Privacy Policy — Cred Count

Version 1 · Published 4 August 2026 · Clever Little Goose LLC

CONTENTS

Cred Count — Privacy Policy

Version 1
Last updated: 4 August 2026
Applies to: Cred Count for Android, for iOS (iPhone and iPad, iOS 15 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 rather than about Cred Count — you're a supplier, a client, or someone we're corresponding with for another reason — that's a separate notice, at cleverlittlegoose.com. This one is about the app.

The 30-second version

You don't have an account. We don't know who you are. We have no way to find out, and we've kept it that way deliberately.

Everything you log — rides, ratings, notes, trips — lives in a database on your phone (§3). There's no copy on our servers. There is no "your data" for us to look at, because we never receive it. If we vanished tomorrow, your app would keep working.

We give your install one random number, and that's the only thing we know about you. It's called a device ID. It isn't your name, your email, your Google account, or anything your phone already had. We generate it ourselves, it means nothing outside Cred Count, and it does two jobs: stopping any single install from running up an AI bill that would sink a free app, and letting us block one that's deliberately vandalising the catalogue. No account, no email, no advertising ID, no profile. It doesn't follow you anywhere.

We're calling it an identifier rather than "anonymous", because that's what it is. Anything that connects Monday's request to Tuesday's isn't anonymous. **§4 is about nothing else** — what it's attached to, how long it lives, and how to make us delete what it's attached to.

When your phone talks to our server we also see its IP address — every website does, it's how the internet delivers a file — and we bin it after 5 days.

Three things leave your phone, and only when something makes them:

1. **Your phone downloads the coaster catalogue from us** (§6). We see your IP, briefly. Not your device ID — the catalogue doesn't carry one.
2. **If you use Smart Import, part of your spreadsheet goes to Google's Gemini AI via our server** (§7). This is the one place your own typing leaves your device, and it has a section to itself because it deserves one.
3. **If you turn on Drive backup or import a Google Sheet, data moves between your phone and your own Google account** (§8). We're not in the middle and never see the file.

There's a fourth, but only if you tap it: if you've added rides we don't have in our catalogue, we'll ask — once, per ride, with every box unticked — whether you'd like to tell us they exist (§9).

One thing goes somewhere without touching us at all: your phone's own backup. If you back up your iPhone to iCloud, or your Android phone to your Google account, your Cred Count vault is in that backup — it's your phone backing up your apps to your account, and we're not a party to it. **§5**

is about that, including a specific and unwelcome wrinkle for **UK iPhone users** (§5.3) that is Apple's and the UK government's doing rather than ours.

No analytics. No crash reporting. No ad IDs. No location — the app never asks for it, on iPhone, on Android, or on the watch. No contacts, no microphone, no camera. §12 is the whole list, and every item on it is checkable.

---

1. Who we are

Clever Little Goose LLC is the **data controller** — responsible for the small amount of personal data described here, and the people you complain to.

- **Registered address:** 1209 Mountain Road Pl 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.
- **Privacy: privacy@credcount.app** — the right address for anything in this policy: a request, an objection, a complaint, or an argument about what's written here.
- **Everything else: support@credcount.app** — bugs, questions, a request for a copy of the catalogue.

Either address reaches the same person. The split exists so a privacy request doesn't sit in a queue behind a bug report, and so we can keep the promise in §13 about how quickly we answer.

Where your data actually is: your vault is on your phone. Our server is in Germany (§6). If you use Smart Import, Google processes that data on Google's own infrastructure, which includes the United States (§7, §15). And if you back your phone up — to iCloud on an iPhone, or to your Google account on Android — a copy of your vault is in that backup, in your account, which we can't reach and aren't told about (§5). And if you email us, that email sits with our mail provider in the EEA (§10). That's the whole map. We'd rather give you the map than a reassurance.

Where Cred Count is available: we don't currently offer it in the European Economic Area. That isn't a judgement about anyone in the EEA — it's a small operation choosing not to take on a set of obligations it can't yet service properly, and we'd rather stay out than do it badly. If that changes we'll appoint an EU representative under Article 27 of the EU GDPR, name them here, and say so in the app before it happens.

Data Protection Officer: we don't have one and aren't required to — we don't monitor people at scale and don't process special category data.

This policy is written for the UK GDPR and the Data Protection Act 2018. If you're somewhere else and your own law gives you rights we haven't mentioned, you keep them; nothing here is meant to be a ceiling.

---

2. Three ideas worth two minutes

Most policies assume you know these. They're the whole story here.

Personal data means information about a living person. That's the legal definition, and it's narrower than people assume — the law says "natural person" (UK GDPR Art 4) and "living individual" (Data Protection Act 2018, s.3). Your notes are personal data. Your IP address is personal data. Your device ID is personal

data. **A rollercoaster is not.** Nemesis Reborn's height, its opening date, which park it's in — none of that is about a person, so none of it is covered by this policy or any of the rights below. That matters, because most of what our server holds is facts about rides.

Local processing means the work happens on your phone's own processor, on data that never leaves it. When Cred Count counts your creds, matches a ride name, works out dispatch capacity or awards a trophy — that's local. Nobody is on the other end. Your phone does the sum. This is how nearly all of Cred Count works.

Server processing means data travels to a computer someone else owns, and that computer's operator can in principle see what arrives.

Every privacy claim here comes down to two questions: *is this about a person?* and if so, *which of the two is happening?* The point of a local-first app is to make the second list very short.

What we hold

The next three sections are the whole of what exists about you and where each part of it sits: on your phone (§3), the one number we know (§4), and the copy your phone puts into your own cloud account without us being party to it (§5).

---

3. What stays on your device

This lives in a SQLite database in Cred Count's private storage, sandboxed by the operating system so other apps can't read it. On Android that's the app's private data directory; on iOS it's the app's own container, and Cred Count doesn't switch on file sharing, so the database doesn't appear in the Files app either. We have no backend copy, no admin screen, no ability to query it. It isn't that we promise not to look — there's nothing to look at.

- **Your ride logs** — every lap, with date, time, rating, row/seat and train.
- **Your notes** — including the personal ones. "*Back row with Dad, his first ever coaster.*" Never uploaded to us, in any feature. (One exception, flagged loudly in §7: a note sitting inside a spreadsheet you choose to Smart Import can be in the sample. Nothing else touches your notes.)
- **Your trips and itineraries.**
- **Your ops logs** — dispatch times, train counts, capacity.
- **Your trophies and achievement progress.**
- **Your own listings** — the parks and rides you've added yourself, because we didn't have them. These are yours. They sit alongside our catalogue, marked as yours, and they stay on your device unless you specifically offer one to us (§9).
- **Time Rewind history** — we soft-delete (mark as deleted rather than destroy) so you can undo mistakes, so a local undo trail exists on your device. A feature, not a shadow profile, and it goes no further.
- **Your custom name mappings** — the aliases you teach the importer.
- **Your Google sign-in tokens**, if you connect Drive or Sheets. Held in the OS secure store on your device — the Android Keystore-backed store, or the iOS Keychain — not in the app's own files. They aren't synced to iCloud Keychain. We never see them, and they're deleted when you disconnect.

An iOS-specific caveat worth knowing. On Android, uninstalling takes the tokens with it. On iOS, the Keychain is not part of the app's container, and deleting an app does not by itself delete what it put there — so a token can outlive the app that stored it, and a later reinstall can find it. **If you want them gone, disconnect Google in Settings before you uninstall**, which revokes and deletes them properly. We'd rather give you the one-line instruction than describe iOS as though it behaved like Android.

- **The email address of the Google account you connected**, alongside those tokens. It's there so Settings can show you *which* account your backups are going to — a connection screen that can't tell you which account it connected is no use to anyone. It stays on your phone. We never receive it.
- **Watch data — Android only.** If you use the Wear OS companion, your catalogue and logs move between phone and watch through Google Play services' data layer — the standard Android channel between two devices you own. We have no watch server. **There is no Apple Watch app**, so on iOS this paragraph describes nothing.
- **Your device ID.** A random number generated on your device the first time Cred Count runs, stored in the app's private storage like everything else above. It is the only identifier in Cred Count and the only thing we know about you, so it gets its own section: **§4**.

Who can see the rest of this? You.

---

4. Your device ID

This is the only identifier in Cred Count, and this section is all of it: what it is, when it leaves your phone, what it's attached to, how long it lasts, and how to make us delete what it's attached to. If you want the short answer to "*what do you actually know about me*", it's this section and nothing else.

What it is. A random number your copy of the app generated on your device the first time it ran.

What it is not. It isn't derived from your hardware, your Google account, your phone number, your SIM, your advertising ID or anything else your phone already knew about you. It's a random number we made up. We can't reverse it into anything, and neither can anyone else.

This is personal data. It's an online identifier: it links your requests together over time, which is the definition of not-anonymous. It's pseudonymous, not anonymous, and the law treats it as personal data (UK GDPR Art 4(1); Recitals 26 and 30). "Anonymous device identifier" would have read better and been wrong.

When it leaves your phone. Three things carry it: **Smart Import**, the ride-matching step that goes with it (§7), and **anything you submit to the catalogue** (§9). Nothing else does — in particular, downloading the catalogue (§6) doesn't carry it, and isn't rate limited per install.

What it's attached to:

- **Daily caps on the AI features** — the number and a count, so no single install can run up an unbounded bill. Deleted within **48 hours**.
- **Catalogue submissions you make** (§9) — so we can spot someone systematically poisoning the catalogue, and so we can find your submissions if you ask us to delete them.
- **A block list**, if it comes to that. If an install is deliberately vandalising the catalogue or hammering the AI endpoints, we can refuse further submissions from that device ID. A blocked ID is kept until we

unblock it — a block with an expiry date isn't a block. We'd rather say this plainly than claim we can "detect abuse" while implying nothing ever happens as a result.
A person makes that decision, not an algorithm. Nothing here blocks you automatically: someone looks at what was submitted and decides. Once decided, the server enforces it. And if you think we've got it wrong, say so — §13 — because we might have.

What it is not attached to: your vault, your logs, your notes, your trips, your ratings, or anything you'd recognise as *your data*. We still don't have any of that.

How long it lasts. Uninstalling removes it from your phone along with everything else. If you later reinstall and the phone restores Cred Count from a backup — Android's own backup, or an iCloud or device-to-device restore on an iPhone (§5) — the same number comes back. That's the restore working as designed, and it means a deletion request you made before the reinstall still matches. A clean install with nothing to restore generates a fresh number, unrelated to the old one.

Lawful basis: legitimate interests (UK GDPR Art 6(1)(f)). Our interest is a server that stays up, an AI bill that doesn't bankrupt a free app, and a catalogue nobody can vandalise at scale. Yours isn't overridden, because the number means nothing, links to nothing, and buys us the ability to honour a deletion request we otherwise couldn't. **You can object** — §13.

Do you have to give us any of this? Nothing here is required by law or by a contract with us — there's no contract, and no statute obliging you to hand anything over. Your IP address is unavoidable in the sense that any request to any server carries one (§6); that's how the internet works, not a choice we've made for you. The device ID is generated whether or not you ever use the features that send it, and it only leaves your phone when you use Smart Import or submit something to the catalogue. **Decline all of that and Cred Count still works** — you'd lose the spreadsheet importer and the ability to contribute corrections, and keep everything else. That's the whole consequence.

Where to find yours, and how to have it erased. Settings → App Info → Device ID, tap to copy. Send it to privacy@credcount.app and we'll delete every record still holding it. §13 sets out exactly what that covers, the three honest limits on it, and how long we take.

---

5. Your phone's own backup

Both Android and iOS have a system feature that copies apps' data into the account you're signed into, so a new phone can be set up like the old one. If you have it switched on, **Cred Count is in it — the vault included.** Your logs, your notes, your trips, your ops logs, your own listings: all of it, in your account with Google or Apple.

This is the largest movement of your data described anywhere in this policy, and it is the one we have least to do with. Everything in §6 to §11 is measured in a ride name or a hundred spreadsheet rows. This is the whole thing — and it happens between your phone and a company you already have an account with, with us nowhere in the path.

We want to be exact about the size of our involvement: it is one switch. Each platform lets a developer opt its app out of the phone's backup. That's the whole of our say. We've chosen not to opt out, on both, for the same reason: it's your backup, of your data, in your account, and it's the difference between a broken phone costing you a morning and costing you your entire logbook. Past that switch we have no part in it. We don't write the backup, we can't read it, we can't delete it, we're never told it happened, and we couldn't produce a copy of yours if a court asked us to. If you back your phone up,

that is your phone backing up your apps to your account under your agreement with Apple or Google — not us sending anything anywhere.

Bear in mind that a reinstall restored from either backup brings your device ID back with it (§4).

We're aware the tidier sentence would have been "uninstall means gone." It isn't quite true on either platform, so we haven't written it.

5.1 Android Auto Backup

It doesn't touch your Drive storage quota, only the most recent copy is kept, and on Android 9 and later it's encrypted with your screen lock — which means Google can't read it either.

To remove it or stop it: **Settings** → **Google** → **Backup**, where you can turn backup off entirely or delete what's stored.

5.2 iCloud Backup

To remove it or stop it: **Settings** → **[your name]** → **iCloud** → **Manage Account Storage** → **Backups**, pick the device, and either turn Cred Count off so it stops being included, or delete the backup. Turning Cred Count off there also deletes what's already been backed up for it.

5.3 If you're in the UK and you use an iPhone, read this bit

We'd have preferred to write the same sentence for both platforms. We can't, and the reason is worth ten lines of your time.

Apple offers an optional setting called **Advanced Data Protection**, which makes iCloud Backup end-to-end encrypted — meaning Apple holds no key and cannot read it, which is roughly what Android has done as standard since Android 9. **Apple withdrew that option in the United Kingdom in February 2025**, after the Home Office served it with a notice under the Investigatory Powers Act 2016 demanding a way in. Apple chose to remove the feature here rather than build one. Apple's own notice on this is still live, and its position as we write is that UK users who had not already turned Advanced Data Protection on **cannot turn it on**, and that device backup is specifically one of the categories affected. **You can verify this on your own device in about fifteen seconds** — Settings → your name → iCloud → Advanced Data Protection. If you're in the UK, the button to turn it on is greyed out, and Apple's explanation is printed directly above it.

So, plainly: if you are in the UK, on an iPhone, with iCloud Backup switched on, your Cred Count vault is in a backup that Apple can decrypt. Not because it's badly protected — it's encrypted in transit and on Apple's servers — but because Apple holds a key to it, which means Apple can be compelled to use it. There is currently no setting that changes this for a UK user. It is not a choice you get to make, and it is not one we get to make for you.

What we can tell you honestly is what it is and isn't. It isn't something we caused, it isn't something we can fix, and it isn't a route to us — we have no access to your iCloud account and never will. It is a consequence of where you live and whose phone you bought, and it applies identically to every other app on your device that doesn't opt out of backup, most of which will never mention it to you. We're mentioning it because a policy that spends a whole section on a random number (§4) and stays quiet about your entire ride history sitting in a backup Apple can open would have its priorities in the wrong order.

And what you can do about it, if this bothers you, is entirely in your hands: turn Cred Count off in the iCloud backup list above, and keep your own copy instead — **Settings** → **Export Data** takes two taps

and gives you a file you control (§4 of our Terms says that export stays free forever). Or use Drive backup (§8), which is a file in your Google account rather than Apple's. Neither costs you anything, and either one puts the copy somewhere you chose.

This is where things stand as this policy is published. The UK's demand has been the subject of a legal challenge and of reporting suggesting it may be narrowed or withdrawn, and if Apple restores the option here we'll update this section rather than leave you reading something stale.

What moves, and where

Six things can travel, each in its own section, each with what's in it and who ends up holding it. Four of them only happen if you make them happen; one is the app fetching a list of rides; one is you writing to us.

---

6. Downloading the catalogue

What happens: so you don't type "Nemesis Reborn, Alton Towers" by hand, your app periodically downloads our catalogue of the world's parks and rides from `api.credcount.app`.

What we receive: your **IP address**, your user-agent (device type and app version), and the time. That's what any web server sees when anything asks it for a file.

What we don't receive: your device ID (§4) — catalogue requests don't carry one, and aren't rate limited per install. And nothing about *you*. The request says "send me the catalogue", not "send me the catalogue, and I'm this person". We can't tell whether you have 3 creds or 3,000.

Where: our server is with **Hetzner, in Germany** 🇩🇪, under a data processing agreement. Deliberately EU. **The DNS that tells your app where to find it is Hetzner's too** — same company, same country, same agreement (§11). Nothing else sits in the path.

Retention: server request logs are kept **5 days**, then automatically deleted.

Rate limiting: the catalogue is protected by a limit on requests per IP address per minute, held in the server's memory and never written down. It exists so one aggressive script can't degrade sync for everyone else.

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

---

7. Smart Import

This is where your own typing can leave your device, so here's precision instead of reassurance. **If you never use Smart Import, none of this applies to you.**

Smart Import does **two separate things**, and both involve AI.

B1. Reading your spreadsheet's shape.
To work out which column is the ride, which is the date, and so on, the app takes a **sample — the first 100 rows, capped at 4,000 characters** — and sends it via our server to **Google's Gemini API**, asking "what's the structure here?"

That sample is **your raw spreadsheet, all columns included.** We don't strip anything. The reasoning, which you're free to disagree with: to remove your notes column we'd first have to identify it, and a filter that guesses wrong is worse than none — it would silently corrupt imports while claiming to protect you.

So: if the first 100 rows contain a notes column, whatever is in it is in that sample. If that's not okay, the fix is genuinely in your hands: don't use Smart Import, or delete the column before importing. The rest of the app works fine without it.

B2. Identifying rides we couldn't match.
After parsing, matching happens locally on your phone. Whatever it can't resolve — "BTR", "Steel Vengance" *(sic)* — you can send to the AI. This sends **only two fields per unmatched ride: the ride name and the park name you typed.** No dates, ratings, notes or other columns. Note the difference from B1: not a sample — **every unmatched row**, in batches of 100. Narrower per row, more rows.

Ride names and park names aren't personal data (§2). The only reason B2 appears in a privacy policy at all is that it's *your typing*, and if you typed "Space Mountain with Dave" then Dave comes along for the ride. We can't filter that without reading it.

Your device ID travels with both (§4), because that's what the daily cap counts against.

Who processes it: our server (Hetzner, Germany) → **Google Gemini API** (`gemini-2.5-flash`). Google is our processor and processes it on Google's infrastructure, which includes the United States, under the **UK Extension to the EU-U.S. Data Privacy Framework** (§15).

Training: we use a **paid, commercial Gemini key**. Under Google's paid-service terms your data is **not used to train Google's models**. That is the difference between the paid tier and the free tier of the same API, and it's the reason we pay for it.

What we keep: nothing. The sample is processed and dropped. Not written to our database, not written to our logs, no record on our side of what was in it. We record that a request happened, its size and whether it worked, because that's what the daily cap counts.

What Google keeps: up to 55 days. Google logs prompts for a limited period — currently 55 days — purely to detect abuse of its API. Not for training. That's the asterisk on "we keep nothing", and it isn't ours to waive: Google offers a zero-retention arrangement for approved projects, and if we're granted one we'll say so here and change the number. Until then, assume 55 days.

Lawful basis: your consent (UK GDPR Art 6(1)(a)). Smart Import does nothing until you point it at a file and tap the button, you're told before you do what gets sent, and the app is fully usable if you never touch it. You can withdraw simply by not using it; there's nothing retained to withdraw from.

Not automated decision-making: the AI reads spreadsheet *structure* and ride *names*. It makes no decision about you, and nothing here has legal or similarly significant effects.

---

8. Google Drive backup and Google Sheets import

What happens: if *you* turn it on, Cred Count backs your vault up to **your own** Google Drive, or reads a Google Sheet you pick.

The important bit: this is between your phone and your Google account. **It does not pass through our servers.** We never see the file or your credentials, and have no access to your Drive. We wrote the button; we're not a party to what it does. Your agreement about that data is with Google, not with us.

What's in the backup: one `cred_count_backup.json` containing your ride logs, trip logs, trip entries, achievements, unmatched logs, and the parks and rides you've added yourself. (Your own listings are in there deliberately — without them, reinstalling would leave you with ride logs pointing at rides that no longer existed anywhere.) It goes to Drive's hidden `appDataFolder` — private to Cred Count, invisible in your Drive listing. Up to **5 dated snapshots** are kept for rollback; older ones auto-delete. The file records "Android Device" or "iPhone" as its source — a generic label, not an identifier.

What Google asks you to approve. Drive backup and Sheets import sign in through **one Google authorisation**, covering three permissions:

- `drive.appdata` — the narrowest Drive scope that exists. It **cannot** read your existing Drive files; it only sees the folder it creates.
- `spreadsheets.readonly` — reads the sheet you pick. We can't modify anything.
- `drive.metadata.readonly` — lists your spreadsheets so you have something to pick *from*. Names and dates only, not contents.

Because it's one authorisation rather than two, **disconnecting either service revokes both at Google's end.** If you disconnect Sheets while still using Drive backup, the app immediately re-authorises Drive so your backups keep working — you may see this in your Google account's activity as a permission being withdrawn and granted again seconds later. That's what it is, and it's why we're telling you rather than letting you find it in a security email.

Google's sign-in code is inside the app, and only on iOS. Signing in to Google has to be done by Google's own code, and on iOS that code ships inside Cred Count — Google's sign-in library and the handful of components it depends on, including an anti-abuse component that exists to tell a real sign-in from an automated one. It is the only third-party code in the app that isn't ours, it does nothing at all unless you tap Connect, and it talks to Google rather than to us. We're listing it because "no third-party SDKs" is a claim people make loosely, and ours would be false by one item if we made it. On Android the equivalent work is done by Google Play services, which is already on your phone.

Deleting it: your backup is a file in your Google account, so you delete it the same way you'd delete anything else of yours there: **Google Drive → Settings → Manage apps → Cred Count → Delete hidden app data.** Disconnecting inside Cred Count revokes and deletes the token from your device but **leaves the backup in your Drive.** We deliberately don't offer a button that reaches into your Google account and deletes your files — and once you've disconnected we have no way in even if we wanted one.

Lawful basis: your consent. Off until you switch it on; disconnecting withdraws it.

---

9. What you contribute to the catalogue

Three different things can go from your phone to our catalogue. Only one of them carries your device ID (§4), and none of them happen without you.

A. Teaching the importer a name. When you confirm that "BTR" means "Batman The Ride", that mapping is sent to us so everyone's import gets better.

These carry no identifier at all. Not your device ID, not a comment, not an account — there isn't one. What arrives is the text you typed, the catalogue record it points at, and a count of how many people have independently made the same match. There is no way for us to work out which of these came from

you, which is worth knowing in both directions: it's the most private thing in this section, and it's the reason §13 can't offer to delete them for you.

If you created a park or ride privately (§3), aliases pointing at it are never sent. Your private listings can't leak out through the back door of a name match.

B. Corrections and proposals. When you tell us a height is wrong, report a problem, or propose a ride or park that's missing, that comes to us with **your device ID and whatever you write in the comment box.**

Mostly this isn't personal data at all — "this ride is 62m tall, not 48m" is a fact about a rollercoaster. It's in this policy for two reasons: the device ID travels with it, and **free-text comments reach us exactly as typed.** If you put a name in one, we get the name. Please keep them to "the height is wrong" rather than anything about you.

C. Offering us your own listings. If you've added a ride or a park we didn't have, you can tell us it exists. **The offer is always available and never automatic** — it is a button you press, and it is the same answer wherever you find it.

Where you'll come across it. There's a panel on the ride's own page saying it isn't in our catalogue yet, with a button to propose it — that one stays there for as long as the ride is unlisted, so you can ignore it today and change your mind next season. You'll also see it when you edit one of your own rides, when a search doesn't find what you're looking for, on a park's page, and — if you've just imported a spreadsheet full of them — once, on a card at the end, with every box unticked so you can tick only the ones you mean.

None of those routes behaves differently. Nothing is sent until you press the button, nothing is pre-selected on your behalf, and walking past any of them costs you nothing. There is no version of this where a ride you created quietly ends up with us.

What's sent is **the ride's name, its type, and the park it's at**, plus your device ID. Not when you rode it, not your rating, not your notes, not the trip it belonged to. We're asking whether the ride exists; everything else is yours and none of our business. Whatever we decide at our end, the listing on your phone is unchanged — offering it hands nothing over, and you keep using your version exactly as it was.

Lawful basis for all three: legitimate interests (Art 6(1)(f)) — building an accurate shared catalogue and keeping it from being vandalised. Your interests aren't overridden, because we're asking about a rollercoaster, not about you. With C you've also gone out of your way to say yes, ride by ride, which doesn't change the basis but makes it an easy balance to strike.

Retention:

- **The accepted catalogue fact** — kept indefinitely. It's a fact about a ride, not about a person, and it isn't personal data.
- **Your device ID and your free-text comment — erased from the record 90 days** after we've accepted or rejected the submission. The submission itself stays, because it's the audit trail for a change to the catalogue; the two fields that could be about a person are blanked out. Until we've reviewed it, it stays as submitted — we can't start the clock on a decision we haven't made. In practice review is measured in days to weeks, and one person does it.

---

10. If you contact us — anyone, not just users

This section covers **everyone who writes to us**: users with a bug, contributors, people asking for a copy of the catalogue, journalists, park press offices, suppliers, prospective clients for our consultancy work, and anyone bringing a complaint or a legal claim. You don't have to use Cred Count for this section to apply to you.

It also covers you if you write to us to exercise a right under this policy — see §13, which explains what we need, how long we take, and the awkward fact that asking us to delete your data means first giving us an email address we didn't have.

What we get: your email address, your name if it's in your message or signature, whatever you write, and anything you attach. If you're a business contact, that may extend to your role, your employer and your phone number — whatever's in your signature block.

There's also a telephone number, and it's here for a reason worth explaining. Apple requires every app's licence agreement to carry one, so ours will be published in our Terms and on our App Store listing. **It rings through to a voicemail box, not to a person at a desk** — we're a very small operation and we'd be pretending otherwise if we implied a phone was being answered. If you leave a message we get an email about it and we'll come back to you, but **email will always be faster**, and it's the route we'd genuinely rather you used.

If you do leave one: we receive the recording, the number you called from, and the date and time. Voicemail runs on **Zoho Voice** — the same company as our mail, on its European data centre, under the same data processing agreement. **We don't record calls.** The setting is off, and the only thing that ever exists is a message you chose to leave. **Recordings are deleted automatically after 7 days**, whether or not we've replied — if a message needs acting on, what survives is our reply and any notes in the email thread, which then live under the retention below like any other correspondence.

What we do with it: reply to you. Keep a record of the conversation. Nothing else. We don't add you to anything, we don't market to you, and there's nothing to opt out of because there's nothing running.

Who processes it: Zoho, as our processor, under a data processing agreement. Our mail and our voicemail both sit on Zoho's **European data centre**, so your message to us doesn't leave the EEA to reach us — whichever way you send it.

Lawful basis:

- **Correspondence generally:** legitimate interests (Art 6(1)(f)) — answering people who contact us. Hard to run anything otherwise, and you started it.
- **If we have or are negotiating a business relationship with you** — supplier, contractor, client: taking steps at your request before entering a contract, and performing it (Art 6(1)(b)).
- **Legal claims:** legitimate interests. If someone brought or threatened a claim, we'd keep what we needed to defend ourselves. We're telling you this because it's true, not because we expect it.

Retention:

- **Voicemail recordings: 7 days**, deleted automatically. Shortest retention in this document, and the one we most wanted to keep short.
- **General correspondence and support: 24 months** from the last message in the thread.

- **Business and contractual records: six years** from the end of the relationship. That's the limitation period for a contract claim in England and Wales (Limitation Act 1980, s.5), and it's how long we might need the file if something goes wrong.
- **Anything connected to an actual or threatened legal claim:** until the claim is resolved and the limitation period has run. Your right to erasure doesn't override this (UK GDPR Art 17(3)(e)), and we'd rather say so plainly than surprise you with it later.

---

11. The website

`credcount.app` is a static site. It sets **no cookies**, runs **no analytics**, and loads **no fonts, scripts or trackers from third parties** — everything it needs, including its fonts, is served from the same place as the page. Open the network tab and check; that's the point of saying it. Our host records standard web server logs (IP, user-agent, time) which are deleted after **7 days**. There is no consent banner because there is nothing to consent to.

The address itself is worth a paragraph, because most policies skip it. Before anything can reach us, something has to answer the question "*where is `credcount.app`?*" That's DNS, and ours is **Hetzner's** — the same company that runs the server, in the same country, under the same agreement. All three of our nameservers sit in Hetzner's German networks, and you can check that yourself: run `whois` on the addresses behind `hydrogen.ns.hetzner.com`, `oxygen.ns.hetzner.com` and `helium.ns.hetzner.de`.

Here's the part that surprises people. Your device doesn't ask us that question directly. It asks whichever DNS resolver it's set up to use — usually your internet provider's, sometimes Google's or Cloudflare's — and *that* resolver asks us. So what reaches our nameservers is that **somebody's resolver** wanted the address, not that **you** did. Some resolvers pass along a coarse version of your network address so they can be given a geographically sensible answer; where that happens it's a `/24`, meaning a block of up to 254 addresses, not yours.

We don't receive any of it. DNS query data isn't something we can see, retrieve or ask for — there's no query log in our control panel and none is provided to us. Whatever exists at Hetzner's own infrastructure level is Hetzner's, held in Germany, under the agreement in §15. We're telling you this rather than claiming nothing is recorded anywhere, because we genuinely don't know, and this policy doesn't guess about the insides of other people's machines.

The guarantees

What we've promised never to do, what you can make us do about it, and how long anything lasts. If you only read one part of this policy after the 30-second version, §12 is the one that's checkable from outside.

---

12. What we never collect

Not "we don't currently." These are architectural facts you can verify:

1. **No analytics.** No Firebase, Google Analytics, Sentry, Mixpanel — not configured-off, **not present**. We don't know which screens you open, how long you use it, what you tap, or how many creds you have.
2. **No crash reporting.** If it crashes, we find out because you tell us.

3. **No location.** The app doesn't request location permission on Android, on iOS or on the watch — there's no location permission in either Android manifest, and no location key in the iOS app's `Info.plist`. Cred Count cannot know where you are.
4. **No advertising IDs, and no tracking.** No AAID, no IDFA. No ads, no ad networks, no behavioural targeting. On iOS this is checkable in a way that's unusually specific: Apple requires every app to ship a **privacy manifest** declaring what it collects and whether it tracks, and Cred Count's says `NSPrivacyTracking: false`, an empty list of tracking domains, and an empty list of collected data types. It declares one thing: that it reads and writes the app's own preferences file, which is where the device ID in §4 lives. That's the whole declaration. You'll never see the "Allow Cred Count to track you?" prompt, because there is nothing behind it to allow.
5. **No account, email, password or sign-up.** There's nothing to create, nothing to log into, and no way to "delete your account" because there was never one to begin with. (Google sign-in is optional, is for *your* Drive, and isn't an account with us.) **The exception is the obvious one: if you email us, we have your email address** — that's you choosing to tell us, not us collecting it, and §10 and §13 both deal with it properly.
6. **No contacts, microphone, camera or sensors.** Cred Count never reads your photo library — the only photo permission is to *add* an image you asked to share, on both platforms. On current Android versions saving an image needs no permission at all; on iOS it's the add-only photo permission, which lets an app put a picture in your library and gives it no ability to look at what's already there. When you import a spreadsheet, your phone hands us the one file you picked; we can't go looking for others.
7. **No special category data.** No health, biometric or political data.
8. **No identifier we didn't make ourselves.** There's exactly one, it's a random number, and it's in §4. Nothing derived from your hardware, your Google account, your SIM, your advertising ID, or anything else your phone knew about you before you installed us.
9. **No selling data, ever.** No brokers, no "trusted partners." There's no business model here in which you're the product.

On permissions, platform by platform.

Android. Cred Count itself declares one: internet. The Wear OS app declares one: keeping the watch screen on while you're timing dispatches. A handful of others arrive with the standard libraries the app is built on — checking whether you're online, opening the file picker, and the biometric prompt that guards the OS secure store where your Google tokens live. None of them are prompts you'll see on a current Android, none collect anything, and none send anything to us.

iOS. iOS works differently: instead of declaring permissions up front, an app declares a reason for each *sensitive* thing it might ask for, and the system prompts you the first time it actually tries. Cred Count declares exactly one — permission to **add** a picture to your photo library, for when you tap Save on a share card. That's the only prompt the app can ever produce. There is no location key, no camera key, no microphone key, no contacts key and no tracking key, so those prompts cannot appear, because the app has no way to ask. Everything else it does — the file picker, the network check, the Keychain, the share sheet — needs no permission on iOS and gives you no prompt.

We'd rather describe these than give you a number that sounds impressive and turns out to be wrong. Both lists are in the app package and you can read them yourself.

---

13. Your rights

You have rights under UK GDPR: access, rectification, erasure, restriction, portability, objection, and withdrawing consent. Most apps list them and give you an email address. Since we hold almost nothing, most of yours are exercisable in about four taps.

> **Your right to object**
>
> You can object at any time to any processing we base on legitimate interests — that's the catalogue download (§6), the device ID (§4), catalogue contributions (§9) and correspondence (§10). To object, email **privacy@credcount.app**. You don't have to give a reason, and we'll stop unless we can show compelling grounds that override your rights.

Access and portability — built in. Settings → **Export Data** (JSON), **Export Ride Logs (CSV)** or **Export Cred List (CSV)**. Your data, open formats, right now — no request, no waiting, no ID check.

Rectification. Edit any log, date or rating in place. For catalogue errors, use Suggest Edit.

Erasure. Your vault is yours, on your hardware, and we have no copy — so this doesn't depend on us:

- **On your device:** delete individual logs in the app, or **uninstall Cred Count** — the OS removes the app's private storage entirely, taking the database with it. (On iOS, see §3 on Google tokens: the database goes, but disconnect Google first if you've connected it.)
- **In your phone's own backup:** if your phone backs itself up to iCloud or to your Google account, a copy of your vault is in there — in your account, not ours. **§5** covers what that means and how to remove it on each platform, including the part UK iPhone users should read (§5.3).
- **In your Google Drive:** yours to delete — see §8.
- **On our servers:** you have a device ID, so this actually works. **Settings → App Info → Device ID.** Send it to privacy@credcount.app and we'll delete every correction, proposal and offered listing submitted from your install, plus any records still holding it.
  Three honest limits. First, **name mappings can't be included** — as §9 explains, they're submitted with no identifier at all, so there is genuinely nothing linking one to you. We could only find "your" aliases by starting to collect something we've deliberately chosen not to collect. Second, if a submission has already been **accepted into the catalogue**, the resulting fact — "this ride is 62m tall" — stays. That's a fact about a rollercoaster, it isn't personal data, and other people's imports now depend on it. We'll delete your submission and your comment; we won't un-know the height. Third, if you uninstall on a device with backup switched off — Android's or iCloud's — the ID is gone and we have no way to reproduce it, so **get the ID before you uninstall.** We can't work backwards from a person to a number, because we've never known the person. The law recognises that limit (UK GDPR Art 11): where a controller genuinely can't identify you, it isn't required to invent a way to.

Restriction. Email us with your device ID and we'll restrict processing of anything it's attached to.

Withdrawing consent. Disconnect Drive or Sheets in Settings. Stop using Smart Import. As easy to withdraw as to give.

Withdrawing doesn't unwind what already happened — an import you ran last month was lawful when you consented to it, and stays lawful. What withdrawal stops is everything from that point on. In practice there's very little to unwind here anyway: we keep nothing from Smart Import, and your Drive backup is in your own account (§8).

Asking us for something

Most of the rights above you exercise yourself, in the app, without telling us. For the ones that need us — anything on our servers, an objection, a restriction, or just an argument about this document — the route is **privacy@credcount.app**.

Emailing us costs you the thing this whole policy is about. We don't know who you are. The moment you write to us, we have your email address, your name if it's in your signature, and whatever you tell us — which is more than we've ever held about you. There's no way around that: a request to delete data has to arrive from somewhere. We'd rather point at the irony than let you discover it. That email is handled exactly as §10 describes, and you can ask us to delete it too once we're done.

What we need from you. For anything on your device: nothing, because you can do it yourself and we couldn't help if we wanted to. For anything on our servers: **your device ID** (Settings → App Info → Device ID, tap to copy). That's the only thing that connects a request to any record we hold. Without it we can search for you, honestly, and find nothing.

We won't ask you to prove who you are. Most companies require ID for a data request, and they're right to — they hold accounts worth stealing. We hold no account, so there's nothing to protect and no identity we could check against anything. Asking you for a passport scan would collect more personal data than the request could ever be about. The device ID is the only credential that means anything here, and if you have it, you have it.

How long we take, and what it costs. We'll respond **within one month**. If a request is genuinely complex we can extend that by up to two further months, and if we ever needed to we'd tell you inside the first month and say why. **There's no charge.** We can only refuse a request if it's manifestly unfounded or excessive, or where the law says a right doesn't apply — and if we ever refuse one, we'll tell you which reason and what you can do about it, rather than going quiet.

If we get it wrong, say so and we'll fix it. If you'd rather not deal with us, the ICO is below and you don't need our permission.

Complaining. You can complain to the **Information Commissioner's Office** — ico.org.uk, 0303 123 1113. If you're outside the UK and your country has its own data protection authority, you can complain to them instead. We'd rather you emailed us first, but it's your right and we're not going to bury it.

---

14. How long we keep things

What	Where	How long
Your vault (logs, notes, trips, ops, 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 phone backups)
Android Auto 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 iPhone users: see §5.3**
Google sign-in tokens	Your device's secure store	Until you disconnect. On iOS, disconnect *before* uninstalling (§3)

What	Where	How long
Drive backup + up to 5 snapshots	Your Google account	Until you delete it; snapshots auto-pruned past 5
Server request logs (IP, user-agent)	Hetzner, Germany	5 days, then auto-deleted
Device ID — AI daily caps	Hetzner, Germany	48 hours
Device ID — block list	Hetzner, Germany	Until unblocked
Website server logs	Hetzner, Germany	7 days, then auto-deleted
DNS queries for `credcount.app`	Hetzner, Germany — never reaches us	Not ours to keep: we receive none and can't retrieve any (§11)
Smart Import contents — our side	Nowhere	Not stored: processed and dropped
Smart Import contents — Google's side	Google	Up to 55 days, abuse monitoring only
Name mappings you teach the importer	Hetzner, Germany	Indefinitely — no identifier attached
Accepted catalogue facts	Hetzner, Germany	Indefinitely — not personal data
Device ID + free-text comment on a submission	Hetzner, Germany	Erased 90 days after we accept or reject it
Voicemail you leave on our published number	Zoho Voice, EU data centre	7 days, then auto-deleted. Calls are never recorded (§10)
General correspondence, support, and privacy requests you send us	Zoho, EU data centre	24 months from last message — including our record of what we did about a request, which is how we show we handled it properly
Business and contractual records	Zoho, EU data centre	6 years from end of relationship
Anything tied to a legal claim	Zoho, EU data centre	Until resolved + limitation period

15. Where your data goes

- **Our server:** Hetzner, Germany 🇩🇪 — EU, under a DPA.
- **Our DNS:** Hetzner, Germany 🇩🇪 — the same company, the same country and the same agreement as the server (§11).
- **Gemini AI (Smart Import only):** Google. Processed on Google's global infrastructure, **including the United States**.
- **Correspondence, and voicemail: Zoho**, on its European data centre, under a DPA with **Zoho Corporation B.V.** (Netherlands) 🇳🇱 — stored in the EEA. Our published telephone number is a Zoho Voice number and its voicemail sits in the same place as the mail (§10), which is why a US dialling code doesn't put anything on a US machine.
- **Your Drive / Sheets / Android backup:** your own Google account, under your agreement with Google, not ours. We're not in the path.

- **Your iCloud backup:** your own Apple account, under your agreement with Apple, not ours. Apple is not our processor and we have no relationship with them about your data — we don't send anything to Apple, and Apple doesn't send us anything. Where that copy physically sits is between you and Apple, and §5.3 explains the one part of it that UK users should know about.

There is exactly one route to a US machine, and it is Smart Import. If you never use it, nothing of yours goes to the United States at all. That includes the machine that answers "*where is `credcount.app`?*" — it's in Germany too (§11), which is the kind of detail worth stating because it's the sort of thing a policy quietly leaves out.

Hetzner's agreement with us doesn't merely happen to be European — it says so. Clause 3(1) of that agreement 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.*" That's a contractual promise rather than a setting on a control panel, which matters because settings can be changed and clauses have to be renegotiated. Their published list of subcontractors does include companies in the United States and Singapore, and we'd rather point that out than have you find it and wonder — those apply to customers who chose a server *in* those places. Ours is in Germany.

How that transfer is lawful. Google LLC is certified under the **UK Extension to the EU-U.S. Data Privacy Framework**, which the UK government has recognised as providing adequate protection. That's an adequacy decision under Art 45 UK GDPR — the same kind of finding that lets data move to, say, Switzerland or Canada — rather than a contract we've written ourselves and hope holds up.

If that certification ever lapsed, Google's own data processing terms fall back automatically to the standard contractual clauses with the UK Addendum. We're telling you the fallback exists because a mechanism that quietly stops applying is exactly the kind of thing a privacy policy should have mentioned in advance.

Your email to us needs no such argument. It's stored in the EEA, and the UK recognises the EEA as providing adequate protection — so there's nothing to justify, because nothing leaves. That is a shorter answer than this section used to be able to give, and the reason it's shorter is that we moved our mail.

One qualification, because "stored in the EEA" is a claim about *storage* and shouldn't be read as more: Zoho is a global group, and its data processing agreement permits its companies outside the EEA to reach that mail where supporting the service requires it, under the standard contractual clauses in that agreement. We'd rather state that than let the sentence above imply something stronger than it is.

You can check all of this yourself, and we'd rather you did than take our word for it. Google's certification is public at `dataprivacyframework.gov` — search for Google LLC and you'll see the UK Extension listed with its current status. The UK government's adequacy regulations for the DPF are on legislation.gov.uk. Google's data processing terms, including the transfer clauses we're relying on, are published at `business.safety.google/processorterms`. Zoho publishes its data processing agreement and its list of sub-processors on `zoho.com`. Hetzner publishes its data processing agreement and its subcontractor list on `hetzner.com`, and the nameserver addresses in §11 resolve to German networks that anyone can look up. If you'd like any of it in a form that isn't a link, email us and we'll send it.

Two things worth saying plainly. Clever Little Goose LLC is registered in New Mexico. That has no bearing on where your data sits: your vault is on your phone, our server is in Germany, our mail is in the EEA, and the single route by which anything reaches a US machine is Smart Import, described above. And if anyone ever demanded your ride history from us under any law anywhere, the answer would be the same as the answer we'd give you: we don't have it.

16. Children

Cred Count isn't aimed at under-13s and we don't knowingly collect their data. Since we collect almost nothing from anyone, this is largely academic — there's no account to create, no profile to build, and nothing to advertise at anybody.

One place it isn't quite academic: **Smart Import runs on your 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 — the rest of the app doesn't send anything anywhere, so nothing else needs asking about. Parents: if you think your child has imported a spreadsheet with something personal in it, email us. Realistically there's nothing for us to delete, because we don't keep the sample — but you're entitled to ask, and we'd rather you did.

---

17. Keeping it safe, and telling you if we don't

Everything between your phone and our server travels over an encrypted connection (HTTPS), as does everything between your phone and Google. On iOS the app sets no exemption to Apple's transport security rules, so that's enforced by the operating system rather than merely intended by us. Your vault sits in Cred Count's private storage, which Android and iOS stop other apps reading, and which the OS encrypts at rest while the device is locked. Your Google sign-in tokens are held in the operating system's secure store — the Keychain on iOS, the Keystore-backed store on Android — not in the app's own files. Our server sits behind a firewall, its administrative interface isn't open to the public internet, and the AI keys never leave it.

None of that is exotic. It's the ordinary standard, and we mention it only because the alternative — saying nothing — invites you to assume either more or less than is true.

If we ever suffered a breach that put you at real risk, we'd have to tell you — and we'd have a problem doing it. We have no account, no email address and no way to reach you individually. That's the whole design, and it cuts both ways. So we'd do what the law allows when individual contact isn't possible: say so **in the app and on credcount.app**, plainly, with what happened and what to do. We'd report it to the ICO within 72 hours where the rules require it.

It's worth being clear about the scale of what's exposed. We don't hold your rides, your notes, your trips or your ratings — so the worst realistic case is not what you'd fear from an app like this. It's your IP address, your device ID, and any comment you've written on a catalogue submission.

---

18. Changes

If we change how any of this works, we'll update this policy and the date at the top. If a change is significant — a new bridge off your device — we'll say so **in the app**, not by quietly editing this page and hoping nobody reads the diff.

Questions, arguments, or a hole in our reasoning: privacy@credcount.app. If you think something here is wrong, tell us. We've already had to correct this policy against ourselves more than once.

Cred Count is built on the belief that software used to respect you, and could again. This policy is meant to be read, not clicked past.