

Privacy Policy for CarDex AI

Last updated: 15 August 2026

This Privacy Policy explains which personal data is processed when using the mobile application **CarDex AI - Collect Cars IRL** (“CarDex” or the “App”), for which purposes such processing takes place, and which rights users have.

Delete account and data: The CarDex account can be deleted directly in the App under **Favorites/Profile view -> Settings (gear icon) -> “Delete CardDex Account”**. If the App is no longer installed, deletion can be requested by email.

Contact: sup.studiomuench@gmail.com. Further details are provided in Section 20.

1. Controller

The controller within the meaning of the General Data Protection Regulation (GDPR) is:

Lukas Johannes Münch

Studio Münch

Zum Stausee 27

55743 Idar-Oberstein

Germany

Email: sup.studiomuench@gmail.com

2. Overview and Principles

CarDex combines real-world vehicle discoveries with a digital card collection. Users can photograph vehicles, have a vehicle identified using artificial intelligence, manage cards and discovery locations, use Google Play Games features, and make optional purchases.

CarDex processes personal data only to the extent necessary to provide the App, where consent has been given, where a legitimate interest exists, or where a legal obligation must be fulfilled. Personal data is not sold.

3. Account, Sign-In and Google Play Games

3.1 Account Creation

A CarDex account is created or linked to an existing account by signing in with **Google Play Games**. In particular, the following data may be processed:

- Google Play Games player ID,
- display name stored in Google Play Games,
- internal CarDex user ID,
- sign-in provider and technical linking identifiers,
- timestamps relating to account creation and latest updates,
- short-lived access tokens and longer-lived refresh tokens for the CarDex session.

As a general rule, CarDex receives **no email address, Google password or telephone number** through this sign-in process. Google also processes the sign-in under its own responsibility. The Google Privacy Policy additionally applies.

For older App versions or migration processes, pseudonymous installation, guest or migration identifiers may be processed. These are used solely to assign an existing inventory to the correct CarDex account.

3.2 Purpose and Legal Basis

The processing is carried out for sign-in, cross-device or cross-account restoration of the collection, synchronization, and protection against unauthorized access. The legal basis is Art. 6(1)(b) GDPR. Security and abuse-prevention measures are additionally based on Art. 6(1)(f) GDPR.

4. Technical Provision and Cloudflare

CarDex uses services provided by **Cloudflare, Inc.** and affiliated companies, in particular Cloudflare Workers, D1/KV storage and technical operational metrics. The following data may be processed:

- IP address,
- date and time of a request,
- requested endpoint and response status,
- device, browser, App and network metadata to the extent technically transmitted with an internet request,
- authentication and security information,
- content required for the respective function, for example card, inventory, purchase or location data.

Cloudflare processes this data to deliver backend functions, defend against attacks, apply rate limiting, analyze errors and ensure availability. The legal bases are Art. 6(1)(b) and (f) GDPR. Further information is available in the Cloudflare Privacy Policy.

CarDex does not use a separate general tracking or user analytics platform within the App. However, technical request and error metrics for the backend may be provided by Cloudflare.

5. Camera, Vehicle Photos and Card Creation

5.1 Capture and Local Storage

The camera function is used only when users actively photograph a vehicle. The original photo is stored in the App's private storage on the device and is used to display the user's self-created card. Users may also share a card using operating-system functions or deliberately save a copy to the gallery.

A copy saved in the gallery or shared through another app is located outside the App storage controlled by CarDex. It is not automatically removed when a card or the CarDex account is deleted and, where necessary, must be deleted by the user in the relevant app or gallery.

5.2 Transmission for Vehicle Recognition

For recognition, a compressed processing copy of the photo is created. Where technically possible, image metadata such as EXIF data is not included. This image copy is transmitted in encrypted form to the CarDex backend and then forwarded to OpenAI for analysis.

CarDex does not permanently store the transmitted image data in the Cloudflare inventory. However, an internal local file reference may be stored in the inventory so that the App can associate the photo stored on the device with the correct card. The AI-processing provider may temporarily store submitted content and technical log data in accordance with its own retention rules; details are provided in Section 6.

Users should only take photos that they are entitled to take and should, where possible, avoid capturing identifiable persons, license plates or other unnecessary personal information.

5.3 Legal Basis

To the extent that processing of a photo concerns personal data of the user and is necessary for the vehicle recognition and card creation requested by that user, the processing is based on Art. 6(1)(b) GDPR. Where a vehicle photo only incidentally contains personal data of third parties, such as identifiable persons or a vehicle license plate that can be linked to a person, CarDex bases the processing limited to vehicle recognition on Art. 6(1)(f) GDPR. The legitimate interest is to technically provide the expressly requested vehicle recognition without intending to identify or monitor the persons shown. CarDex takes the interests of affected third parties into account in particular through data minimization, purpose-limited image processing, and the notice that unnecessary personal content should be avoided where possible.

Camera permission can be revoked at any time in the Android settings; the capture function will then no longer be available.

6. AI-Based Vehicle Recognition by OpenAI

CarDex uses the API of **OpenAI Ireland Ltd.** to analyze captured vehicle images. In particular, the following data is transmitted:

- the compressed image copy,

- a technical task description for vehicle recognition,
- where applicable, contextual information required for recognition,
- technical request and security metadata.

The AI may return information such as make, model, vehicle type, model year or an estimated classification. Results may be incorrect and should not be understood as a binding technical or economic assessment.

According to OpenAI's published information, data from the API is generally not used to train or improve models unless the API customer expressly opts in to such use. Safety and abuse-monitoring logs may be retained for up to 30 days by default, unless longer retention is legally required or reasonably necessary to protect the services or third parties. With the Responses API, application-state data may additionally be stored depending on the specific API configuration. OpenAI currently describes a 30-day retention period for standard Responses API storage and states that response data is retained for at least 30 days in that configuration. The retention period actually applicable to CarDex therefore also depends on the OpenAI configuration used and the data controls enabled for the API project. Further information: OpenAI API Data Controls and OpenAI Data Processing Addendum.

The legal bases for image processing are set out in Section 5.3. OpenAI processes the submitted content as part of the commissioned AI analysis. CarDex does not intentionally use personal or license-plate data contained in images to identify individuals.

7. Collection, Cards and Favorites

To provide the collection, CarDex processes in particular:

- internal card ID and user assignment,
- vehicle data recognized or confirmed by the user,
- creation and modification timestamps,
- card status, source and sorting information,
- purchased or unlocked cards and entitlements,
- optionally the discovery location,
- technical usage counters and limits,
- locally stored favorites and App settings.

The server-side inventory is assigned to the CarDex account. Certain data, such as photos, favorites, settings and cached inventory data, is additionally or exclusively stored locally on the device. The legal basis is Art. 6(1)(b) GDPR.

When an individual card is deleted, its server-side card record is removed. An image file already stored in the App's private storage may technically remain until the account is deleted, the App is uninstalled, or the App data is manually deleted. Copies saved in the gallery or in other apps also remain there.

8. Location Data and Discovery Map

Users can allow CarDex to capture their location when creating a card. Depending on the Android permission granted, this may be an approximate or precise location. In particular, latitude and longitude as well as the associated card and capture timestamp are processed.

The location is used to display where a card was discovered in the user's personal collection and on the interactive map. Discovery locations stored in CarDex are not automatically made public or displayed to other users.

Location processing is based on consent under Art. 6(1)(a) GDPR. Consent can be withdrawn at any time through the Android permission settings with effect for the future. CarDex can continue to be used without granting location permission; location-related functions will then be limited.

9. Map Display via OpenFreeMap

To display the interactive map, CarDex loads map styles and map data from **OpenFreeMap**, operated by Hyperknot Software Kft., Hungary. During these requests, technically necessary data such as the IP address, time, App/device information and the requested map area may be processed. The specific cards and discovery markers stored in CarDex are not transmitted as such to OpenFreeMap; however, the requested map area may allow conclusions to be drawn about the region being viewed.

According to OpenFreeMap, IP addresses are not routinely stored in standard logs. In the event of security incidents, IP logging may temporarily be enabled, generally for no more than 30 days. Further information: OpenFreeMap Privacy Policy.

The processing serves to provide the map function requested by the user. The legal basis is Art. 6(1)(b) GDPR; secure and efficient provision is additionally based on Art. 6(1)(f) GDPR.

10. Network and Wi-Fi Checks for Manipulation Prevention

When creating a card, CarDex checks technical characteristics of the current network connection in order to make manipulation of regional pricing or recognition functions more difficult. Depending on the Android version and permissions granted, the following data may be processed locally:

- connection type,
- Wi-Fi status,
- SSID and BSSID,
- local IP and gateway information,
- security characteristics of reachable Wi-Fi networks.

Raw SSID, BSSID, IP, gateway and Wi-Fi scan data is checked exclusively on the device and is not permanently transmitted to or stored by the CarDex backend. Only derived technical information is sent to the backend, in particular whether a Wi-Fi connection exists and whether it is recognized as a private or protected Wi-Fi network. This information is used to assess the respective request and does not become part of the card collection.

The processing serves fraud, abuse and manipulation prevention. The legal basis is Art. 6(1)(f) GDPR. To the extent information is read from the user's terminal device for this purpose, this is carried out - where applicable - as technically necessary access under Section 25(2) no. 2 TDDDG. Required Android permissions can be revoked in the system settings; individual functions may then be unavailable or only available to a limited extent.

11. Google Play Games, Achievements and Leaderboards

CarDex uses Google Play Games for sign-in, achievements and leaderboards, among other purposes. The Google Play Games player ID, display name, game progress, unlocked achievements and leaderboard scores may be transmitted to Google. Google processes this data under its own responsibility in accordance with the Google Privacy Policy.

The processing is carried out to provide the requested game and account functions on the basis of Art. 6(1)(b) GDPR.

12. Advertising and Consent Management

In the free version, CarDex may display advertising through **Google AdMob**. Google User Messaging Platform (UMP) is used to obtain and manage privacy-related choices. Depending on region, consent, device settings and technical availability, personalized, non-personalized or limited ads may be served.

In particular, the following data may be processed:

- IP address and approximate region,
- device and App information,
- advertising ID, where available and permitted,
- interactions with ads,
- consent and privacy signals,
- technical information for delivery, fraud prevention, reach measurement and frequency capping.

Non-personalized ads may also use contextual information and, in certain modes, local identifiers for delivery, reporting or frequency capping. In limited ads mode, functions using local identifiers are reduced or disabled. Further information is available in the Google Privacy Policy, AdMob privacy information, and AdMob ad-serving modes.

Where consent is required, processing is based on Art. 6(1)(a) GDPR and - to the extent information is stored on or read from the terminal device - Section 25(1) TDDDG. Without consent, access to terminal-device information may take place only to the extent that the requirements of Section 25(2) TDDDG are actually met, in particular where access is strictly necessary to provide a digital service expressly requested

by the user. Necessary security and fraud-prevention measures may additionally be based on Art. 6(1)(f) GDPR. A choice already made can be changed through the privacy options offered in CarDex or through Android/Google settings.

Advertising in CarDex can be disabled by purchasing “Remove Ads” or the “Full Version”. Section 13 applies to purchase data.

13. In-App Purchases and Google Play Billing

CarDex offers optional in-app purchases, for example individual cards, “Remove Ads”, “Unlimited Collection” or the “Full Version”, through Google Play Billing. Payment processing is handled by Google. CarDex does not receive complete payment or credit-card details.

For verification, assignment, restoration and prevention of multiple redemption, CarDex processes in particular:

- product ID,
- Google Play purchase token,
- order ID, where provided by Google,
- a hash value of the purchase token,
- purchase, acknowledgment and assignment status,
- timestamp and associated CarDex user ID,
- entitlements derived from the purchase in the inventory.

The purchase token is transmitted to the Google Play Developer API for server-side verification. Processing is carried out for performance of the contract under Art. 6(1)(b) GDPR, for fraud prevention under Art. 6(1)(f) GDPR and, where required, to comply with legal obligations under Art. 6(1)(c) GDPR.

When a CarDex account is deleted, the CarDex-side purchase assignment and entitlements are deleted. Purchase history stored by Google and payment records required by law are not deleted as a result. Eligible purchases that remain associated with the Google account may, where applicable, be restored in a CarDex account created later.

14. Local Storage and Android Backup

CarDex stores on the device, in particular, photos of self-created cards, favorites, settings, cache data and inventory data. Session tokens are stored in protected Android storage.

The App permits Android Auto Backup and Android device transfer. As a result, local App files and settings may - depending on the Android version, Google account, device settings, available backup storage and system limitations - be backed up to a private Google Drive backup or during device transfer and restored after reinstallation. The protected storage used by CarDex for session tokens is expressly excluded from this backup.

Android backups are controlled by Google and the user. Deletion within CarDex removes data from the currently used device and the CarDex backend, but cannot immediately remove existing backup copies from the Google account. Google provides information and control options in the Android Auto Backup documentation and in Android/Google backup settings.

The legal basis for local storage is Art. 6(1)(b) GDPR; Section 25(2) no. 2 TDDDG additionally applies to technically necessary storage access.

15. External Links, Sharing, Reviews and Updates

CarDex contains optional external links, including links to YouTube, Instagram, TikTok or X, for example in connection with free cards. The relevant external app or website is opened only after the user actively selects the link. The privacy policies of the respective provider then apply; customary technical connection data may be transmitted to that provider. CarDex does not intentionally transmit the CarDex inventory or CarDex user ID in this process.

When users share cards through the sharing function, they themselves choose the recipient or third-party app. The provider of the selected service is responsible for any further processing. Links to reviews or updates open Google Play and are subject to Google’s privacy policies.

16. App Permissions

CarDex may request, in particular, the following Android permissions:

- **Camera:** capturing a vehicle,
- **Location:** optional discovery location for a card and technically required Wi-Fi functions,
- **Network and Wi-Fi status / nearby devices:** connection detection and manipulation prevention,
- **Internet:** communication with backend and third-party services,
- **Advertising ID:** ad delivery, where available and permitted,
- **Notifications or gallery/media access:** only where a corresponding optional function is used and the operating system requires such permission.

Permissions can be revoked in the Android settings. Revocation applies for the future and may restrict the respective function.

17. Recipients and Processors

Depending on use, data may be transmitted to the following categories of recipients:

- **Cloudflare:** backend, database, network and security services,
- **OpenAI Ireland Ltd. and, where applicable, other OpenAI companies/sub-processors:** AI-based vehicle recognition,
- **Google:** Play Games, Google Play Billing/Developer API, AdMob, UMP and Android Backup,
- **OpenFreeMap / Hyperknot Software Kft.:** retrieval of map styles and map data,
- **apps and external services selected by the user:** only when the user actively shares content or opens a link,
- public authorities or other bodies where there is a legal obligation to disclose data.

Where providers act as processors, they are engaged on the basis of a contract pursuant to Art. 28 GDPR. Some providers additionally process data for their own purposes and are independently responsible for such processing.

18. Transfers to Third Countries

CarDex uses internationally operating service providers. Depending on the service, contractual structure and technical processing, personal data may therefore also be processed outside the European Economic Area or made accessible from outside it. This applies in particular to services provided by Cloudflare, OpenAI and Google. Under OpenAI's current contractual terms, OpenAI Ireland Ltd. is generally the contracting entity for API customers established in the EEA; nevertheless, transfers to affiliated companies or sub-processors outside the EEA may also take place.

Where personal data is transferred to a third country, this is carried out in accordance with Arts. 44 et seq. GDPR. Transfer mechanisms may in particular include an adequacy decision of the European Commission under Art. 45 GDPR - such as the EU-U.S. Data Privacy Framework where the respective recipient is validly certified - or appropriate safeguards under Art. 46 GDPR, in particular the EU Standard Contractual Clauses. Where necessary, supplementary technical and organizational safeguards are taken into account.

Users can request information about the specific transfer mechanisms and safeguards used by contacting the email address stated in Section 1.

19. Retention Periods

Personal data is stored only for as long as necessary for the respective purpose. In particular, the following criteria apply:

- account, inventory and entitlement data generally until the CarDex account is deleted,
- individual server-side card data until the card or account is deleted,
- local photos and App data until account deletion, uninstallation, manual deletion of App data or removal by the operating system; an image file may remain locally after deletion of only an individual card,
- session and refresh tokens until they expire, are replaced, the user signs out, or the account is deleted,
- security, rate-limiting and abuse-prevention data for as long as required for protection and enforcement of the relevant limits; records directly associated with the account are removed when the account is deleted unless a superior retention obligation applies,

- CarDex-side purchase assignments until account deletion; purchase and payment data remaining with Google in accordance with the retention periods applicable there,
- OpenAI content and security logs generally in accordance with the provider retention periods stated in Section 6,
- technical logs and backups in accordance with the deletion and retention cycles of the respective infrastructure or platform provider,
- data subject to statutory retention obligations for the duration of the respective statutory period.

Once the purpose no longer applies, data is deleted or anonymized unless legal obligations or the establishment, exercise or defense of legal claims require continued retention.

20. Deleting Cards, Account and Data

20.1 Individual Cards and Local Copies

Deletable self-created cards can be removed directly in CarDex. This deletes the server-side card record. As explained in Section 7, the local image file may remain until the account is deleted, the App is uninstalled, or the App data is manually deleted. Copies saved in the gallery or other apps, or copies that have been shared, must be deleted separately there.

20.2 Deleting the CarDex Account in the App

The CarDex account can be deleted in the App using the following path:

Favorites/Profile view -> Settings (gear icon) -> “Delete CardDex Account”

After an additional confirmation, the App sends an authenticated deletion request to the CarDex backend. In particular, the CarDex user account, server-side inventory, cards and discovery locations, entitlements, free-card claims, CarDex-side purchase assignments, active sessions, and directly associated usage and security counters are deleted. The App then removes local CarDex data and session tokens from the device currently in use.

The following data, in particular, is not automatically deleted:

- data in the Google Play Games account, such as achievements or leaderboard scores,
- purchase and payment history at Google Play,
- images saved in the gallery or shared with other apps,
- existing Android/Google backup copies,
- data that a provider must continue to retain under its own responsibility or because of legal obligations,
- purely technical security logs that are no longer directly associated with an active account, until the applicable provider retention period expires.

Account deletion is final. Signing in again at a later time may create a new CarDex account. Eligible Google Play purchases may, where applicable, be restored; the deleted card collection will not be restored as a result.

20.3 Requesting Deletion Without the App Installed

Users can also request deletion of their CarDex account and associated CarDex data without reinstalling the App by sending an email to **sup.studiomuench@gmail.com**.

Recommended subject line: **CarDex Account Deletion**

To help identify the account, users should provide their Google Play Games display name and - if still available in the App - the internal CarDex ID. A reachable email address is required for follow-up questions and confirmation. Please never send passwords, purchase tokens or vehicle photos by email. To protect against unauthorized deletion, appropriate proof of identity or confirmation through the linked account may be requested.

The request will be handled without undue delay and generally within one month. Statutory exceptions, identity verification or a permissible extension of the response period remain possible. Sections 19 and 20.2 explain which data is deleted and which data may continue to be retained.

This publicly accessible Privacy Policy also provides an external means of requesting account deletion. The deletion route must remain permanently accessible, easy to find and functional on the published page; users must not be required to reinstall the App in order to submit an external deletion request.

21. Security

CarDex implements appropriate technical and organizational measures, including encrypted HTTPS connections, protected session tokens, server-side authentication, purchase verification, rate limiting and plausibility checks. However, no system can guarantee absolute security. Users should protect access to their Google account and device and report any irregularities without undue delay using the contact address.

22. Overview of Legal Bases

Depending on the processing activity, processing is based in particular on:

- **Art. 6(1)(a) GDPR:** consent, for example for optional precise location processing or advertising requiring consent,
- **Art. 6(1)(b) GDPR:** provision of the account, vehicle recognition, collection, map, purchases and other requested App functions,
- **Art. 6(1)(c) GDPR:** compliance with legal obligations,
- **Art. 6(1)(f) GDPR:** IT security, stability, error analysis, prevention of abuse, fraud and manipulation, and enforcement of reasonable usage limits,
- **Section 25(1) TDDDG:** storing information in, or accessing information from, terminal equipment where consent is required,
- **Section 25(2) TDDDG:** technically necessary storage or necessary access to terminal equipment.

Where processing is based on legitimate interests, those interests consist in particular in the secure, stable and abuse-resistant operation of CarDex.

23. Requirement to Provide Data and Consequences of Not Providing It

As a general rule, the provision of personal data is neither legally required nor is there a general obligation to provide optional data. However, certain information and processing operations are technically or contractually necessary if the respective function is to be used.

In particular:

- To create and use a CarDex account, the identifiers required for Google Play Games sign-in and account assignment are necessary. Without this data, account-related functions, synchronization and restoration cannot be provided, or cannot be provided in full.
- For AI-based vehicle recognition, a processing copy of the captured vehicle photo must be transmitted to the backend and the AI service. Without this transmission, automatic vehicle recognition is not possible.
- Location data is optional. Without granting location permission, CarDex can generally still be used; discovery-location functions will then be limited.
- In-app purchases are optional. The purchase and transaction identifiers required for them are processed only when a purchase is made, verified or restored.
- Consent to advertising or terminal-device access requiring consent is voluntary and can be withdrawn with effect for the future. The specific ad delivery may change as a result; paid ad-free functions are unaffected.

24. Rights of Data Subjects

Subject to the applicable legal requirements, data subjects have in particular the right to:

- access under Art. 15 GDPR,
- rectification under Art. 16 GDPR,
- erasure under Art. 17 GDPR,
- restriction of processing under Art. 18 GDPR,
- data portability under Art. 20 GDPR,
- object to processing based on Art. 6(1)(e) or (f) GDPR under Art. 21 GDPR,
- withdraw consent with effect for the future under Art. 7(3) GDPR.

Withdrawal of consent does not affect the lawfulness of processing carried out on the basis of consent before its withdrawal. Requests may be sent to the email address stated in Section 1. Appropriate proof of identity may be requested in order to prevent unauthorized disclosure or deletion.

25. Right to Lodge a Complaint

Data subjects may lodge a complaint with a data protection supervisory authority in accordance with Art. 77 GDPR. For the controller, the competent authority is in particular the **State Commissioner for Data Protection and Freedom of Information of Rhineland-Palatinate (Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz)**. Information and contact details are available at www.datenschutz.rlp.de. The right to contact another competent supervisory authority remains unaffected.

26. Automated Processing and AI Results

AI-based vehicle recognition is used solely to generate suggestions for vehicle data and card content. Technical manipulation, limit or security checks may automatically reject an individual request. These processes do not produce legal effects or similarly significant effects within the meaning of Art. 22 GDPR. If an obvious error occurs, users can try the function again or contact CarDex using the contact address.

27. Changes to this Privacy Policy

This Privacy Policy may be updated if functions, providers, legal requirements or data-processing activities change. The current version will be made available in the App and/or through the privacy webpage specified in the store listing. Users will be informed in an appropriate manner of material changes.