

Privacy Policy – Drinqo

Effective Date: 17 April 2026

In this document, you will find details regarding the personal data that **Drinqo**, operated by Jacob König in Vienna, Austria ("we", "us" or "our"), collects in connection with the Drinqo mobile application (the "App"). We also explain the purposes for which we collect this data and how we process and protect it, in compliance with the General Data Protection Regulation (GDPR) and other applicable laws.

What Are Personal Data?

"Personal data" means any information relating to an identified or identifiable natural person. This includes details such as a person's name, contact information, or even a device identifier or IP address. Personal data is protected by privacy laws like the GDPR and the Austrian Data Protection Act (DSG), which regulate how such information can be collected, used, and shared.

Privacy at a Glance

Drinqo is designed to be a no-friction party game. With that in mind:

- **No account, no email, no password.** You can play without signing up. The App uses anonymous authentication only.
- **Player names stay on your device.** The names you type at the start of a game (e.g. "Anna", "Tom") are processed locally and are not stored on our servers.
- **Question content is not personal data.** All "Who is most likely to..." questions are pre-written by us and are the same for every user.
- **We never collect payment details.** All purchases of card decks are processed by Apple or Google.

User Data Collection & Storage

We collect and store only the limited information needed to operate the App and to remember which card decks you have unlocked. The data we collect is limited to what is necessary for providing our services:

- **Anonymous User ID:** When you first open the App, Firebase Authentication automatically generates a random anonymous user ID (UID) and assigns it to your installation. This ID is not linked to your name, email or any real-world identity. We use this UID to remember which decks you have purchased and to keep your trial progress between sessions.
- **Display Name (optional):** If you choose to set a name for yourself in the App, we store it together with your anonymous profile so it can be shown back to you. You may change or remove it at any time.
- **Unlocked Decks & Purchases:** We store the list of card decks you have unlocked, your total purchase count, and an audit log of each in-app purchase (deck ID, product ID, platform "iOS" or "Android", price, currency, status, transaction ID and timestamp). We use this to deliver the content you have paid for and to restore your purchases on a new device.
- **Trial Progress:** For paid decks that include a free trial, we store a counter of how many trial cards you have already used per deck (e.g. "nsfw: 7 of 10"). This is used to show the paywall once the free cards are consumed.

- **Session Statistics:** Aggregated counters such as total games played, total cards played and the last deck played, plus timestamps for when your profile was created and when you were last active in the App.
- **Player Names Entered During a Game:** The first names or nicknames you type before starting a game are kept in the App's local memory only for the duration of that game. They are not transmitted to our servers and are erased when you close the App or start a new game.
- **Diagnostic & Crash Data:** If our App crashes, Firebase may collect technical information about the crash (such as device model, operating system version and a stack trace). This helps us fix bugs.

Important: We **do not** know who you are. Drinqo does not collect your name, email address, phone number, contacts, photos, location, or any other personal information beyond what is described above. The "Who is most likely to..." questions and any answers given during the game (taps to assign a drink) are processed on the device only and are not stored on our servers.

All profile data described above (anonymous UID, unlocked decks, trial progress and session counters) is stored securely in our cloud database powered by Firebase Firestore (a service by Google). This data is kept only until you delete the App and ask us to delete the associated profile (see User Rights & Data Deletion below).

You are not obligated to provide any personal data to use Drinqo. The App can be played without setting a display name. The only data that is technically required to use the App is the anonymous UID, which is generated automatically and contains no personal information about you.

Authentication & Security

We use Firebase Authentication (provided by Google) to manage anonymous sign-in. When you first open the App, Firebase issues a random user ID for your installation. No email address, no password and no third-party login is required. We do not store any login credentials on our servers, because no credentials exist.

All communication between the App and Firebase is encrypted in transit using HTTPS/TLS to safeguard your information. We also implement industry-standard security measures to protect the data we hold and we regularly update our systems and practices to maintain its security and confidentiality.

Purposes of Data Processing

We process the limited personal data described above only for specific, legitimate purposes related to the operation and improvement of Drinqo. These purposes include:

- **Providing and Improving Services:** To provide, maintain and improve the App's features (e.g. remembering which decks you have unlocked, restoring purchases, showing the correct paywall after the trial cards are used, and keeping basic session statistics).
- **Purchase Verification & Restoration:** To verify your in-app purchases through Apple or Google and to restore them when you reinstall the App or switch devices.
- **Security and Enforcement:** To enforce our Terms and Conditions, prevent misuse of the App, and ensure the security and integrity of our platform. This includes monitoring for fraudulent or suspicious activities such as fake purchases.
- **Research and Analytics:** To analyze usage patterns and user interactions in an aggregated and anonymized manner so we can understand how the App is used and improve the user experience.

- **Contractual Necessity:** To fulfill our obligations to you when you make an in-app purchase (legal basis: Art. 6(1)(b) GDPR – performance of a contract or pre-contractual steps).
- **Legitimate Interests:** To safeguard our legitimate interests, such as the security of our IT infrastructure, the prevention of fraud and the basic improvement of our service, provided such interests are not overridden by your rights (legal basis: Art. 6(1)(f) GDPR).

We will not use your personal data for any purposes that are incompatible with those listed above without first obtaining your consent.

In-App Purchases & Payment Processing

Drinqo is free to download. The App includes a free starter card deck and additional themed card decks (such as Party, Couples, NSFW, Bachelorette, College and seasonal packs) that can be purchased individually or as a bundle. All in-app purchases are one-time, non-consumable unlocks: once you buy a deck, you own it permanently on your platform account and can restore it on any device that uses the same Apple ID or Google account.

- **Payment Processing by Apple/Google:** All payments for in-app purchases are processed through your platform of choice (Apple App Store on iOS, Google Play Store on Android). We **do not** collect or store any of your billing information (such as credit card numbers or other payment details) on our servers. Your payment details are handled securely by Apple or Google via their in-app purchase system.
- **What We Receive:** From the platform, we receive a transaction confirmation containing the product ID of the deck purchased, the platform ("iOS" or "Android"), the price and currency, the transaction status and a transaction ID. We link this confirmation to your anonymous UID so we can grant you the deck and restore the purchase later.
- **Restore Purchases:** You can re-trigger a purchase restoration at any time from the App's shop or settings. The App will then ask Apple or Google for the list of products purchased on your platform account and re-unlock the corresponding decks.

Data Sharing with Third Parties

We value your privacy and handle your data with care. We do not sell, rent, or trade your personal information to any third parties for marketing or any other purposes. We only share data with third parties in the limited scenarios necessary for operating the App or when required by law:

- **Service Providers (Processors):** We share data with a few trusted third-party service providers only as needed to run the App and deliver its services. These providers act on our behalf and are contractually obligated to protect your information and use it only for the purposes we specify. The key service providers we use are:
- **Google Firebase (Authentication & Storage):** We use Firebase Authentication to issue your anonymous user ID and Firebase Firestore to store your profile data (unlocked decks, trial progress, session statistics) as described above. Firebase is a service provided by Google LLC.
- **Apple App Store and Google Play:** These platforms handle in-app purchases. When you buy a deck, Apple or Google will process your payment details, and we will receive the resulting transaction confirmation linked to your anonymous UID.
- **Legal Compliance:** If we are under a legal obligation to disclose your data – for example, in response to a court order, subpoena or other legal process – we may share information as required by law. We will only do so after verifying the request is

legitimate and necessary, and where possible and lawful, we would inform you of such disclosure.

- **With Your Consent:** In any situation where you have given us specific consent to share your data with a third party, we will honor that consent.

Aside from the cases above, no personal data is shared with any other third parties. All third parties that process data on our behalf (Firebase, Apple App Store, Google Play) are listed above and have privacy measures in place. We ensure that each of these providers only receives the minimum information necessary for them to perform their function.

International Data Transfers

Some of the third-party service providers we use are located outside of the European Union (EU) or the European Economic Area (EEA). In particular, using the App may involve transferring your personal data to servers in the United States or other countries that may have different data protection standards than your home country. For example, parts of Firebase, Apple's and Google's infrastructure may be based in the U.S.

Whenever we transfer personal data out of the EU/EEA, we take steps to ensure that an adequate level of protection is accorded to your information in line with GDPR requirements. These steps include:

- **Adequacy Decisions:** If the data is sent to a country that the European Commission has recognized as providing an adequate level of data protection, we rely on that decision (such as the EU–U.S. Data Privacy Framework, where applicable to the recipient).
- **Standard Contractual Clauses:** In the absence of an adequacy decision, we rely on European Commission-approved Standard Contractual Clauses (SCCs) or equivalent legal safeguards as part of our agreements with the service providers. These clauses contractually require your data to be protected to EU privacy standards regardless of where it is processed.
- **Other Safeguards:** We may also implement additional technical and organizational measures (such as encryption and strict access controls) to protect data transferred internationally. We continually monitor legal developments and our partners' practices to ensure ongoing compliance.

By using Drinqo, you understand that your data may be transferred to and processed in countries outside your own. However, please rest assured that we always safeguard your privacy by ensuring any such transfers are lawful and secure.

User Rights & Data Deletion

As a user of Drinqo and as a data subject under GDPR and other applicable laws, you have several rights regarding your personal data. We are committed to upholding these rights. Subject to certain legal conditions and exceptions, you have the right to:

- **Access Your Data:** You can request confirmation of whether we are processing your personal data, and if so, request a copy of the data we hold about you. Note that, because the App uses anonymous authentication, you will need to provide us with your anonymous user ID (visible in the App's settings) so we can locate the data associated with your installation.
- **Rectification:** You have the right to ask us to correct or update any inaccurate or incomplete personal data we have on file about you (for example, your display name).

- **Erasure (Right to be Forgotten):** You can request that we delete your personal data. This includes the option to delete your in-App profile, which will remove all data we hold that is linked to your anonymous UID (see below).
- **Restriction of Processing:** You can ask us to restrict the processing of your personal data in certain circumstances – such as if you contest the accuracy of the data or object to us processing it.
- **Object to Processing:** You have the right to object to certain types of processing, including processing based on a legitimate interest. If you object, we will reconsider our processing activities or cease processing your data, unless we have compelling legitimate grounds to continue.
- **Withdraw Consent:** If we ever rely on your consent to process your data, you can withdraw that consent at any time. Withdrawing consent will not affect the lawfulness of any processing we carried out based on your consent before its withdrawal.
- **Data Portability:** You have the right to receive your personal data that you provided to us in a structured, commonly used, machine-readable format, and to have that data transmitted to another controller where technically feasible.
- **Lodge a Complaint:** If you believe your data protection rights have been violated, you have the right to file a complaint with the relevant data protection supervisory authority. In Austria, this is the Österreichische Datenschutzbehörde (Austrian Data Protection Authority, www.dsb.gv.at).

Profile Deletion: You can request deletion of your Drinqo profile at any time by contacting us at the email address in the Contact section below and providing your anonymous user ID. When you request deletion, we will erase the profile data we hold (display name, unlocked decks list, trial progress, session statistics) from our active databases. Please note that:

- Deletion of your in-App profile data does **not** refund or revoke purchases recorded by Apple or Google. Your purchases remain associated with your Apple ID or Google account on the platform side, and you will still be able to restore them in the future via Apple's or Google's "Restore Purchases" mechanism.
- Once profile deletion is completed, we cannot recover the deleted data. If you continue using the App after deletion, a new anonymous UID will be created and you will appear to us as a new user.

To exercise any of your rights, you can contact us using the information provided in the Contact section below. We will respond to your requests in accordance with applicable law, typically within one month. Because we generally have no way to verify your identity beyond your anonymous UID, we may need additional information to make sure we act on the correct profile.

Retention Policy

We retain your personal data only for as long as necessary to fulfill the purposes outlined in this Privacy Policy or as required to provide you with our services. In practice, this means we keep your profile data for as long as the corresponding installation of Drinqo remains active or until you ask us to delete it.

If we receive a verified deletion request from you, we will promptly delete your profile data from our active databases. In general, once your profile is deleted, your data will no longer be accessible through the App or our systems.

There are a few exceptions to immediate deletion in order to comply with legal and administrative obligations:

- We may retain certain data for a short period in backup systems, which are kept securely. Any personal data in backups will be purged or overwritten in accordance with our regular backup retention cycle.
- We may retain data if necessary to comply with applicable laws or regulations. For example, in-app purchase records may need to be kept for a certain period to satisfy accounting or tax regulations.
- If there is an outstanding issue, claim or dispute requiring us to keep your information (for instance, an unresolved legal matter or a chargeback), we will retain the necessary data until the issue is resolved and/or for the duration that legal requirements demand.

In all cases, when we retain data for legal or contractual requirements, we ensure it is only kept for the minimum duration necessary and access to it is restricted. After the applicable retention period expires, or once the reason for retention has been resolved, the data will be securely deleted or anonymized.

Age Limit & Alcohol Disclaimer

17+ Only. Drinqo is rated 17+ in the Apple App Store and is intended for an adult audience. The App contains references to drinking alcohol, mature humor and, in some optional decks, sexually suggestive content. The App is **not** directed at children. We do not knowingly collect personal data from children under the age of consent applicable in their jurisdiction (which is 14 in Austria under the DSG, and varies between 13 and 16 across the EU under Art. 8 GDPR).

Drink responsibly. Drinqo is a party game that may suggest taking a sip of alcohol as part of gameplay. The App is for entertainment purposes only. Alcohol consumption is voluntary, and you may always replace alcoholic drinks with a non-alcoholic alternative. Please drink responsibly and only if you are of legal drinking age in your jurisdiction. Never drink and drive. We strongly discourage minors, pregnant individuals, and people for whom alcohol is medically inadvisable from consuming alcohol while playing.

If we become aware that we have inadvertently collected personal data from a child below the applicable age of consent without verifiable parental consent, we will take steps to delete that information promptly. Parents or guardians who believe a child may have used the App may contact us using the details below.

Contact Information

If you have any questions, concerns or requests regarding this Privacy Policy or your personal data, please do not hesitate to contact us. The responsible entity (Data Controller) for Drinqo is:

Jacob König

1010 Vienna, Austria

Email: jkoenig.project@gmail.com

You can reach out to us via the email above for any privacy-related inquiries — such as asking about your data, requesting deletion, or anything else outlined in the User Rights section. When contacting us about your in-App profile, please include your anonymous user ID (visible in the App's settings) so we can locate your data.

Changes to this Policy

Last Updated: 17 April 2026

This Privacy Policy may be updated from time to time. We will notify you of any significant changes by posting the new policy within the App or on our website and updating the "Last Updated" date. We encourage you to review this policy periodically to stay informed about how we are protecting the personal data we collect. By continuing to use the App after any changes come into effect, you acknowledge the revised policy.