

Privacy Policy — Cred Count

Version 2 · Published 4 October 2026 · Clever Little Goose LLC

CONTENTS

What this covers	2
The 30-second version	2
§1 Who we are	3
§2 Three terms this policy relies on	3
Where your information is	4
§3 What stays on your device	4
§4 Your device ID	5
§5 Your device's own backup	6
§5.1 Android backup	6
§5.2 iCloud Backup	6
§5.3 UK iOS users	6
What leaves your device	7
§6 Downloading the catalogue	7
§7 Smart Import	7
§8 Google Drive backup and Google Sheets import	8
§9 What you send us for the catalogue	9
§10 If you contact us	10
§11 The website	11
Limits and rights	11
§12 What we don't collect	11
§12.1 Crash reports from Apple and Google	12
§13 Your rights	12
Asking us for something	13
§14 How long we keep things	14
§15 Where your data goes	15
§16 Children	16
§17 Security, and telling you about a breach	16
§18 Changes	17

Cred Count Privacy Policy

Version 2

Last updated: 4 October 2026

Applies to: Cred Count for Android, for iOS (iPhone and iPad, iOS 17 and later) and for Wear OS; credcount.app; and anyone who contacts us about Cred Count, whether or not they use it.

If you're here about Clever Little Goose LLC as a company instead of Cred Count (you're a supplier, a client, or someone we're corresponding with for another reason), there's a separate privacy notice at cleverlittlegoose.com. This one is specific to Cred Count.

The 30-second version

Cred Count has no accounts and we don't know who you are. What you log is yours; collecting and selling user data isn't how we choose to make money; data we never hold can't be lost or misused.

Everything you log (your rides, ratings, notes and trips) is stored on your device (§3). We don't keep a copy, so there's nothing of yours for us to look at, and the app works without us. It also means we can't restore your logbook if you lose your device. So keep your own backup: your device's automatic backup (§5), or one of the two built into the app, a backup file or Google Drive backup (§8).

We can tell one copy of the app from another, and that's all. Each install creates a random number, its device ID. It isn't linked to your device's hardware, your Google account, your name or your email. It only reaches us when you use Smart Import or send us something for the catalogue. We use it for two things: the daily limit on Smart Import, which keeps our costs manageable, and blocking an install that's vandalising the catalogue. It tells us nothing about the person using the app, or what's in it. Privacy law counts this as personal data, so §4 explains it in more detail.

Like every website, our server sees your IP address when your device talks to it. Our logs delete it after 5 days, and server backups can hold it for up to 30 (§14).

What reaches us:

1. **Catalogue downloads** (§6). Your IP address. No device ID.
2. **Smart Import, if you use it** (§7). A sample of your spreadsheet passes through our server to Google's Gemini AI, which processes it in the European Union. Our server makes the request. Google does not receive your device ID or IP address.
3. **What you send us for the catalogue** (§9). Corrections, proposals and attractions you've added and choose to offer us, with your device ID. Name matches you confirm while importing ("BTR" is "Batman The Ride"), with no identifier at all.
4. **Emails you send us** (§10).

What goes to your own accounts, not to us:

- **Google Drive backup and Google Sheets import** (§8) run between your device and your Google account. Cred Count asks Google for two Drive permissions, neither of which can read your other files.

- **Your device's own backup** (§5). If your device backs up to iCloud or to your Google account, Cred Count is included, like your other apps. UK iOS users, please read §5.3.

Everything about you that we handle is stored and processed in Europe. Our server is in Germany, our email is in the EEA, and the AI that reads your spreadsheet runs in Google's EU region (§15).

Cred Count asks for as few permissions as it can. It has no analytics, no crash reporter and no advertising ID, and it doesn't ask for your location, contacts, microphone or camera. §12 lists what we don't collect, and how you can check.

1. Who we are

Clever Little Goose LLC is the data controller for Cred Count: the company responsible for the personal data in this policy, and the one to contact or complain to about it.

- **Registered address:** 1209 Mountain Road PI NE, Ste N, Albuquerque, NM 87110, USA
- **A limited liability company** organised in the State of New Mexico on 15 July 2026 under the Limited Liability Company Act (Chapter 53, Article 19 NMSA 1978), registration number 0008116920.
- **Registered with the UK Information Commissioner's Office** as a data controller, reference **ZC213564**. The register is public, so you can look us up at ico.org.uk. Registration is a fee every UK data controller pays, not an inspection or an endorsement. It means the regulator knows who we are, and it gives you a reference to quote if you need to complain to them (§13).
- **Privacy:** privacy@credcount.app, for anything about this policy: a request, an objection, a complaint, or a question about something written here.
- **Everything else:** support@credcount.app, for bugs, questions, or a copy of the catalogue.

We keep the two addresses separate so a privacy request is never queued behind a bug report, and so we can keep to the response times in §13.

Where Cred Count is available. Cred Count isn't currently offered in the European Economic Area, so we haven't appointed a representative in the EU under Article 27 of the EU GDPR.

Data Protection Officer. We haven't appointed one. The law requires a Data Protection Officer when an organisation's core work involves monitoring people on a large scale, or handling sensitive data such as health records on a large scale. Cred Count does neither.

This policy is written for the UK GDPR and the Data Protection Act 2018. If the law where you live gives you further rights, you have those too.

2. Three terms this policy relies on

Personal data is information about a living person (UK GDPR Art 4; Data Protection Act 2018, s.3). Your notes, your IP address and your device ID are personal data. A rollercoaster isn't. Nemesis Reborn's height, its opening date and the park it's in are facts about an attraction, not a person, so this policy and the rights in it don't cover them. Most of what our server holds is facts like these.

On-device processing means your device does the work, on data that stays on it. Counting your creds, matching a ride name, working out dispatch capacity and awarding trophies all happen on your device. Almost all of Cred Count works this way.

Server processing means data is sent to a computer someone else runs, whose operator could see what arrives.

There are two questions to ask of everything in this policy: is it about a person, and if it is, does it stay on your device or go to a server? We've built Cred Count to keep the second list short.

Where your information is

The next three sections cover everything that exists about you: what's on your device (§3), your device ID (§4), and the copy your device's own backup makes (§5).

3. What stays on your device

Cred Count keeps your data in a database in the app's private storage on your device. The operating system stops other apps from reading it, and on iOS it doesn't appear in the Files app. We don't have a copy of it, and we have no way to see or search it.

- **Your logs:** every ride, with the date, time, rating, row, seat and train.
- **Your notes**, including personal ones. We never receive them. The only way a note can leave your device is inside a spreadsheet you choose to use for Smart Import (§7).
- **Your trips, visits and days**, what you've written about them, and the To Scale comparisons beside them.
- **Your measurements:** dispatch timings, train counts and capacity, including a timing in progress.
- **The trophies you've earned.**
- **Your own listings:** parks and attractions you've added yourself because our catalogue didn't have them, with your private descriptions of them. They stay on your device unless you offer one to us (§9), and the private description is never sent.
- **Things you've deleted.** The app marks them as deleted instead of erasing them straight away, so a mistake can be undone. After six months, the app erases them completely.
- **Imports:** rows still waiting to be matched to the catalogue, and an import you haven't finished.
- **The names you've taught the importer**, such as "BTR" for "Batman The Ride".
- **The corrections and suggestions you've sent us**, with your comments and whether we've reviewed them.
- **Your Google sign-in tokens, only if you use Google Drive backup.** They're kept in your device's secure store (the Keychain on iOS, Keystore-backed storage on Android), aren't synced to iCloud Keychain or included in your device's backup, and are deleted when you unlink. Importing a Google Sheet stores no token at all (§8).

On an iPhone or iPad, unlink before you uninstall. iOS keeps an app's Keychain entries after the app is deleted. Cred Count clears them when it's installed fresh, but a reinstall restored from a backup can still find the old tokens. Unlinking (Logbook → Tools → Google Drive Backup → Unlink Google Drive) revokes and deletes them. You can also cut the connection from your Google account at any

time, with or without the app: **drive.google.com/drive/settings** → **Manage apps** → **Cred Count** → **Disconnect from Drive**.

- **The email address of the Google account you connected**, so the app can show which account your backups go to (Logbook → Tools → Google Account). It stays on your device. We aren't sent a copy, and we can't read it.
- **Watch data, on Android.** The Wear OS app gets your catalogue and logs from your phone through Google Play services, the standard link between an Android device and its watch. We have no watch server. There's no Apple Watch app.
- **Your device ID** (§4).

Only you can see any of this, with one exception you control: **what you've logged today can appear on your Home Screen and Lock Screen**. The widgets, the Live Activity on an iPhone and the park-day notification on Android show the park you're at, your count for the day and your latest ride, so anyone who can see your lock screen can see those too. To turn this off, switch off **Today on the Lock Screen** in Settings, or remove the widgets.

Sharing. The share button turns your stats into an image. It's made on your device and it only goes where you send it, whether that's your photo library, or an app you choose from your device's share sheet. We don't receive a copy.

4. Your device ID

What it is. A random number the app creates the first time it runs. It isn't based on your hardware, phone number, SIM, or Google account and it can't be turned back into any of them. It also isn't an advertising ID.

Why we treat it as personal data. It links your requests to each other over time, so it identifies an install even though it doesn't identify you. The law treats identifiers like this as personal data (UK GDPR Art 4(1); Recitals 26 and 30).

When it leaves your device. Only with Smart Import (§7), and with corrections, proposals and listings you offer us (§9). Catalogue downloads (§6) and name matches don't carry it. It stops at our server: we don't pass it to Google or anyone else.

What we keep with it:

- **Smart Import's daily limit:** a record of each import with your device ID and IP address, deleted after **48 hours** by a sweep that runs once a day, so within 3 days at most. The IP address stops a reinstall from resetting the limit.
- **Your catalogue submissions** (§9), so we can spot anyone deliberately corrupting the catalogue, and find your submissions if you ask us to delete them.
- **A block list, if it's ever needed.** If an install is vandalising the catalogue or abusing Smart Import, we can refuse further submissions from its device ID. A person makes that decision, not an automated system. A block lasts until we lift it. If you think we've blocked you by mistake, please tell us (§13).

Device ID is not attached to your logs, notes, trips or anything else on your device.

How long it lasts. Uninstalling Cred Count deletes it. If your device restores Cred Count from a backup (§5), the same ID comes back. A fresh install with nothing to restore creates a new, unrelated ID.

Lawful basis: legitimate interests (UK GDPR Art 6(1)(f)): keeping the server running, keeping costs under control, and protecting the catalogue from vandalism. We don't think this overrides your interests, because the ID says nothing about who you are, and it's what lets us act on a deletion request. **You can object** (§13).

Do you have to provide it? No law or contract requires it. The app creates the ID either way, but it only leaves your device if you use Smart Import or send us something for the catalogue. If you never do, the rest of Cred Count works exactly the same.

Finding yours. **Settings** → **App Info** → **Device ID**, then tap to copy it. Send it to privacy@credcount.app and we'll delete every record that holds it. §13 explains what that covers and its limits.

5. Your device's own backup

Android and iOS can back up your apps to your Google or Apple account, so a new device can be set up like the old one. If that's switched on it means Cred Count's data is included: your logs, notes, trips and everything else in §3.

This is the largest copy of your data anywhere and we're not involved in it. We can turn this setting off, but we haven't opted out on either platform, because losing a device shouldn't mean losing your logbook. This backup is between you and Apple, or Google. We don't create it, can't read or delete it, we aren't told about it, and couldn't hand over a copy if we were asked to.

Restoring from either backup brings your device ID back too (§4).

5.1 Android backup

Android's backup doesn't count towards your Google Drive storage, it keeps only the latest copy, and on Android 9 and later that backup is encrypted with your screen lock, so Google can't read it.

To turn it off or delete it: **Settings** → **Google** → **Backup**.

5.2 iCloud Backup

To turn it off or delete it: **Settings** → **[your name]** → **iCloud** → **Manage Account Storage** → **Backups**, choose the device, then either switch Cred Count off or delete the whole backup. Switching Cred Count off also deletes what's already been backed up for it.

5.3 UK iOS users

Apple offers a setting called **Advanced Data Protection**, which encrypts iCloud backups so that only your devices can read them, not Apple. **Apple withdrew it from the UK in February 2025**, after the Home Office served a notice under the Investigatory Powers Act 2016 requiring access. UK users who hadn't already switched it on can't do so now, and device backups are among the data affected. You can see this on your device: **Settings** → **[your name]** → **iCloud** → **Advanced Data Protection**.

If you're in the UK and your iPhone or iPad backs up to iCloud, your Cred Count data is in a backup which Apple holds a key to and could be required to open. It's still encrypted on the way to Apple and on Apple's servers. This applies to every app included in your iCloud Backup, not just Cred Count. Unfortunately, we can't change it.

If that concerns you, you can switch Cred Count off in your iCloud backup list (§5.2) and keep your own copy instead: **Logbook** → **Tools** → **Backup File**, or Drive backup (§8).

This section is correct on the date at the top of this policy. The Home Office's notice has been challenged, and the position may change, so the setting on your device is the best guide.

What leaves your device

Sections 6 to 11 cover each way information moves between your device and us, or between your device and your own Google account: what's sent, who holds it, and for how long.

6. Downloading the catalogue

What happens. The app downloads our catalogue of parks and attractions from `api.credcount.app`, and checks it for updates from time to time.

What we receive. Your IP address and the time, as any web server does, and a user agent: a generic label naming the software library that made the request. It doesn't name your device or your version of the app. No device ID, and nothing about you or your logbook.

Where. Our server is with **Hetzner, in Germany**, under a data processing agreement. Hetzner also runs our DNS (§11).

Retention. Request logs are kept for **5 days**, then deleted automatically. Server backups hold copies for up to 30 days (§14).

Rate limiting. So that one script can't slow things down for everyone, the server limits how many requests each IP address can make per minute. It counts in memory and doesn't write the addresses down.

Lawful basis: legitimate interests (Art 6(1)(f)): running a server that stays up and can be protected from abuse. **You can object** (§13).

7. Smart Import

Smart Import reads a spreadsheet of your past logs and works out which column is which. It's the one feature that sends your own content to an AI service, so this section goes into detail. If you don't use Smart Import, none of it applies to you.

What's sent. A sample of your spreadsheet: the **first 100 rows, up to 4,000 characters**, with one sample per sheet if the file has several. It goes to our server, which asks **Google's Gemini AI** how the spreadsheet is laid out.

The sample includes every column. We don't filter it. To leave out a notes column we'd first have to recognise it, and a filter that guessed wrong would quietly break imports. If the first 100 rows include notes you don't want sent, delete that column before importing, or don't use Smart Import.

What Google receives. The sample and nothing else. **No device ID and no IP address.** Our server makes the request, so Google sees our server in Germany, not your device and nothing says who the sample came from. Your device ID stops at our server, where it counts towards the daily limit (§4).

Who processes it, and where. Google, as our processor, on the Gemini Enterprise Agent Platform's **European Union multi-region endpoint** (`gemini-3.5-flash-lite`). Google publishes a commitment that processing on that endpoint happens inside the EU (§15).

Training. Google's Service Specific Terms don't allow Google to use our data to train or fine-tune AI models without our permission or instruction. We haven't given either.

What we keep. For the daily limit we record each request: your device ID and IP address, the sample's size, and whether it worked (§4).

What we don't keep. The sample. It isn't written to our database or our logs.

What Google keeps. Nothing, unless its safety systems flag the request. We've checked each way the platform can keep data against how we use it:

- **Logging requests to a database** is an opt-in feature. It has never been set up on our project.
- **Stored conversations** don't apply. Each request stands alone.
- **Search and Maps grounding** keep data of their own. We use neither.
- **In-memory caching**, which Google switches on by default and which can hold inputs for up to 24 hours, is switched off on our project.

The safety check. Google runs automated checks for misuse of its AI. If one flags a request, the request may be kept for up to **90 days** so a person can review it. It's stored in the same EU region and isn't used for training. This only applies to flagged requests, and anything kept is spreadsheet text with nothing attached to identify you.

Lawful basis: your consent (UK GDPR Art 6(1)(a)). Nothing is sent until you choose a file and tap the button, the app tells you what will be sent before you do, and the rest of the app works without it. To withdraw consent, stop using it. We keep nothing that would need deleting.

Not automated decision-making. The AI reads how a spreadsheet is laid out. It doesn't make decisions about you.

8. Google Drive backup and Google Sheets import

What happens. If you switch them on, Cred Count can back up to **your own** Google Drive, and import a Google Sheet you choose.

We're not in the middle. Both run directly between your device and your Google account. Nothing passes through our server, and we don't see the file or your Google sign-in. Your agreement about that data is with Google.

What's in the backup. One file, `cred_count_backup.json`, which holds your logs and measurements, notes, trips and their days, what you've written about your visits and trips, the To Scale comparisons, your trophies, rows from imports that aren't yet matched to the catalogue, and the parks and attractions you've added yourself, with your private descriptions. Your own listings are included so that a restore doesn't leave logs pointing at attractions that no longer exist. The file is stored in Drive's hidden app folder, which only Cred Count can see and which doesn't appear in your Drive. Up to **5 dated copies** are kept beside it, and older ones are deleted automatically. The file's source is labelled "Android Device" or "iPhone", which doesn't identify your device.

What Google asks you to allow. Two Drive permissions, which Google classes as *non-sensitive*, its lowest tier, because neither can see your other files:

- `drive.appdata`, for backup: access to Cred Count's own hidden folder, and nothing else.
- `drive.file`, for importing: access to the one file you pick, and nothing else.

Switching on backup also signs you in with Google, which gives the app your basic Google profile, including your email address, so it can show which account your backups go to (§3). That stays on your device.

Picking a sheet. Google's own file picker shows you your files, on Google's side, and hands back only the one you choose. That's why Cred Count never needs permission to list what's in your Drive. On iOS the picker opens in a secure browser window over the app, after iOS asks whether Cred Count may use google.com to sign in; on Android, Google Play services shows it. The import keeps no permission once it's done. Importing a file through your device's own file browser doesn't involve Google at all.

Backup and import are separate. Unlinking backup doesn't stop you importing, and an import keeps no access that would need unlinking.

Google's code in the app. Backup and the sheet picker rely on Google's code, which ships inside Cred Count. On iOS, we use Google's sign-in library and the libraries it depends on. On Android, it's Google's client libraries, which work through Google Play services. This code only runs when you use one of those two features, and it talks only to Google, not to us.

Deleting your backup. From your Google account: drive.google.com/drive/settings → **Manage apps** → **Cred Count**. **Delete hidden app data** deletes the backup, and **Disconnect from Drive** removes Cred Count's access. This works on Android and iOS, and after you've uninstalled.

Unlinking inside Cred Count revokes access and deletes the token from your device, but leaves the backup in your Drive. The app has no button that deletes files from your Google account.

Lawful basis: your consent. Both are off until you switch them on, and unlinking withdraws consent.

9. What you send us for the catalogue

There are three kinds. Each is sent only because of something you've done, and two of them carry your device ID (§4).

A. Name matches. When you confirm during an import that "BTR" is "Batman The Ride", the match is sent to us when the import finishes, so imports work better for everyone. It carries no identifier. Like any request it arrives with an IP address, which only our request log keeps (§6). We receive the name you typed, the catalogue entry it points to, and a count of how many times the same match has been sent. We can't tell which matches came from you, which is also why we can't find them to delete (§13). Matches to parks or attractions you've added yourself are never sent.

B. Corrections and proposals. When you tap **Something wrong or missing?** on a park or attraction and send your changes for review, we receive the changes, any link you give as a source, your device ID, and anything you write under **How do you know?**, exactly as you typed it. Most of this is facts about attractions, not people. If you put your name in a comment, though, we'll have it and we'd rather we didn't. Please keep comments to the attraction.

C. Offering us your own listings. If you've added a park or attraction we don't have, you can offer it to us. It's never sent automatically. The app asks **Suggest for the catalogue?** when you add one, lists them in Explore under **Send Them to Us**, and offers them at the end of a spreadsheet import, where every box starts unticked. Whichever route you use, nothing is sent until you choose to send it.

We receive the details you've filled in about it (its name and type, its park or country, and facts such as its manufacturer, height or opening date), with your device ID. We don't receive your private description,

when you rode it, your rating, your notes or your trips. Whatever we decide, your own listing stays exactly as it is on your device.

Lawful basis for all three: legitimate interests (Art 6(1)(f)): an accurate shared catalogue, protected from vandalism. We don't think this overrides your interests, because these are about attractions, not about you. With C, you also choose to send each one.

Retention:

- **Accepted catalogue facts** are kept indefinitely. They're facts about attractions, not personal data.
- **Your device ID and comment** are erased **90 days** after we accept or reject a submission, or **12 months** after you sent it if we haven't decided by then. The rest of the submission is kept as the record of a catalogue change.

10. If you contact us

This section covers anyone who writes to us about Cred Count, whether or not you use it: users, contributors, journalists, parks, and anyone making a complaint or a legal claim. It also covers writing to us to use your rights (§13).

What we receive. Your email address, your name if you include it, your message and any attachments, and whatever's in your email signature, such as your job title or phone number.

Our phone number. Apple requires a phone number in an app's licence agreement, so ours appears on our App Store listing and in the copy of our Terms inside the app. We use a voicemail system. If you leave a message, we receive the recording, the number you called from and the date and time. Calls aren't recorded; the only recording is a message you choose to leave. Recordings are deleted automatically after **7 days**. If a message needs acting on, our reply and any notes are kept like any other email. Email is the quicker way to reach us.

What we do with it. Reply to you, and keep a record of the conversation. We don't add you to a mailing list or use your details for marketing.

Who processes it. **Zoho**, our email and voicemail provider, as our processor under a data processing agreement. Both are stored in Zoho's **European data centre**, so your message doesn't leave the EEA to reach us.

Lawful basis:

- **Correspondence:** legitimate interests (Art 6(1)(f)): replying to people who contact us.
- **If we have, or are discussing, an agreement with you about Cred Count:** taking steps at your request before entering into a contract, and carrying it out (Art 6(1)(b)).
- **Legal claims:** legitimate interests: keeping what we need to establish or defend a legal claim.

Retention:

- **Voicemail recordings:** **7 days**, then deleted automatically.
- **General correspondence and support:** **24 months** from the last message in the conversation.
- **Business and contractual records:** **6 years** from the end of the relationship, the limitation period for a contract claim in England and Wales (Limitation Act 1980, s.5).

- **Anything connected to an actual or threatened legal claim:** until the claim is resolved and the limitation period has passed. The right to erasure doesn't override this (UK GDPR Art 17(3)(e)).

11. The website

`credcount.app` is a static site. It sets **no cookies**, runs **no analytics**, and loads **nothing from other companies**: its fonts and everything else come from our own server. You can check this in your browser's developer tools. The server keeps standard logs (IP address, user agent and time) for **7 days**, then deletes them. There's no cookie banner because there's nothing to agree to.

DNS. Before your device can reach `credcount.app`, it has to look up where the site is. That's DNS, and our DNS is run by **Hetzner**, in Germany, under the same agreement as our server. You can check where our three nameservers are by looking up the addresses behind `hydrogen.ns.hetzner.com`, `oxygen.ns.hetzner.com` and `helium.ns.hetzner.de`.

Your device doesn't usually ask our nameservers directly. It asks a DNS resolver, normally your internet provider's, or one such as Google's or Cloudflare's, and that resolver asks ours. Our nameservers see the resolver, not you. Some resolvers pass on part of your network address, a range of about 250 addresses, to get a nearby answer.

We don't receive any of this. Hetzner doesn't give us DNS query logs, and we can't request them. Anything Hetzner keeps is held in Germany under our agreement with them (§15).

Limits and rights

What we don't collect (§12), your rights (§13), how long everything is kept (§14), where it's processed (§15), and the rest.

12. What we don't collect

Each of these can be checked.

1. **No analytics.** No Firebase, Google Analytics, Sentry, Mixpanel or anything like them. They aren't switched off; they aren't in the app. We don't know which screens you open, how long you spend in the app, or how many creds you have.
2. **No crash reporter in the app.** Apple and Google may share crash reports with us, if you've allowed it on your device (§12.1).
3. **No location.** Neither Android app declares a location permission, and the iOS app has no location key in its `Info.plist`, so the app can't ask for your location.
4. **No advertising IDs and no tracking.** No AAID or IDFA, no ads, and no ad networks. On iOS, every app ships a **privacy manifest** declaring what it collects and whether it tracks you. Cred Count's says `NSPrivacyTracking: false`, lists no tracking domains and no collected data, and declares one thing: that the app reads and writes its own preferences file, where the device ID (§4) is kept. You'll never see a prompt asking to let Cred Count track you.
5. **No account.** No sign-up, email or password, so there's no account to delete. Google sign-in is for your own Drive and isn't an account with us. If you email us, we'll have your email address (§10).

6. **No contacts, microphone or camera, and no access to your photos.** The only photo permission lets the app add an image you choose to save, such as a share card. It can't see what's already in your library. On Android 10 and later, saving an image needs no permission at all. When you import a file, your device gives the app only the file you picked.
7. **No special category data.** We don't collect health, biometric or political data.
8. **One identifier.** The device ID in §4, a random number the app creates. Nothing taken from your hardware, Google account, SIM or advertising ID.
9. **No selling or sharing of data.** No data brokers and no "partners".

Permissions on Android. Cred Count declares two permissions: internet access, and showing notifications, which it asks you for so it can show the park-day notification. The Wear OS app declares two: showing notifications, and keeping the watch awake. The standard libraries the app is built on add a few more: checking whether you're online, reading a file you pick, the fingerprint or face check that protects the secure store where your Google tokens are kept, and, on Android 9 and earlier, saving an image to your device's storage. Apart from notifications, you'd only see a prompt for storage, on older versions of Android. None of them collect anything.

Permissions on iOS. iOS asks you the first time an app tries to use something sensitive, and an app can only ask if it has declared a reason. Cred Count declares one: adding an image to your photo library when you save a share card. It declares nothing for location, camera, microphone, contacts or tracking, so iOS can't show those prompts. iOS also shows two prompts of its own: when you connect Google, it asks whether Cred Count may use google.com to sign in, and it may ask whether to allow Cred Count's Live Activity. The file picker, the network check, the Keychain and the share sheet need no permission.

Both lists are in the app package, if you want to check them.

12.1 Crash reports from Apple and Google

The app itself reports nothing. Your device is a different matter.

Apple and Google collect crash reports themselves, under their own terms, if you've allowed it: *Share With App Developers* on iOS (Settings → Privacy & Security → Analytics & Improvements), or *Usage & diagnostics* on Android. If you have, and Cred Count crashes, they show us a report: the app version, your device model and operating system version, and where in the code it failed. It doesn't include your logbook or your name, and we can't tell whose device it came from. If you haven't allowed it, we receive nothing.

What we do with it. Fix the bug. We don't build anything from reports or pass them on.

Lawful basis: legitimate interests (Art 6(1)(f)): finding out why our app stopped working, on a device whose owner chose to share that.

Retention. Any copy we download is deleted once the bug is fixed and the affected build is no longer in use. Apple and Google keep their own copies under their own terms.

13. Your rights

Under the UK GDPR you have the right to access your data, correct it, delete it, restrict how it's used, take a copy with you, object to how it's used, and withdraw your consent. Because nearly everything is on your device, you can do most of this yourself, in the app.

Your right to object

You can object at any time to anything we do on the basis of legitimate interests: the catalogue download (§6), the device ID (§4), catalogue submissions (§9) and correspondence (§10). Email privacy@credcount.app. You don't have to give a reason, and we'll stop unless we have compelling grounds that override your rights.

Access and portability. **Logbook** → **Tools**, under **Take Them Out**: a **Backup File** (JSON), a **Spreadsheet of Your Logs** (CSV), or a **Spreadsheet of Your Creds** (CSV). No request, no waiting and no ID check.

Correcting your data. Edit any log, date or rating in the app. For a mistake in the catalogue, tap **Something wrong or missing?** on the park or attraction.

Deleting your data.

- **On your device:** delete logs in the app, or uninstall Cred Count, which deletes the app's private storage and the database with it. On an iPhone or iPad, unlink Drive backup first if you use it (§3).
- **In your device's own backup:** §5 explains how to remove Cred Count from an iCloud or Android backup.
- **In your Google Drive:** drive.google.com/drive/settings → **Manage apps** → **Cred Count**, which deletes the backup and disconnects the app, on Android or iOS, even after you've uninstalled (§8).
- **On our server:** send us your device ID (**Settings** → **App Info** → **Device ID**) at privacy@credcount.app. We'll delete every correction, proposal and listing sent from your install, and any other record holding the ID.
There are three limits. **Name matches can't be included**, because they carry no identifier (§9), so nothing links them to you. **Accepted catalogue facts stay**: "this attraction is 62m tall" isn't about you, and other people's imports rely on it, but we'll delete your submission and your comment. **If you uninstall without a backup, your device ID is gone**, and without it we can't find your records, so copy it before you uninstall. The law doesn't require us to identify you by other means when we can't (UK GDPR Art 11).

Restricting how your data is used. Email us your device ID and we'll restrict anything attached to it.

Withdrawing consent. Unlink Drive backup in Logbook → Tools, or stop using Smart Import. Importing a sheet keeps no permission, so there's nothing to withdraw (§8). Withdrawing stops what happens next; it doesn't make earlier imports unlawful. There's little to undo anyway: we don't keep anything from Smart Import, and your Google Drive backup is in your own account.

Asking us for something

For anything on our server, an objection, a restriction, or a question about this policy, email privacy@credcount.app.

Writing to us means giving us your email address, which we otherwise wouldn't have. We handle it as §10 describes, and you can ask us to delete it once your request is dealt with.

What we need. For anything on our server, your device ID (Settings → App Info → Device ID). It's the only thing that links a request to our records.

We don't ask for proof of identity. There's no account to protect and nothing we could check a passport against, so asking for one would mean collecting more about you than your request concerns. Your device ID is enough.

How long we take. We reply **within one month**. If a request is complex we can take up to two more months; if we do, we're required to tell you within the first month and explain why. **There's no charge.** We can only refuse a request if it's clearly unfounded or excessive, or if the law says the right doesn't apply. If we refuse, we'll tell you why and what you can do about it.

Complaining. You can complain to the **Information Commissioner's Office**: ico.org.uk, 0303 123 1113. We're on their register as **Clever Little Goose LLC**, reference **ZC213564** (§1). If you're outside the UK, you can complain to your own country's data protection authority. We'd appreciate the chance to put things right first, but you don't need to come to us before going to a regulator.

14. How long we keep things

What	Where	How long
Your logbook (logs, notes, trips, measurements, trophies, your own listings)	Your device only	Until you delete it. We hold no copy
Your device ID	Your device	Until you uninstall (see §5 on device backups)
Android backup copy	Your Google account	Until you delete it. We have no access
iCloud Backup copy	Your Apple account	Until you delete it. We have no access. UK iOS users: see §5.3
Google sign-in tokens, Drive backup only	Your device's secure store	Until you unlink. On iOS, unlink before uninstalling (§3)
Google permission for importing a sheet	Not kept	Granted for each import, then discarded (§8)
Drive backup and up to 5 dated copies	Your Google account	Until you delete it. Copies beyond 5 are deleted automatically
Server request logs (IP address, user agent)	Hetzner, Germany	5 days, then deleted automatically
Device ID and IP address, Smart Import daily limit	Hetzner, Germany	48 hours, removed by a daily sweep, so within 3 days
Device ID, block list	Hetzner, Germany	Until the block is lifted
Website server logs	Hetzner, Germany	7 days, then deleted automatically
Crash reports Apple or Google show us	Apple and Google, under their terms; a copy on our computer while a bug is open	Until the bug is fixed and the build retired (§12.1)
DNS lookups for <code>credcount.app</code>	Hetzner, Germany. We don't receive them	Not ours to keep (§11)
Smart Import sample, our side	Not stored	Processed and discarded

What	Where	How long
Smart Import sample, Google's side	Google, EU multi-region	Not kept, unless flagged by an automated safety check; then up to 90 days, in the EU, for review only (§7)
Name matches you teach the importer	Hetzner, Germany	Indefinitely. No identifier attached
Accepted catalogue facts	Hetzner, Germany	Indefinitely. Not personal data
Device ID and comment on a submission	Hetzner, Germany	Erased 90 days after we accept or reject it, or 12 months after you sent it, whichever comes first
Server backups	Hetzner, Germany, on the same server	30 days, then deleted automatically. See below
Voicemail you leave on our number	Zoho Voice, EU data centre	7 days, then deleted automatically. Calls are never recorded (§10)
Correspondence, support, and privacy requests	Zoho, EU data centre	24 months from the last message, including our record of how we handled a request
Business and contractual records	Zoho, EU data centre	6 years from the end of the relationship
Anything connected to a legal claim	Zoho, EU data centre	Until it's resolved and the limitation period has passed

Server backups. The server is backed up every night so it can be rebuilt if it fails, and each backup is deleted after 30 days. That's shorter than the 90 days a submission's device ID and comment are kept, so a backup never holds those longer than the table says. A backup copies the whole server, so two things in it are kept longer than usual: **server request logs** (normally 5 days) and **Smart Import's daily-limit records** (normally 3 days at most). In a backup, each lasts up to 30 days.

15. Where your data goes

- **Our server:** Hetzner, Germany, in the EU, under a data processing agreement.
- **Our DNS:** Hetzner, Germany, under the same agreement (§11).
- **Gemini AI (Smart Import only):** Google, on its **European Union multi-region**, processed in the EU, under Google's Cloud Data Processing Addendum (§7).
- **Email and voicemail:** Zoho, on its European data centre, stored in the EEA, under a data processing agreement with **Zoho Corporation Limited**, a UK company. Our phone number is a Zoho Voice number, and its voicemail is stored in the same place as our email (§10), so a US dialling code doesn't mean a US server.
- **Your Drive backup, Google Sheets and Android backup:** your own Google account, under your agreement with Google. We're not involved.
- **Your iCloud Backup:** your own Apple account, under your agreement with Apple. Apple isn't our processor, and we send nothing to Apple and receive nothing from it about your data. §5.3 covers what UK users should know.

Everything about you that we hold or send anywhere is processed in Europe. None of it goes to a server in the United States, and no feature changes that.

Hetzner's agreement requires it. Clause 3(1) of our agreement with Hetzner commits them to processing "*exclusively in a member state of the European Union or in another member state party to the Agreement on the European Economic Area.*" Hetzner's published list of subcontractors includes companies in the United States and Singapore; those serve customers who choose servers in those countries. Ours is in Germany.

No transfer safeguards are needed. The UK recognises the EEA as giving data adequate protection, and none of this data leaves Europe.

You can check these. Google publishes which regions process what, per model, in its Agent Platform data residency documentation, and its Cloud Data Processing Addendum is at cloud.google.com/terms/data-processing-addendum. Zoho publishes its data processing agreement and sub-processors at zoho.com. Hetzner publishes its data processing agreement and subcontractors at hetzner.com. If you'd like any of these as a document instead of a link, email us.

Our New Mexico registration. Clever Little Goose LLC is registered in New Mexico. That doesn't change where your data is, and it doesn't put us outside UK data protection law: we're registered with the ICO (§1), and you can enforce the rights in §13 through a UK regulator. If anyone asked us for your ride history, we couldn't provide it. We don't have it.

16. Children

Cred Count isn't aimed at children under 13, and we don't knowingly collect their data. There's no account to create and no profile to build, and almost nothing is collected from anyone.

Smart Import is the exception to keep in mind. It relies on consent (§7), and in the UK a child under 13 can't give that consent for themselves. If you're under 13, ask a parent before using Smart Import. Nothing else in the app sends anything that needs asking about. Parents: if you think your child has imported a spreadsheet with something personal in it, email us (§13). We don't keep the sample, so there's unlikely to be anything to delete, but you're entitled to ask.

17. Security, and telling you about a breach

Everything between your device and our server travels over an encrypted connection (HTTPS), as does everything between your device and Google. On iOS the app makes no exceptions to Apple's secure-connection rules, so the operating system enforces this. Your data sits in Cred Count's private storage, which Android and iOS stop other apps reading, and which is encrypted while your device is locked. Your Google sign-in tokens are held in your device's secure store (§3). Our server is behind a firewall. Its database dashboard can only be reached over a private network, its hosting control panel needs a second sign-in step, and our AI keys never leave it.

If a breach put you at real risk, we'd have to tell you, and we have no way to contact you individually. There's no account and no email address. So we'd do what the law allows when individual contact isn't possible: publish a notice on credcount.app and in the app, saying what happened and what to do. Where the rules require it, we'd report the breach to the ICO within 72 hours.

We don't hold your logs, notes, trips or ratings, so a breach of our server couldn't expose them. What we do hold is IP addresses, device IDs, comments on catalogue submissions, and emails people have sent us.

18. Changes

When this policy changes, we publish a new version with a new date, and a page explaining what changed. Earlier versions stay readable at credcount.app/versions.

Questions, disagreements, or something we've got wrong: privacy@credcount.app.