I. Catégories de données.

Données générées par l'utilisateur

Fichiers personnels : photographies, vidéos, documents (par exemple, PDF/Word).

Données d'application : historiques de chat, progression dans les jeux, historique des achats (applications de commerce électronique).

Données biométriques : modèles d'empreintes digitales et de reconnaissance faciale (stockés dans des puces sécurisées).

Données système et journaux

Journaux de diagnostic : rapports d'erreurs, données de performance (conservés pendant 30 à 90 jours par défaut).

Activité réseau : enregistrements de connexion Wi-Fi, cache de requêtes DNS.

Données de services tiers

Identifiant publicitaire : utilisé pour la publicité personnalisée (réinitialisable manuellement).

Données de synchronisation cloud : par exemple, événements Google Agenda.

II. État de l'appareil

État du matériel

État de la batterie : pourcentage de capacité actuel.

Espace de stockage : capacité utilisée/restante (mise à jour en temps réel via les paramètres système).

État du logiciel

Version du système d'exploitation : par exemple, Android 15.

Correctifs de sécurité : date de la dernière mise à jour (corrections de vulnérabilités critiques)..

État du réseau

Type de connexion : liste des appareils connectés au Wi-Fi 5/4G/Bluetooth.

État du VPN : activation ou non du tunnel crypté.

III. Données d'utilisation.

Analyse comportementale

Temps d'utilisation de l'écran : durée d'utilisation quotidienne par application.

Fréquence d'interaction : nombre de lancements pour les applications fréquemment utilisées.

Données de performance

Utilisation du processeur/de la mémoire : consommation des ressources par les processus en arrière-plan (visible en mode développeur).

Enregistrements de surchauffe : historique des alertes de température élevée (certains fabricants conservent les journaux pendant 7 jours).

IV. Géolocalisation

Méthodes de positionnement

GPS : positionnement extérieur haute précision (par exemple, navigation cartographique).

Wi-Fi/antennes-relais : positionnement intérieur ou au niveau de la ville (précision moindre).

Utilisation des données

Dépendance au service : les applications météo récupèrent les prévisions locales ; les applications de livraison de repas affichent les commerçants à proximité.

Risques pour la vie privée : l'historique de localisation peut être utilisé par les annonceurs à des fins de profilage (nécessite la désactivation de la fonction « Localisation précise »).

Recommandations de gestion (mise à jour 2025)

Conformité réglementaire : la loi européenne sur les marchés numériques impose la mise à disposition d'options de suppression des données de localisation.

Contrôle par l'utilisateur : suppression groupée de l'historique de localisation disponible via les paramètres (par exemple, « Chronologie » de Google Maps).

V. Méthodes d'accès aux données

Données stockées localement

Gestionnaire de fichiers : accédez aux documents, images, vidéos, etc. via l'application de gestion de fichiers intégrée au système (par exemple, l'application « Fichiers » d'Android).

Galerie/Bibliothèque de photos : visualisez directement les photos et vidéos capturées.

Données dans l'application : telles que les historiques de chat, les sauvegardes de jeux, etc., qui doivent être consultées dans l'application correspondante (par exemple, « Paramètres >

Général > Stockage »).

Données stockées dans le cloud

Services cloud du fabricant : accédez aux fichiers synchronisés via Google Drive (Android).
Applications cloud tierces.

Données dans les paramètres système

Informations sur le compte : affichez les adresses e-mail connectées, les comptes de réseaux sociaux, etc. sous « Paramètres > Comptes ».

Historique des positions : accédez-y via la « Chronologie » du compte Google (nécessite une autorisation pour être activée).

VI. Méthodes de suppression des données

Suppression des données locales

Suppression manuelle des fichiers : appuyez longuement sur le fichier dans le gestionnaire de fichiers et sélectionnez « Supprimer » ou « Déplacer vers la corbeille ».

- Effacer le cache de l'application : accédez à « Paramètres > Gestion des applications », sélectionnez l'application et appuyez sur « Effacer le cache » ou « Effacer les données » (cette dernière option réinitialisera l'application).
- Réinitialisation d'usine : efface complètement toutes les données (chemin d'accès : Paramètres > Système > Réinitialiser).

Suppression des données dans le cloud

Fichiers dans le cloud : supprimez les fichiers dans l'application du service cloud.

Déconnexion du compte : la suppression des comptes cloud de la tablette interrompt la synchronisation, mais les données cloud nécessitent une connexion séparée pour être supprimées.

Effacement spécialisé des données confidentielles

Historique du navigateur : dans Chrome, sélectionnez « Effacer les données de navigation ».

Données biométriques : les données d'empreintes digitales ou de reconnaissance faciale doivent être supprimées via « Paramètres > Sécurité ».

Précautions

Sauvegardez les données critiques : créez des sauvegardes via un ordinateur ou des services cloud avant la suppression.

Risque lié aux données résiduelles : les fichiers partiellement supprimés peuvent être récupérés à l'aide d'outils spécialisés ; la suppression définitive nécessite un écrasement du stockage ou un effacement crypté.

VII. Catégories courantes de périodes de conservation des données

.Données générées par l'utilisateur

Stockage local : conservées jusqu'à leur suppression manuelle par l'utilisateur ou la réinitialisation de l'appareil (par exemple, photos, documents).

Sauvegardes cloud : conservées automatiquement conformément aux politiques des services cloud.

Journaux système et d'application

- Données de diagnostic : Android les conserve généralement pendant plusieurs mois (elles peuvent être effacées manuellement).
- Cache d'application : certaines applications l'effacent automatiquement (par exemple, les historiques de chat sont conservés par défaut pendant 7 jours, sauf si les paramètres de sauvegarde sont activés).

Données relatives à la conformité légale

- Dossiers financiers/médicaux : conservés pendant 5 à 10 ans conformément aux exigences réglementaires (par exemple, le RGPD).
- Communications d'entreprise : certains secteurs imposent la conservation des e-mails et des enregistrements de transactions pendant 3 à 7 ans.

VIII. Facteurs clés influant sur les périodes de conservation

Capacité de stockage : les systèmes peuvent automatiquement effacer les données les plus anciennes lorsque l'espace devient insuffisant.

Paramètres utilisateur : par exemple, le dossier « Supprimés récemment » dans les albums photo conserve les éléments pendant 30 jours (durée ajustable).

Conditions d'utilisation : les services cloud tiers peuvent appliquer des règles pour effacer les données des comptes inactifs (par exemple, les comptes Google déclenchent la suppression

après deux ans d'inactivité).