'application.

### 5. Base juridique

Selon le contexte d'utilisation et la législation applicable, les traitements peuvent reposer sur :

- l'exécution d'un contrat ou d'une mission confiée à l'utilisateur professionnel ;
- l'intérêt légitime de l'établissement à gérer ses opérations, sa traçabilité, sa sécurité alimentaire et ses obligations internes ;
- le respect d'obligations légales ou réglementaires applicables à l'établissement, notamment en matière d'hygiène, sécurité alimentaire, traçabilité ou conservation de justificatifs ;
- le consentement de l'utilisateur lorsque la loi l'exige, par exemple pour certaines permissions facultatives ou certains services non strictement nécessaires.

L'organisation qui exploite l'instance ToqueHub doit vérifier la base juridique applicable à son propre usage.

## 6. Stockage local et fonctionnement offline

ToqueHub Mobile peut stocker des données directement sur l'appareil afin de permettre l'utilisation en cuisine même lorsque le réseau est indisponible.

Ce stockage local peut inclure :

- les données saisies dans les modules HACCP ;
- les opérations en attente de synchronisation ;
- certains paramètres de session ;
- les préférences utilisateur ;
- les informations nécessaires à la reprise de synchronisation.

Lorsque le serveur ToqueHub configuré redevient joignable, les données en attente peuvent être synchronisées automatiquement avec ce serveur.

Si l'appareil est perdu, volé ou partagé avec d'autres personnes, les données locales peuvent être exposées. L'organisation utilisatrice doit mettre en place des mesures adaptées : code de verrouillage, gestion des appareils, suppression à distance si disponible, comptes nominatifs et limitation des droits.

## 7. Serveur local ou self-hosted

En usage réel, ToqueHub Mobile communique avec l'instance ToqueHub sélectionnée par l'utilisateur ou l'administrateur.

Cette instance peut être :

- un serveur local dans l'établissement ;
- un serveur installé sur un ordinateur, NAS, Raspberry Pi ou infrastructure privée ;
- une instance accessible via un réseau privé, VPN ou hébergement choisi par l'organisation.

La sécurité, l'hébergement, les sauvegardes, les comptes utilisateurs, les durées de conservation et les éventuelles intégrations externes de cette instance relèvent de l'organisation qui l'exploite.

ToqueHub Mobile ne peut pas garantir la configuration de chaque instance self-hosted.

## 8. Mode démo

Le mode démo permet de découvrir ToqueHub Mobile sans serveur local.

En mode démo :

- les données affichées sont fictives ;
- aucune instance ToqueHub réelle n'est utilisée ;
- aucune donnée métier réelle n'est envoyée vers un serveur ToqueHub ;
- les données de démonstration peuvent être réinitialisées lorsque l'utilisateur quitte ou relance le mode démo.

Ce mode est notamment prévu pour la découverte de l'application et pour la revue App Store / Google Play.

## 9. Permissions utilisées par l'application

ToqueHub Mobile peut demander certaines permissions système. Elles sont utilisées uniquement pour les fonctionnalités correspondantes.

### Réseau local

Utilisé pour détecter les serveurs ToqueHub et les imprimantes disponibles sur le réseau Wi-Fi de l'établissement.

### Internet et état du réseau

Utilisés pour communiquer avec le serveur ToqueHub choisi, vérifier sa disponibilité et synchroniser les données.

### Bluetooth

Utilisé pour détecter ou communiquer avec des imprimantes compatibles, notamment certaines imprimantes Brother.

### Caméra

Utilisée lorsque l'utilisateur choisit de scanner ou photographier une facture, un bon de livraison, une étiquette, un lot, une production ou un justificatif.

### Photos / bibliothèque multimédia

Utilisée lorsque l'utilisateur choisit d'importer une image ou un document depuis son appareil.

### Localisation lorsque l'application est ouverte

Utilisée pour afficher une météo locale sur le tableau de bord ou proposer une ville pertinente. La localisation n'est pas utilisée à des fins publicitaires ou de suivi.

### Notifications

Utilisées pour les rappels, alertes HACCP, alertes capteurs ou informations opérationnelles, selon la configuration.

L'utilisateur peut refuser certaines permissions. Certaines fonctionnalités associées peuvent alors être indisponibles, mais l'application doit rester utilisable pour les autres modules.

## 10. Partage des données avec des tiers

ToqueHub Mobile ne vend pas les données personnelles et ne les partage pas avec des régies publicitaires.

Par défaut, les données métier sont envoyées uniquement vers le serveur ToqueHub choisi par l'utilisateur ou l'organisation.

Des tiers peuvent intervenir dans certains cas :

- Apple ou Google pour la distribution de l'application, les permissions système, les notifications ou le fonctionnement du système d'exploitation ;

- les fournisseurs d'imprimantes ou SDK d'impression lorsque l'utilisateur utilise une fonctionnalité matérielle compatible ;
- les services externes éventuellement configurés par l'administrateur dans son instance ToqueHub, par exemple OCR, sauvegarde, e-mail, stockage, météo ou intégration métier ;
- les prestataires techniques choisis par l'organisation pour héberger ou maintenir son serveur.

L'usage de ces services dépend de la configuration de chaque instance ToqueHub. L'organisation qui exploite l'instance doit informer ses utilisateurs des services tiers effectivement activés.

## 11. Transferts hors Union européenne

ToqueHub Mobile n'organise pas par défaut de transfert de données métier vers un pays situé hors de l'Union européenne.

Toutefois, des transferts peuvent exister si l'organisation choisit :

- d'héberger son serveur hors Union européenne ;
- d'utiliser des services externes hébergés hors Union européenne ;
- d'activer des intégrations tierces impliquant de tels transferts.

Dans ce cas, l'organisation responsable de l'instance doit s'assurer que les garanties légales appropriées sont mises en place.

## 12. Durée de conservation

Les données stockées localement restent sur l'appareil tant que l'application, la session ou les données locales ne sont pas supprimées.

Les données synchronisées avec une instance ToqueHub sont conservées selon les règles définies par l'organisation qui exploite cette instance.

Certaines données HACCP, de traçabilité ou de conformité peuvent devoir être conservées pendant une durée minimale en raison d'obligations réglementaires ou internes. L'organisation utilisatrice est responsable de définir et respecter ces durées.

## 13. Sécurité

ToqueHub Mobile met en oeuvre des mesures raisonnables pour limiter les risques, notamment :

- stockage local nécessaire au fonctionnement offline ;
- conservation sécurisée de certains secrets ou jetons lorsque les mécanismes du système le permettent ;
- limitation des échanges au serveur configuré par l'utilisateur ;
- permissions demandées uniquement pour les fonctionnalités concernées ;
- fonctionnement en mode démo sans serveur réel.

La sécurité globale dépend aussi fortement :

- du verrouillage de l'appareil ;

- de la gestion des comptes utilisateurs ;
- de la configuration réseau ;
- de l'usage ou non de HTTPS/VPN ;
- des sauvegardes ;
- des mises à jour du serveur et de l'application.

Aucun système ne peut garantir une sécurité absolue.

## 14. Droits des personnes

Selon la législation applicable, vous pouvez disposer de droits sur vos données personnelles, notamment :

- droit d'accès ;
- droit de rectification ;
- droit d'effacement ;
- droit d'opposition ;
- droit à la limitation du traitement ;
- droit à la portabilité ;
- droit de retirer votre consentement lorsque le traitement repose sur celui-ci.

Pour exercer ces droits dans le cadre d'une instance ToqueHub utilisée par votre établissement, contactez l'administrateur ToqueHub ou le responsable de votre organisation.

Si vous ne savez pas qui contacter, vous pouvez écrire au support ToqueHub, qui pourra vous orienter sans nécessairement avoir accès aux données de votre instance locale.

## 15. Données des collaborateurs et utilisateurs internes

ToqueHub peut être utilisé par plusieurs membres d'une équipe : chefs, cuisiniers, responsables HACCP, magasiniers, administrateurs ou autres collaborateurs.

L'organisation qui déploie ToqueHub doit informer ses collaborateurs de l'utilisation de l'application, des données traitées, des finalités, des durées de conservation et de leurs droits.

Les comptes doivent idéalement être nominatifs afin d'assurer une traçabilité correcte et d'éviter le partage d'identifiants.

## 16. Données sensibles et champs libres

ToqueHub est destiné à la gestion opérationnelle et HACCP des cuisines. Les utilisateurs ne doivent pas saisir dans les champs libres des informations inutiles ou sensibles, notamment des données médicales, opinions, informations privées sur des personnes ou données sans lien avec les finalités professionnelles de l'application.

L'organisation utilisatrice doit former ses équipes à une saisie proportionnée et pertinente.

## 17. Enfants

ToqueHub Mobile est une application professionnelle. Elle n'est pas destinée aux enfants ni au grand public mineur.

## 18. Open source et licence

ToqueHub est distribué en open source sous licence AGPL-3.0-only, sauf composants tiers soumis à leurs propres licences.

Le code source et les informations de licence peuvent être consultés à l'adresse :

<https://github.com/toquehub/toquehub>

L'utilisation open source du logiciel ne modifie pas les obligations de confidentialité et de protection des données de l'organisation qui exploite une instance ToqueHub.

## 19. Modifications de cette politique

Cette politique peut être mise à jour pour refléter les évolutions de l'application, des fonctionnalités, des obligations légales ou des pratiques de traitement.

La date de dernière mise à jour indiquée en haut du document permet d'identifier la version applicable.

## 20. Contact

Pour toute question générale sur ToqueHub Mobile :

Support : <https://toquehub.app/contact>

Politique publique à utiliser dans les stores :

<https://toquehub.app/privacy>

Pour les demandes relatives aux données d'une instance locale ou self-hosted, contactez d'abord l'administrateur de cette instance ou le responsable de votre organisation.

# Privacy Policy - ToqueHub Mobile

Last updated: July 30, 2026

This privacy policy explains how the ToqueHub Mobile app processes data when you use it on iOS or Android.

ToqueHub Mobile is a professional app for kitchens, restaurants, central kitchens, caterers, hotels, care facilities, public organizations and other organizations using a local or self-hosted ToqueHub instance.

ToqueHub Mobile follows a local-first approach: the app works with the ToqueHub server selected by the user or administrator. By default, ToqueHub Mobile does not send business data to a central ToqueHub server.

## 1. Data controller

For data processed during actual use of ToqueHub, the data controller is generally the organization that installs, configures and operates its ToqueHub server: a restaurant, company, public organization, facility or self-hosted administrator.

The publisher of ToqueHub Mobile provides the app and open-source software, but does not generally control data stored or synchronized on local or self-hosted instances operated by users.

If you use ToqueHub in your organization, contact your ToqueHub administrator or organization first for requests concerning your data.

## 2. Data that may be processed

Depending on the modules used, ToqueHub Mobile may process the following categories of data:

- account and session data: user identifier, role, permissions, authentication tokens and selected server;
- organization data: organization name, site, kitchen, equipment, zones and locations;
- HACCP data: temperature readings, checks, corrective actions, cleaning plans, validations, history and daily reports;
- traceability data: products, batches, dates, use-by or best-before dates, deliveries, production, label photos and supplier information;
- production and inventory data: production tasks, movements, products, units, inventory records, purchasing documents or delivery notes;
- media data: photos taken with the camera or imported from the library when the user chooses to add them;
- local technical data: app preferences, printer configuration, synchronization status, offline queues and technical logs needed for diagnosis;
- approximate location or selected city: used to display local weather when this feature is enabled;
- notification data: notification preferences and, depending on configuration, a push notification token needed to send alerts.

Not all of these data are used in every installation. The data actually processed depends on enabled modules, permissions, server configuration and the organization's use of the app.

### 3. Data not collected by default

ToqueHub Mobile does not collect by default:

- advertising data;
- identifiers used for advertising tracking;
- data used for marketing profiling;
- address-book contacts;
- payment data in the mobile app;
- medical health data, unless an organization voluntarily enters information in free-text fields. This is discouraged when such information is not necessary.

ToqueHub Mobile does not use app data to track users across third-party apps or websites.

### 4. Purposes of processing

Data is processed to:

- enable connection to a local or self-hosted ToqueHub instance;
- record HACCP checks and kitchen operations;
- provide traceability for products, batches, deliveries and production;
- support offline use and deferred synchronization;
- generate history, reports, control records and internal documents;
- configure and use compatible printers;
- display useful dashboard information, such as local weather or synchronization status;
- send reminders or alerts related to checks or sensors when notifications are enabled;
- secure access to the app and selected server;
- diagnose technical incidents related to app use.

### 5. Legal basis

Depending on the context and applicable law, processing may be based on:

- performance of a contract or professional assignment;
- the organization's legitimate interest in managing operations, traceability, food safety and internal obligations;
- compliance with legal or regulatory obligations, including hygiene, food safety, traceability or record-keeping requirements;
- user consent when required by law, for example for optional permissions or non-essential services.

The organization operating the ToqueHub instance must verify the appropriate legal basis for its own use.

### 6. Local storage and offline use

ToqueHub Mobile may store data directly on the device to support kitchen use when the network is unavailable.

Local storage may include HACCP entries, pending synchronization operations, session settings, user preferences and information needed to resume synchronization.

When the configured ToqueHub server becomes reachable again, pending data may be synchronized automatically with that server.

If the device is lost, stolen or shared, local data may be exposed. The organization should use appropriate safeguards, including a device passcode, device management, remote deletion where available, individual accounts and restricted permissions.

## **7. Local or self-hosted server**

During normal use, ToqueHub Mobile communicates with the ToqueHub instance selected by the user or administrator.

This instance may be a local server, a computer, NAS, Raspberry Pi or private infrastructure, or a server reached through a private network, VPN or hosting provider selected by the organization.

Security, hosting, backups, user accounts, retention periods and external integrations for that instance are managed by the organization operating it. ToqueHub Mobile cannot guarantee the configuration of each self-hosted instance.

## **8. Demo mode**

Demo mode lets users discover ToqueHub Mobile without a local server. Displayed data is fictional, no real ToqueHub instance is used, no real business data is sent to a ToqueHub server and demo data may be reset when the user exits or relaunches demo mode.

## **9. App permissions**

ToqueHub Mobile may request system permissions for the corresponding features:

### **Local network**

Used to discover ToqueHub servers and available printers on the organization's Wi-Fi network.

### **Internet and network status**

Used to communicate with the selected ToqueHub server, check availability and synchronize data.

### **Bluetooth**

Used to discover or communicate with compatible printers, including certain Brother printers.

### **Camera**

Used when the user chooses to scan or photograph an invoice, delivery note, label, batch, production record or supporting document.

### **Photos or media library**

Used when the user chooses to import an image or document from the device.

## **Location while the app is in use**

Used to display local weather or suggest a relevant city. Location is not used for advertising or tracking.

## **Notifications**

Used for reminders, HACCP alerts, sensor alerts or operational information, depending on configuration.

Users may deny optional permissions. Associated features may then be unavailable, while other app modules should remain usable.

## **10. Sharing data with third parties**

ToqueHub Mobile does not sell personal data and does not share it with advertising networks.

By default, business data is sent only to the ToqueHub server selected by the user or organization.

Third parties may be involved in limited cases, including Apple or Google for app distribution, system permissions, notifications or operating-system services; printer manufacturers or printing SDK providers when compatible hardware is used; external services configured by the administrator, such as OCR, backup, email, storage, weather or business integrations; and technical providers selected by the organization to host or maintain its server.

The use of these services depends on the configuration of each ToqueHub instance. The organization operating the instance must inform its users about the third-party services actually enabled.

## **11. Transfers outside the European Union**

ToqueHub Mobile does not by default arrange transfers of business data to countries outside the European Union.

Transfers may occur if the organization hosts its server outside the European Union or enables external services or integrations involving such transfers. The organization responsible for the instance must ensure that appropriate legal safeguards are in place.

## **12. Retention period**

Data stored locally remains on the device until the app or local data is deleted. Data synchronized with a ToqueHub instance is retained according to the rules defined by the organization operating that instance.

Some HACCP, traceability or compliance records may need to be retained for a minimum period under applicable regulations or internal rules. The organization is responsible for defining and following those periods.

## **13. Security**

ToqueHub Mobile uses reasonable measures to reduce risks, including local storage needed for offline use, secure storage of certain secrets or tokens when supported by the operating system, limiting exchanges to the server configured by the user, requesting permissions only for relevant features and providing demo mode without a real server.

Overall security also depends on device locking, user-account management, network configuration, HTTPS or VPN use, backups, and server and app updates. No system can guarantee absolute security.

## 14. Individual rights

Depending on applicable law, you may have rights over your personal data, including access, correction, deletion, objection, restriction, portability and withdrawal of consent where processing is based on consent.

For rights requests concerning an instance used by your organization, contact your ToqueHub administrator or organization. If you do not know whom to contact, you may write to ToqueHub support, which can direct you without necessarily having access to your local instance data.

## 15. Employee and internal user data

ToqueHub may be used by chefs, cooks, HACCP managers, warehouse staff, administrators and other employees. The deploying organization must inform its staff about the data processed, purposes, retention periods and rights.

Individual accounts are recommended to ensure proper traceability and avoid shared credentials.

## 16. Sensitive data and free-text fields

ToqueHub is intended for operational and HACCP management in kitchens. Users should not enter unnecessary or sensitive information in free-text fields, including medical data, opinions, private information or data unrelated to the professional purposes of the app.

The organization should train its teams to enter information that is proportionate and relevant.

## 17. Children

ToqueHub Mobile is a professional app. It is not intended for children or the general underage public.

## 18. Open source and license

ToqueHub is distributed as open-source software under the AGPL-3.0-only license, except for third-party components subject to their own licenses.

Source code and license information are available at <https://github.com/toquehub/toquehub>. Open-source distribution does not change the privacy and data-protection obligations of the organization operating a ToqueHub instance.

## 19. Changes to this policy

This policy may be updated to reflect changes to the app, features, legal requirements or processing practices. The last-updated date at the top identifies the applicable version.

## 20. Contact

For general questions about ToqueHub Mobile:

Support: <https://toquehub.app/contact>

Public policy for app stores: <https://toquehub.app/privacy>

For requests concerning data in a local or self-hosted instance, contact the instance administrator or your organization.