

Privacy Policy – Juqed Web (Account)

Generated on 2026-08-15 from <https://juqed.com/en/legal/privacy-juqed-web>

Privacy Policy – Juqed Web (Account)

This policy applies to the user account at **web.juqed.com**. For your guests joining an event via **go.juqed.com**, the [Juqed Go section](#) continues to apply; for the marketing site juqed.com, see the [website section](#).

As of: 15 August 2026

1. Controller

The controller under the GDPR for the processing of personal data in connection with the user account is the operator named in the [Legal Notice](#).

2. Scope

web.juqed.com provides a host access point that lets you run events straight from your browser: user account and sign-in, creating and managing an event (section 7), and music playback through your own Apple Music account (section 6). Your guests join via **go.juqed.com** as before; the [Juqed Go section](#) applies to them.

Alongside the free tier there are paid tiers. Purchase, payment and invoicing run through our partner **Paddle**; what is processed in doing so is set out in section 8. The conditions of the contractual relationship are in the [Terms for Juqed Web](#), the deadlines and consequences of a withdrawal in the [withdrawal instructions](#).

3. Account and sign-in

Signing in requires **your email address only**. There is no password. Instead we send a six-digit sign-in code to that address; entering it signs you in. An account is created only on the first successful sign-in – entering an address without redeeming the code creates nothing.

The following is stored with your account:

- your email address
- the language detected in your browser (German or English), so our system emails reach you in your language
- the time the account was created and of your last sign-in
- the account's access status and the tier assigned to it
- the time the welcome email was sent – so that a later sign-in does not trigger it a second time

- the time of the **first track played in your account**. It starts the trial period of the free tier and is never changed afterwards; without it, a time-limited trial could be repeated indefinitely simply by creating new events.
- if we have terminated the contract on our side: the time since which no new purchases are possible for your account, and the reason for it (section 9)
- which in-app notices you have already dismissed, and when

The sign-in code itself is never stored in plain text, only as a non-reversible hash (HMAC-SHA256 with a secret key held on the server alone). It expires after ten minutes, can be used only once, and is blocked after five failed attempts. The legal basis is Art. 6(1)(b) GDPR (performance of, or steps prior to, the contract).

We use the same route – a code by email – for two further steps where an unattended signed-in computer would otherwise be enough: **deleting the account** and **the data copy** (section 10). For every code requested we therefore also store its occasion – sign-in, deletion or data copy –, the time it was requested, the time it expires, whether and when it was redeemed, the number of failed attempts, and the language it was sent in. A code for one occasion only invalidates older codes for that same occasion.

Notices inside the application. After you sign in, we occasionally show you a notice about something new or about a change to the service. Who gets to see it is decided from details already held with your account – all accounts, or only those on a particular tier or with beta access (section 12). **No additional data is collected for this, and your behaviour within the application is not analysed.**

When you dismiss a notice, we record with your account that it is done with, so that it does not appear again. That marker sits **on our server, not in your browser** – so dismissing it also takes effect on another computer, and it requires neither a further cookie nor any storage on your device. **We do not measure who saw or clicked a notice**; all that is recorded is which one you closed.

The legal basis is Art. 6(1)(b) GDPR where the notice concerns your contract, and otherwise Art. 6(1)(f) GDPR – our legitimate interest in telling you about what is new while asking exactly once rather than at every sign-in. Should a notice ever promote a paid tier, you may object to that at any time and without giving reasons under Art. 21(2) GDPR; we will then stop it. The markers are deleted with your account.

4. Consents and pre-contractual information

Before an account is created and before every purchase, we present you with the **Terms** and this privacy policy; you consent to both explicitly by ticking a box. The **withdrawal instructions** are also presented to you before a purchase, but are **not** ticked: they are information, not consent.

So that this can be evidenced later, we record with your account the time of your most recent acceptance of the Terms, the version of the Terms you accepted (for example “2026-08-11”), and the time of your consent to this privacy policy. That record would be overwritten by every further acceptance – someone buying in the seventh month would thereby lose the evidence of their acceptance at registration. Each individual occasion therefore also creates its own entry, containing:

- the occasion (registration or purchase)

- the document (Terms, privacy policy or withdrawal instructions)
- whether you consented or whether the text was merely presented to you
- the version of the document
- the time
- a non-reversible hash of your IP address – the address itself is not stored here either

Purpose and legal basis: § 305(2) BGB requires that the Terms were incorporated before the contract was concluded, Art. 246a EGBGB that the withdrawal instructions were provided, and Art. 7(1) GDPR that we can *demonstrate* a consent given. The legal basis is therefore Art. 6(1)(c) GDPR (compliance with these record-keeping duties) and otherwise Art. 6(1)(f) GDPR (legitimate interest in a provable conclusion of contract). These entries are attached to your account and deleted with it.

5. Session cookie

After a successful sign-in we set one strictly necessary cookie so that you stay signed in:

- `juqed_web_session` — contains nothing but a random string with no reference to your person, lifetime 30 days. It is limited to `web.juqed.com` (*HttpOnly, Secure, SameSite=Lax*) and is transmitted neither to `juqed.com` nor to `go.juqed.com`.

On the server side, too, we store not the cookie value itself but only its hash. Alongside the session we record the time it was created, when it expires, when it was last used, the browser identifier (user agent) and a non-reversible hash of the IP address the sign-in came from. The browser identifier is there so that a future device overview can show you which sign-ins are active; the IP hash makes it possible to attribute a session to an origin should something look wrong, without keeping the address itself (Art. 6(1)(f) GDPR). Signing out deletes the session immediately.

No consent is required for this cookie, as it is strictly necessary for the service you explicitly requested (§ 25(2) no. 2 TDDDGD). The legal basis for the processing is Art. 6(1)(b) GDPR. No tracking takes place; Matomo is not embedded on `web.juqed.com`.

6. Music playback through Apple Music

Playback in the browser runs through **Apple Music** and requires your own paid Apple Music subscription. Technically the page loads the **MusicKit JS** library from a server operated by Apple Inc. (`js-cdn.music.apple.com`). That request alone transmits your IP address to Apple.

Signing in with Apple. To start playback you sign in once in a window that Apple itself serves and operates. **We see neither your Apple Account identifier nor your password.** After a successful sign-in, MusicKit stores an access credential for your Apple Music account in your browser (a so-called *Music User Token*). That credential stays on your device; it is neither transmitted to us nor stored by us. It is strictly necessary for the playback you explicitly requested (§ 25(2) no. 2 TDDDGD).

Apple is an independent controller. The audio stream flows directly between your browser and Apple; it does not pass through our servers. In doing so Apple processes the data of your own Apple Music contract – in particular which tracks are played, when and for how long – as its own controller and under

its own privacy policy, available at apple.com/legal/privacy. In this respect we are neither controller nor processor and have no influence on that processing.

Third-country transfer. Apple Inc. is based in the USA. Connecting your Apple Music account transfers data to a third country. The basis for this is your own contractual relationship with Apple; the transfer takes place under the arrangements Apple has put in place for it. If you would rather not, simply do not connect Apple Music – there will be no playback, while your account and the other functions remain usable.

Access to your library. Only if you explicitly choose “*Your own Apple Music playlists*” as the music source does the page read the names of your playlists and the tracks they contain from your Apple Music library. This happens in the browser; we do not store the tracks themselves. The only thing stored on our side is **which playlists you selected** – as identifiers attached to the event, so the selection is available on another computer as well. That entry is deleted together with the event.

The legal basis for the playback function is Art. 6(1)(b) GDPR (performance of the user relationship).

7. Your events

An event you create in the browser belongs to **your account** – unlike in the app, where it is tied to the device. That is the only way to carry it on from another computer. The following is stored for it:

- the event code your guests use to join, and the name you give it
- its status, its type, the chosen country setting of the music catalogue, and the times of creation, expiry and the player's last check-in
- the event's settings (such as music source, language and voting behaviour)
- the open music requests with title, artist, source and number of votes
- the history of tracks already played, with title, artist, source and time
- where you made your own selection, the identifiers of the Apple Music playlists chosen (section 6)

Your guests do not belong here. What go.juqed.com processes about them – their nickname, for instance – is set out in the [Juged Go section](#). In the disclosure about your account (section 16), requests therefore appear without any indication of who made them (Art. 15(4) GDPR).

The legal basis is Art. 6(1)(b) GDPR (performance of the user relationship). The event and everything attached to it is deleted when it ends.

The song list by email. When clearing the history and when ending an event, you can tick a box in the confirmation dialogue to have us send the list of played tracks to your account address – the box is **not pre-selected**. The email contains title, artist and time, **but not the nicknames of your guests**. The list is not kept on our side; we store only **that** an email went out: the event code, the number of tracks, the occasion (history cleared or event ended) and the time. This limits how often our outgoing mail can be used this way (Art. 6(1)(f) GDPR – legitimate interest in the deliverability of our domain) and answers your question of what we sent you and when (Art. 6(1)(c) GDPR in conjunction with Art. 15 GDPR). These entries are deleted with your account.

8. Payment, subscription and one-off purchase (Paddle)

For the paid tiers, the purchase is handled by **Paddle.com Market Limited**, 30 Old Bailey, London EC4M 7AU, United Kingdom. Paddle acts as reseller and merchant of record and is therefore **an independent controller** under the GDPR – not our processor. Payment methods, billing address, VAT details and invoices are held by Paddle alone. **We see neither card details nor bank account.** Paddle's own privacy policy applies to its processing and is available at paddle.com/legal/privacy.

The checkout window is served by Paddle. Opening it loads a script from `cdn.paddle.com` and transmits your IP address to Paddle. In this context Paddle sets its own cookies to run the payment process and to prevent fraud; they are strictly necessary for the purchase you explicitly requested (§ 25(2) no. 2 TDDDG). As long as you buy nothing, nothing is loaded from Paddle.

What we transmit to Paddle: the internal identifier of your account – a sequential number that says nothing about you on its own – as the only bridge between payment and account, plus your email address to pre-fill the form. Nothing else.

What we receive back from Paddle and store:

- for a subscription: the subscription and customer identifiers at Paddle, the identifier and name of the price chosen (week, month or year), the status of the subscription in Paddle's own wording (such as active, payment due, paused, cancelled), the start of the contract as reported by Paddle, the end of the paid period, scheduled changes and the time of a cancellation;
- for a one-off purchase: the time of purchase, the transaction number and – if refunded – the time of the refund. The time of purchase remains on record even after a refund: the refund withdraws the paid tier, but it does not undo the purchase, and without it we would have no answer to “but I did pay”;
- the identifiers of the event notifications delivered by Paddle, so that the same notification is not processed twice;
- a marker recording which billing period we have already sent the renewal reminder for.

A reminder before every renewal. Before a subscription renews automatically, we send you an email stating the date and amount of the next charge and how to cancel. A daily job checks which subscriptions are coming up for renewal; the marker mentioned above prevents the same announcement from going out again on every day of the lead time. The legal basis is Art. 6(1)(b) GDPR, supplemented by Art. 6(1)(f) GDPR (legitimate interest in no one being surprised by a charge).

Purpose and legal basis: this data is required to assign the paid tier to your account, to withdraw it again on expiry or cancellation, and to trigger a refund. The legal basis is Art. 6(1)(b) GDPR (performance of the contract); for the safeguard against double processing, Art. 6(1)(f) GDPR (legitimate interest in error-free operation).

Third-country transfer: Paddle is based in the United Kingdom. The European Commission has found the level of data protection in the United Kingdom to be adequate. Should that decision lapse, the transfer is based on the standard contractual clauses Paddle provides for this purpose.

Test operation: accounts with “beta” access purchase in Paddle's sandbox, a test environment without real payment traffic. No money moves and no payment method is charged. The same data as above is processed.

9. Withdrawal and cancellation

The footer of every page on web.juqed.com carries two buttons that work **without signing in**: “Withdraw from contract” (§ 356a BGB) and “Cancel contracts here” (§ 312k BGB). What you enter there is stored: name, email address, chosen language, which contract it concerns, an optional invoice or transaction number, and the time of receipt.

The name is mandatory because § 356a(2) BGB requires it. We do not otherwise know it and do not keep it with your account – it is part of the declaration and nothing else.

To establish your identity we send a confirmation of receipt containing a one-time link to the address given. We store not the link but only its hash; it expires after a short time. In addition we record when the confirmation of receipt and the reminder were sent, when and by what route identity was established, how the matter ended and – in the case of a withdrawal – which subscription or transaction number the refund was attached to. Anyone declaring while signed in does not need the email loop; the click from the session is itself the proof of identity.

So that the forms cannot be abused to flood other people's mailboxes, your IP address is **not stored**, only kept as a non-reversible hash for throttling.

Legal basis is Art. 6(1)(b) GDPR (performance of the contract) and Art. 6(1)(c) GDPR (compliance with the confirmation and record-keeping duties under §§ 312k, 356a BGB).

If we terminate – for instance by ordinary notice under the Terms – that declaration is recorded in the same form: the type of declaration, your email address, the time, its execution and the outcome. The entire contractual history of an account thus sits side by side on one timeline. In that case we additionally note on your account that no new purchases can be made through it, and the reason for that (section 3) – a termination after which a new subscription could be taken out the next day would have no effect. **Your access is not affected:** sign-in, the data copy and disclosure under Art. 15 GDPR continue to work. Only purchasing is blocked. The legal basis is Art. 6(1)(b) and (f) GDPR.

These declarations survive the deletion of an account. They are legal acts whose receipt we have confirmed to you in text form, and in the case of a withdrawal a refund is attached to them. We therefore retain them within the commercial and tax retention periods (§ 147 of the German Fiscal Code); Art. 17(3)(b) and (e) GDPR cover this. The address given remains in place – it is the content of the declaration, not a reference to an account.

10. Data protection requests

When you start a **data copy** (Art. 15(3), Art. 20 GDPR) or the **deletion of your account** (Art. 17 GDPR) from your account, we record the request itself. Stored for each event are:

- which right it concerned – access and data copy, or erasure
- which step: requested or delivered

- the time
- a non-reversible hash of your IP address – the address itself is not stored here either

What is not stored is the content of the disclosure. The data copy is assembled anew on each request and is never written to disk; an export file left lying on the server would be a data breach with an expiry date.

Purpose and legal basis: Art. 12(3) GDPR gives us one month to respond, and Art. 5(2) GDPR requires that we can *demonstrate* we kept to it. The interval between “requested” and “delivered” is precisely that evidence. Without it, the only trace would be the sign-in code used to confirm the request – and that is cleared away once it expires. The legal basis is therefore Art. 6(1)(c) GDPR in conjunction with Art. 5(2) and Art. 12(3) GDPR.

Retention. These entries are attached to your account and deleted with it. In the case of an erasure, only the request is therefore recorded, not its execution: carrying it out removes the entry along with everything else. Your receipt for it is the confirmation of deletion by email, not an entry that outlives your account – Art. 17 GDPR makes no exception for records that happen to be in our favour.

Requests that reach us by email to the address given in the [Legal Notice](#) are handled in our mailbox; they are not additionally logged in this form.

11. Protection against misuse

So that the sign-in function cannot be abused to flood other people's mailboxes, the number of code requests per address and per sender is capped. For this your IP address is **not stored**, only kept in non-reversible form (as a hash) together with the request in question. The legal basis is Art. 6(1)(f) GDPR (legitimate interest in abuse-free operation).

12. Observation in beta access

Juqed Web offers **beta access**. Accounts with that access can use new features ahead of time and help us put them to the test. As long as your account has that access, the player reports technical events to our server: the start and end of playback, playback errors from Apple Music, an empty playlist, the closing of the browser tab and the playing time reached so far. Browser and operating system are recorded in coarse form (for example “Chrome”, “Windows”).

No content is recorded: no song titles, no search terms, no names of your guests and no IP addresses. The sole purpose is the question whether and for how long a browser survives a whole event, and what makes playback fail.

Legal basis is our legitimate interest in a functioning, low-error service (Art. 6 (1) (f) GDPR). The data is deleted automatically after **90 days**, and immediately when an account is deleted. When your account's beta access ends, this collection ends with it; accounts without beta access are not affected in the first place.

13. Hosting and server log files

web.juqed.com is hosted by **Hetzner Online GmbH**, Industriestr. 25, 91710 Gunzenhausen, Germany; the servers are located in Germany. Hetzner acts as a processor under Art. 28 GDPR; a data processing agreement is in place. The scope and retention period of the server log files match the details under [Privacy Policy \(Website\), section 3](#) (automatic deletion after no more than 14 days).

14. Email delivery

Sign-in codes and other system messages are sent from `noreply@juqed.com` via the outgoing mail server of **Hetzner Online GmbH** (processor under Art. 28 GDPR), TLS-encrypted. Your address is not passed on to third parties for advertising purposes; there is no newsletter.

The only messages sent to your address are those belonging to a specific step. These are the ones that arise in normal operation:

Account and sign-in (section 3):

- the sign-in code
- the welcome email after your first sign-in
- the code confirming an account deletion
- the code confirming a data copy
- the confirmation that your account has been deleted

Event (section 7):

- the song list of an event – only if you ticked the box

Purchase and subscription (section 8):

- the confirmation of a one-off purchase
- the confirmation of a subscription taken out
- the reminder before every automatic renewal
- the notice of a failed payment
- the notice that a subscription is ending for want of payment
- the confirmation that you have cancelled your subscription

Withdrawal and cancellation (section 9):

- the confirmation of receipt of a withdrawal
- the confirmation of receipt of a cancellation
- the reminder when your confirmation via the link is still outstanding
- the notice that no contract exists for your address
- the notice that the withdrawal period had already expired
- the notice that your withdrawal has been carried out
- the notice that your cancellation has been carried out

- our own termination, where we end the contract

Important notices about your running contract. Beyond the list above, we reserve the right to write to you where something material changes about a running contract – for instance a new version of the Terms or of the prices, a restriction or discontinuation of the service, an outage affecting an event you have coming up, or an incident touching the security of your data. This happens **only in such exceptional cases** and not at regular intervals: a change to your contract that you never hear about would leave you worse off.

This is not advertising. Such notices contain **no promotional content whatsoever** and are not advertising within the meaning of § 7 UWG (German Act Against Unfair Competition). This route brings you no newsletter, no product announcement, no offer of a higher tier and no reminder about unused features. It is confined to what you need to know about your own contract.

The legal basis is Art. 6(1)(b) GDPR: informing you about your own contract forms part of performing it. Where a notice is required of us by law – such as advance notice of amended conditions, or notification under Art. 34 GDPR of a breach affecting your personal data – Art. 6(1)(c) GDPR applies in addition. Because these messages are part of the contractual relationship, they cannot be unsubscribed from individually while the contract runs; there is no right to object under Art. 21 GDPR in this respect, as we do not rely on a legitimate interest for them. They end when the contract ends.

Legal texts as attachments. The welcome email carries the Terms as a PDF, purchase confirmations additionally the withdrawal instructions, and the emails around a withdrawal likewise the withdrawal instructions. The reason is § 312f(2) BGB: what you are meant to keep has to reach you on a durable medium – a link will not do, because the content behind it can be changed at any time.

Archive copy. Of those system emails that evidence a contractual or account step – purchase and subscription messages, the renewal reminder, withdrawal, cancellation, termination by us, and the confirmation of deletion – a blind copy is additionally sent to an archive mailbox at juqed.com. It serves as proof that the email was sent and with what content (Art. 6(1)(c) GDPR in conjunction with §§ 312f, 356a BGB, supplemented by Art. 6(1)(f) GDPR). **Not copied** are the sign-in code, the codes for deletion and the data copy, and the song list – there is nothing to evidence there, and a copy would be an added risk without a purpose.

15. Retention and deletion

- **Sign-in codes:** they expire after ten minutes and are deleted automatically no later than 24 hours after expiry.
- **Sessions:** they end after 30 days at the latest and are deleted then; immediately when you sign out.
- **Dismissed in-app notices (section 3):** the marker is attached to your account and deleted with it.
- **Consents and pre-contractual information (section 4):** attached to your account and deleted with it.
- **Events including settings, requests and history (section 7):** deleted when the event in question ends, at the latest with your account.

- **Log of song lists sent (section 7):** attached to your account and deleted with it. The list itself is never stored in the first place.
- **Subscription and purchase data (section 8):** attached to your account and deleted with it. Your invoices are held by Paddle and subject to its own statutory retention periods.
- **Event notifications from Paddle:** 90 days, deleted automatically afterwards.
- **Withdrawal and cancellation declarations (section 9):** they survive the deletion of an account and are deleted once the commercial and tax retention periods have elapsed.
- **Data protection requests (section 10):** attached to your account and deleted with it.
- **Archive copies of contract emails (section 14):** retained within the commercial and tax retention periods (§ 147 of the German Fiscal Code).
- **Apple Music credential:** it lives in your browser only. Use “Disconnect Apple Music” in your account, or clear the site data in your browser, to remove it; it was never stored with us.
- **Your playlist selection:** it is attached to the event and deleted together with it.
- **Beta log:** 90 days from each event, deleted automatically afterwards (see section 12).
- **Account:** it remains for as long as you wish to use it. You can delete it yourself at any time: “Delete account” in your account, confirmed with a code we send you by email. This removes your email address, your sessions, your subscription and purchase data and any running event including its playlist, history and guest requests; a running subscription is cancelled in the process. A request to the address named in the [Legal Notice](#) works just as well. You will receive a confirmation of deletion by email.

16. Your rights

Under the GDPR, you have the following rights: access (Art. 15), rectification (Art. 16), erasure (Art. 17), restriction of processing (Art. 18), objection (Art. 21) and data portability (Art. 20). For requests, please contact the email address listed in the [Legal Notice](#).

You can get a copy of your data without going through us: in your account under “Your data”, use “Request a data copy” for a disclosure under Art. 15(3) and Art. 20 GDPR, confirmed with a code by email. You can view it on the page or download it as a file. It does not include the billing and payment data held by Paddle (section 8) – you get those from Paddle – nor details concerning other people, such as your guests' nicknames (Art. 15(4) GDPR). Access credentials such as code and session hashes are not included either; the copy does state that they exist and since when. The fact that you requested a data copy or an erasure is also part of it (section 10).

You also have the right to lodge a complaint with the competent data protection supervisory authority. The competent authority is the **State Commissioner for Data Protection and Freedom of Information of North Rhine-Westphalia (LDI NRW)**, Postfach 20 04 44, 40102 Düsseldorf, www.ldi.nrw.de.

17. Changes

This privacy policy will be adjusted as soon as the scope of Juqed Web changes. The current version is available at juqed.com/en/legal/privacy-juqed-web.

Provider identification pursuant to § 5 DDG (German law)

Legal Notice (Impressum)

As of: July 10, 2026

Information pursuant to § 5 DDG

Michael Hankemann

Zum Gehölz 2
45731 Waltrop
Germany

Email: mail@juqed.com

This legal notice covers all of the operator's offerings: **juqed.com** (website), **go.juqed.com** (Juqed Go guest page) and **web.juqed.com** (host access with user account), as well as the Juqed and Juqed Go apps. The applicable privacy policy for each is available under [Legal](#).

Responsible person pursuant to § 18 (2) MStV

Michael Hankemann, Zum Gehölz 2, 45731 Waltrop, Germany

VAT identification number

VAT identification number pursuant to § 27a of the German VAT Act (Umsatzsteuergesetz):
DE463506983

Note: The Juqed app is distributed exclusively through the Apple Mac App Store. Apple Inc. acts as Merchant of Record and is responsible for processing the purchase, including its tax treatment.

Dispute resolution

The operator is neither willing nor obliged to participate in dispute resolution proceedings before a consumer arbitration board (§ 36 VSBG).

Liability for content

The contents of this site have been created with the greatest care. However, no guarantee can be given for the accuracy, completeness or currency of the contents. As a service provider, the operator is responsible under § 7 (1) DDG for own content on these pages in accordance with general laws.

Liability for links

This website contains references to external third-party websites (Apple Mac App Store, Hetzner Online GmbH, LDI NRW) over whose content we have no influence. The respective provider is always responsible for the contents of linked pages. Should we become aware of any legal violations, the

corresponding links will be removed promptly.

Copyright

The content and works on this site created by the operator are subject to German copyright law.

Duplication, processing, distribution and any form of exploitation outside the limits of copyright require the written consent of the author. Juqed assumes no responsibility for the music content played through the app. The host is responsible for complying with copyright in their own music collection.