Heyblocks — Privacy Policy (valid until 2026-08-01)

1. Controller

Controller within the meaning of the General Data Protection Regulation (GDPR):

Heyblocks

Sole proprietorship

Helene-Junghans-Str. 43/1, 78713 Schramberg

E-mail: info@heyblockslabs.com

Responsible for content pursuant to Section 18(2) MStV: Justin Hofmann,

Helene-Junghans-Str. 43/1, 78713 Schramberg

2. Data protection at a glance

General information

The following information provides a simple overview of what happens to your personal data when you use our application. Personal data is any data by which you can be personally identified.

Data collection

Some of the data is collected in order to ensure the error-free provision of the application. Other data is collected when you provide it to us in the course of registration, use, or contact. Uploaded content (audio files, video files, texts, URLs) is transmitted to external AI service providers for processing (see Section 5). When you use the research function, web searches are carried out via an external search service (see Section 5.4).

Your rights

You have the right at any time to obtain free information about the origin, recipients, and purpose of your stored personal data. You also have the right to rectification, deletion, or restriction of the processing of this data. In addition, you have the right to lodge a complaint with the competent supervisory authority.

3. General information on data processing

As a matter of principle, we process the personal data of our users only insofar as this is necessary to provide a functional web application as well as our content and services. Heyblocks is currently available exclusively as a web application (browser). A mobile app or desktop application is currently not offered.

4. Hosting & infrastructure

4.1 Hosting via Railway

Our application is operated via the service Railway Corp. The application runs

in Docker containers on servers in the Netherlands (EU).

The following data may be processed in this context:

- IP address
- Browser and device information
- Request headers
- Log files

Legal basis: Art. 6(1)(f) GDPR (legitimate interest in the

secure and efficient provision of our application).

4.2 Railway Redis (rate limiting)

To protect against abusive use (e.g. brute-force attacks,

excessive API calls), we use a Redis service provided via

Railway Corp.

The following data is temporarily stored in this context:

- IP address (anonymized key) or user ID
- Timestamps of the requests

The data is used exclusively to enforce request limits and is

automatically deleted after the respective time window has elapsed (generally a few minutes up to a maximum of

24 hours).

Legal basis: Art. 6(1)(f) GDPR (legitimate interest in the

security and integrity of the application).

4.3 Cloudflare (database & DNS)

We use Cloudflare Inc. as our infrastructure and database service provider. User data is

stored in a Cloudflare D1 database.

The following data may be processed in this context:

- Account data (e-mail, username, encrypted password, Google ID)
- Created notes, transcripts, and generated tab content
- Usage statistics (token consumption, generation duration, costs)
- Subscription tier, usage quotas, and transaction history

Cloudflare is engaged as a processor. Insofar as data is transmitted to third countries (e.g.

the USA), this is done on the basis of the standard contractual clauses.

Legal basis: Art. 6(1)(b) GDPR and Art. 6(1)(f) GDPR.

4.4 Cloudflare Turnstile (bot protection)

To protect against automated attacks and abuse (e.g. during payment transactions),

we use Cloudflare Turnstile. Turnstile is a CAPTCHA service from Cloudflare Inc.

that checks, without visible interaction or by means of a simple click, whether a

request originates from a real user.

The following data may be processed in this context:

- IP address
- Browser and device information
- Interaction data (mouse movements, click behavior)

The data is processed by Cloudflare to distinguish between human users and bots.

No personal account data is transmitted to Turnstile.

Legal basis: Art. 6(1)(f) GDPR (legitimate interest in the

security of the application and the prevention of fraud).

4.5 Tigris Object Storage (media files & source files)

Uploaded and processed files are stored with Tigris Data Inc. (S3-compatible

object storage). Files are stored under a user- and note-specific path.

- Audio and video files
- Documents and image files uploaded as a source (e.g. PDF, images)

Extensive transcript and source texts that exceed the storage limit of the database

are offloaded as a text file (canonical storage of the respective text)

Access to stored audio files is provided via time-limited, signed URLs

(validity: 4 hours).

Legal basis: Art. 6(1)(b) GDPR (performance of a contract).

5. AI-supported processing

5.1 Groq Inc. (transcription & content generation)

Heyblocks uses AI services from Groq Inc. (Mountain View, USA)

to process your content.

Speech recognition: Uploaded audio and video files are transmitted to

Groq's speech-to-text API in order to perform an automatic transcription.

The file is transmitted to Groq in full in this process.

Content generation: The generated transcript text is transmitted to an

AI language model via Groq in order to generate structured content from it

(e.g. summaries, notes, custom tabs).

According to Groq's terms of use, data transmitted via the API is

not used to train models.

Since Groq is based in the USA, a transfer of data to a third country takes place.

The transfer is based on the European Commission's standard contractual clauses (Module 2)

as well as an accompanying transfer impact assessment (TIA). A certification under the

EU-U.S. Data Privacy Framework does not currently exist.

Legal basis: Art. 6(1)(b) GDPR (performance of a contract –

the AI processing is a core component of the service).

5.2 OpenAI Inc. (content generation)

Heyblocks uses AI services from OpenAI Inc. (San Francisco, USA) for content generation in both modes (Fast and Pro).

Content generation: The transcript text is transmitted to an AI language model from OpenAI in order to generate structured content from it (e.g. summaries, notes, custom tabs, flashcards, quiz questions).

Data transmitted to Groq/OpenAI	Not transmitted
Audio/video files (for transcription, Groq only)	E-mail addresses or account data
Transcript text (for content generation)	Payment information
Tab labels (for content generation)	Users' IP addresses

According to OpenAI's terms of use, data transmitted via the API is not used to train the models, unless the customer expressly consents.

We have not consented to this.

Since OpenAI is based in the USA, a transfer of data to a third country takes place.

The transfer is based on the European Commission's standard contractual clauses (Module 2) as well as an accompanying transfer impact assessment (TIA). OpenAI is not certified under the EU-U.S. Data Privacy Framework; the transfer is therefore based exclusively on the standard contractual clauses.

Legal basis: Art. 6(1)(b) GDPR (performance of a contract – the AI processing is a core component of the service).

5.3 Automated content review (content safety)

Before processing by AI models, the transcript text is automatically checked for possible violations of our content policies. For this purpose, the transcript text is transmitted to a safety model from Groq Inc. In the case of exceptionally long transcripts, the part that exceeds the technical processing limit of the safety model is additionally transmitted to the moderation service of OpenAI Inc. (San Francisco, USA).

This review serves to protect against abusive content (e.g. glorification of violence, hate speech, illegal content) as well as against attempts to manipulate the AI systems (prompt injection).

No personal account data is transmitted to the safety or moderation services – only the content to be reviewed (transcript text or image).

Image moderation: Image files uploaded as a source are transmitted to the moderation service of OpenAI Inc. (San Francisco, USA) before further processing, in order to automatically check them for violations of our content policies. Transmitted is exclusively the respective image file, no account data. Since OpenAI is based in the USA, the transfer is based on the European Commission's standard contractual clauses.

Legal basis: Art. 6(1)(f) GDPR (legitimate interest in the security and integrity of the application as well as protection against unlawful content).

5.4 Serper Inc. (web search – research function)

When you use the research function, search queries are transmitted to the service Serper Inc.

in order to carry out web searches and find relevant sources.

The following data is transmitted in this context:

- Search terms (the research topic entered by the user)

No personal account data, e-mail addresses, or IP addresses of the users are transmitted to Serper. The search results (URLs and titles) are subsequently retrieved and processed server-side.

Legal basis: Art. 6(1)(b) GDPR (performance of a contract – the research function is a component of the service).

5.5 Supadata (YouTube transcripts)

For the extraction of transcripts and metadata from YouTube videos, Heyblocks uses the service Supadata. In this process, only the YouTube video URL is transmitted to Supadata. No personal data of the users is passed on to Supadata.

Legal basis: Art. 6(1)(b) GDPR (performance of a contract).

6. User accounts & registration

The creation of a user account is required in order to use the application.

6.1 Registration via e-mail and password

When you register via e-mail and password, we process:

- E-mail address
- Username

Password (stored exclusively as a cryptographic hash using Argon2; for older existing accounts, bcrypt is used and is automatically migrated to Argon2 at the next sign-in. The plaintext password is not stored.)

6.2 Registration / login via Google (OAuth)

Alternatively, you can sign in via your Google account. In this process, we receive from Google:

- E-mail address
- Name
- Google user ID
- Profile picture URL

Authentication is carried out via the service „Google Identity Services“ from Google Ireland Limited. We do not receive any Google password and no access to further Google account data.

Legal basis: Art. 6(1)(b) GDPR (performance of a contract).

6.3 Session management

After a successful sign-in, a JSON Web Token (JWT) is created and stored as an HttpOnly cookie in the browser. This cookie:

- contains exclusively the user ID and an expiry time
- cannot be read out via JavaScript (HttpOnly)
- is transmitted only over encrypted connections (Secure flag)
- has a validity of 7 days

Legal basis: Art. 6(1)(f) GDPR in conjunction with Section 25(2) TDDDG (technically necessary cookie).

7. Processed usage data

7.1 Source files

Audio and video files uploaded by the user are:

- temporarily stored on the server (for processing)
- transmitted to Groq for transcription (see Section 5)
- stored in Tigris Object Storage (see Section 4.5)
- deleted from the server after processing is complete

automatically deleted from object storage as soon as the associated note is removed,

but no later than around 30 days. Uploads flagged as non-compliant are

retained within this period for moderation review. The transcript remains

unaffected by this and stored in the database.

URLs and texts added by the user are extracted server-side and stored as source text in the database. Documents and image files uploaded as a source are also processed, and the extracted text is stored as source text (see Section 4.5). Web sources collected via the research function are also stored as source text.

7.2 Generated content

The following AI-generated content is stored in our database:

- Transcripts
- Automatically generated title
- Summary
- Custom tab content (e.g. bullet points, vocabulary, etc.)
- Flashcards (question/answer pairs) for spaced repetition
- Quiz questions including answer options

7.3 Usage statistics

For internal cost calculation, billing, the enforcement of the usage limits of

your plan, and to monitor the technical performance of the service (e.g. average

and worst-case generation times), we store per generation:

- Number of tokens consumed (input and output)
- Duration of the audio file
- Generation duration
- Calculated API costs (internal, not evaluated on a personal basis)
- Usage time consumed (minutes)

Legal basis for the above: Art. 6(1)(b) GDPR (performance of a

contract – metering and billing the plan you booked), and, as far as these

records are evaluated in aggregate for internal cost analysis and technical performance monitoring, Art. 6(1)(f) GDPR (legitimate interest in an economically viable, stable, and fast service). Because the metering records are required to provide the service itself, they cannot be switched off; they are deleted when your account is deleted (Section 12). You can object to the aggregate evaluation at any time under Art. 21 GDPR using the contact details in Section 1.

In addition, to understand which functions are actually used and to improve them, we record when you export a generated set (e.g. flashcards to Anki). We store only the export format, the note concerned, and the time – never the exported content itself. This evaluation is internal, is not passed on to third parties, and no profiling takes place. These entries are deleted automatically after 30 days at the latest. You can object to this recording at any time in your account settings (option „Data collection“); no further entries linked to your user ID will then be stored.

Legal basis for the export records: Art. 6(1)(f) GDPR (legitimate interest in the needs-based further development and improvement of our own functions).

7.4 Blueprints

Users can create „Blueprints“ (templates) that contain tab labels.

These are stored server-side in the database.

Legal basis: Art. 6(1)(b) GDPR (performance of a contract).

7.5 Learning data (flashcards & quiz)

If you use the learning functions, we store the following to provide the repetition and progress logic:

Flashcard repetitions: your self-assessment per card as well as the scheduling data calculated from it for the next repetition (spaced repetition algorithm) and the associated timestamps

Quiz attempts: score achieved, number of questions, and time of the attempt

Legal basis: Art. 6(1)(b) GDPR (performance of a contract – provision of the learning functions).

7.6 Blueprint store (publishing templates)

Users can voluntarily publish their self-created blueprints in the „Store“ in order to make them available to other users. Publication takes place exclusively upon your active initiative.

Upon publication, the following data becomes visible to all users:

- Name of the blueprint and its tab labels
- Your username (as author of the blueprint)
- Number of installations

You can remove a published blueprint from the store again at any time by deleting the underlying blueprint.

Legal basis: Art. 6(1)(a) GDPR (consent through active publication).

7.7 Sharing notes

Users can voluntarily share individual notes with others. Sharing takes place exclusively upon your active initiative and can be revoked at any time.

Two modes are available:

Public link: anyone who has the link can view the shared note (title, tab content, and your username as the author). The link contains a randomly generated, non-guessable token; the note is not otherwise listed or discoverable.

Specific people: the note is accessible only to the e-mail addresses you specify. Those recipients must sign in with the invited e-mail address in order to view the note.

When you share a note, the following data is processed:

the e-mail addresses of the people you invite (in the „specific people“ mode), stored in order to control access – these may be addresses of persons who are not themselves users;

- the shared content (title, tabs), which becomes visible to the respective recipients;
- your username, which is shown to recipients as the author of the shared note.

In the „specific people“ mode, we send a one-time invitation e-mail to each newly added address (see Section 8a). Recipients can add a shared note to their own library; this creates an independent copy in their account. You can stop sharing at any time by removing the share – the link then stops working immediately – and deleting the note also removes the share.

Legal basis: Art. 6(1)(a) GDPR (consent through active sharing); for the invitation e-mails additionally Art. 6(1)(f) GDPR (legitimate interest in enabling the sharing requested by the user).

7.8 Flashcard reminder e-mails (opt-in)

Optionally, you can activate e-mail reminders that notify you when saved flashcards are due for repetition. This function is deactivated by default and is used only after your active consent (opt-in) –

via the toggle in the settings or the corresponding prompt during a study session.

When activated, we process the following data:

your notification setting (activated/deactivated) and the time of the last reminder sent (to ensure at most one reminder per day);

a coarse regional send window („Asia-Pacific“, „Europe/Middle East/Africa“, or „Americas“), derived once from your browser's UTC offset at the moment of activation so that reminders arrive at a reasonable local time. Only this three-value region is stored – never your precise time zone or location – and it is used exclusively for send timing.

Each reminder e-mail contains the number of due flashcards, the titles of the affected notes, and your username; dispatch is handled by our e-mail service provider (see Section 8a). Every reminder contains an unsubscribe link that works without logging in; you can also deactivate the reminders at any time in the settings. Upon deactivation – by either route – the stored send window is deleted immediately; the setting and the timestamp are deleted at the latest with the user account.

Legal basis: Art. 6(1)(a) GDPR (consent). You may withdraw your consent at any time with effect for the future (Art. 7(3) GDPR) via the settings or the unsubscribe link.

8. Payment processing

For paid services (e.g. concluding and managing subscriptions), we use the payment service provider Stripe Inc. Stripe processes personal data on its own responsibility in accordance with Stripe's respective applicable data protection provisions. We do not receive any complete payment information (e.g. credit card numbers) from Stripe.

After a successful payment, we receive from Stripe exclusively:

- a confirmation of the transaction
- the selected subscription tier and the billing period

Legal basis: Art. 6(1)(b) GDPR (performance of a contract).

8a. E-mail dispatch

For sending transactional e-mails (e.g. welcome e-mail after registration, replies to contact requests, one-time invitation e-mails when you share a note with specific e-mail addresses, and – only with your consent – reminder e-mails about due flashcards, see Section

7.8), we use the service Resend Inc.

The following data is transmitted to Resend in this context:

- E-mail address of the recipient
- Content of the e-mail (e.g. welcome text, support reply)

Resend processes this data exclusively for the purpose of e-mail delivery.

Since Resend is based in the USA, the transfer is carried out on the basis of the

European Commission's standard contractual clauses.

Legal basis: Art. 6(1)(b) GDPR (performance of a contract) and

Art. 6(1)(f) GDPR (legitimate interest in communicating with users); for the

flashcard reminder e-mails Art. 6(1)(a) GDPR (consent, see Section 7.8).

---

9. Cookies & consent

Our application uses the following cookies:

Cookie | Purpose | Type | Validity
heyblocks_session | Authentication (JWT token) | Technically necessary | 7 days
heyblocks_consent | Storage of cookie consent preferences | Technically necessary | 365 days

The session cookie and the consent cookie are technically necessary and do not require

separate consent pursuant to Section 25(2) TDDDG.

Additionally, the following cookies may be set, provided that you

expressly consent:

Cookie | Purpose | Type | Provider
_gcl_*, _gac_* | Google Ads conversion tracking | Marketing (consent required) | Google LLC

On your first visit to our application, you are asked for your consent via a cookie banner.

There you can choose between the following options:

- Accept all – Essential and marketing cookies are activated.
- Essential only – Only technically necessary cookies are set. No tracking.
- Manage settings – You can individually enable or disable specific cookie categories.

Marketing cookies (Google Ads conversion tracking) are loaded exclusively after

your express consent. Without consent, no

tracking takes place.

Legal basis: Essential cookies: Art. 6(1)(f) GDPR

in conjunction with Section 25(2) TDDDG. Marketing cookies: Art. 6(1)(a) GDPR

in conjunction with Section 25(1) TDDDG (consent).

10. Personalization

Personalization functions (e.g. language settings, theme preferences) are

currently stored exclusively locally in the browser (localStorage). No server-side

evaluation or profiling takes place.

11. Analysis & tracking

11.1 Google Ads conversion tracking

We use the service Google Ads Conversion Tracking from Google LLC (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; hereinafter „Google“).

Important: Google Ads tracking is activated exclusively after your express consent via our cookie banner. Without your consent, no tracking scripts are loaded and no cookies from Google are set.

If you have consented, a cookie is set on your device when you reach our application via a Google ad. With the help of this cookie, we and Google can determine whether a user, after clicking on an ad, carried out a specific action (registration, generation of a note).

The following data may be processed in this context:

- Cookie identifier (anonymized)
- Information about the page visited
- Date and time of the visit

Conversion events, namely completed registration and the successful generation of a note. Only the fact that the event occurred is transmitted – never the content of your notes, recordings, or files.

The information generated by the cookie is generally transmitted to a Google server in the USA and stored there. Google is certified under the EU-U.S. Data Privacy Framework; the transfer is additionally based on the European Commission's standard contractual clauses.

You can withdraw your consent at any time by changing your cookie settings in the application or deleting your cookies. In addition, you can disable the collection via the Google Ads settings manager or at www.aboutads.info.

Legal basis: Art. 6(1)(a) GDPR (consent) in conjunction with Section 25(1) TDDDG.

11.2 Log and diagnostic data

To ensure security, for error analysis, and to defend against abuse, we store server-side application logs in our database (see Section 4.3).

These logs serve exclusively the operation and security of the application; no profiling or advertising evaluation takes place.

The following data may be processed in this context:

- IP address exclusively in pseudonymized form (salted hash, never in plaintext)
- Browser/device identifier (user agent)
- User ID (if signed in)
- Path accessed, HTTP method, and response status
- Error information (error type, technical error message)
- Processing duration and size of the request

Right to object: You can object to user-related logging in your account settings (option „Data collection“). If this is disabled, no further logs that are linked to your user ID are stored. For compelling security reasons (e.g. defending against attacks), technically necessary, non-account-related logs may still be generated. Log data is automatically deleted after 90 days.

Legal basis: Art. 6(1)(f) GDPR (legitimate interest in the security, stability, and error-free operation of the application).

12. Storage period & deletion

Personal data is stored only for as long as is necessary for the respective purposes:

Type of data	Storage period
User account	Until deletion by the user; final deletion 30 days after account deletion
Audio/video files	Until deletion of the associated note, at the latest after approx. 30 days
Source files (documents, images)	Until deletion of the associated note by the user
Notes, transcripts, tabs	Until deletion by the user
Learning data (flashcards, quiz, repetition and attempt history)	Until deletion of the associated note or the user account
Flashcard reminder settings (notification setting, regional send window, time of last reminder)	Send window: deleted immediately upon deactivation/unsubscribe; setting and timestamp: until deletion of the user account
Usage statistics	Until deletion of the user account
Export events (Section 7.3)	Automatically after 30 days at the latest
Blueprints	Until deletion by the user
Application logs (diagnostic data, see 11.2)	90 days
Violation logs (automated content review)	Until deletion of the user account
Note shares (share links, invited e-mail addresses)	Until the share is removed by the user, the note is deleted, or the user account / all data is deleted
Server log files (hosting/Railway)	7–30 days
Backups	Maximum 30 days

When a note is deleted, the associated audio file is removed from the object storage (Tigris).

13. Data security

We employ the following technical and organizational security measures:

- Encrypted data transmission (TLS/HTTPS) with HSTS preloading
- Content Security Policy (CSP) to protect against cross-site scripting (XSS)
- HttpOnly cookies to protect session data from JavaScript access

Passwords are stored exclusively as cryptographic hashes (Argon2 for new accounts; bcrypt for existing accounts with automatic migration)

- Audio files are accessible only via time-limited, signed URLs
- The application runs in isolated Docker containers with restricted permissions
- Input validation and path checking to protect against injection attacks
- CSRF protection through origin/referer validation on all modifying API requests

- Rate limiting on all sensitive endpoints to protect against brute-force attacks

14. Third-country transfer

The following service providers based in the USA are used:

Service provider | Purpose | Safeguard
Groq Inc. | AI transcription & content generation | Standard contractual clauses (Module 2) + TIA
OpenAI Inc. | AI content generation, image & text moderation | Standard contractual clauses (Module 2) + TIA
Cloudflare Inc. | Database, DNS, security | Standard contractual clauses, EU-U.S. Data Privacy Framework
Stripe Inc. | Payment processing | Standard contractual clauses, EU-U.S. Data Privacy Framework
Railway Corp. | Hosting, Redis (rate limiting) | Standard contractual clauses
Tigris Data Inc. | File storage | Standard contractual clauses
Google LLC | OAuth authentication, Google Ads conversion tracking (only with consent) | Standard contractual clauses, EU-U.S. Data Privacy Framework
Resend Inc. | Transactional e-mail dispatch | Standard contractual clauses
Serper Inc. | Web search (research function) | Standard contractual clauses
Supadata | YouTube transcripts & metadata | Standard contractual clauses

The currency of the DPF certifications is regularly checked via

dataprivacyframework.gov.

Should a certification lapse, we base the transfer

exclusively on standard contractual clauses in conjunction with a transfer impact assessment.

15. Rights of data subjects

Within the framework of the applicable statutory provisions, you have the following rights:

- Access to your stored personal data (Art. 15 GDPR)
- Rectification of inaccurate or incomplete data (Art. 16 GDPR)
- Deletion of your data (Art. 17 GDPR)
- Restriction of processing (Art. 18 GDPR)
- Data portability (Art. 20 GDPR)
- Objection to processing (Art. 21 GDPR)

Insofar as processing is based on your consent, you can withdraw it at any time with

effect for the future. You can carry out the withdrawal of cookie consent

at any time via the cookie settings in the application.

In addition, you have the right to lodge a complaint with a

data protection supervisory authority, in particular in the Member State of your

habitual residence or the place of the alleged infringement.

The supervisory authority responsible for us is:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

Lautenschlagerstraße 20, 70173 Stuttgart

Telephone: +49 (0) 711 / 615541-0

E-mail: poststelle@lfdi.bwl.de

Web: www.baden-wuerttemberg.datenschutz.de

Requests can be made at any time via the contact details provided in the legal notice.

15a. Automated decision-making (Art. 22 GDPR)

Heyblocks employs an automated content review (content safety) that checks uploaded content for violations of our usage policies before processing (see Section 5.3). This review can result in content being automatically rejected or, in the case of repeated violations, access to the service being restricted (warning system).

How it works: An AI model evaluates a section of the transcript text with regard to possible violations (e.g. glorification of violence, hate speech, illegal content, prompt injection). If a violation is detected, processing is rejected and an entry is created in the warning system. After repeated violations, access to the service may be temporarily or permanently restricted.

Significance and consequences: An automatic rejection prevents the generation of content for the material in question. In the case of repeated violations, the user account may be blocked.

Right to contest: You have the right to contest an automated decision and to request a review by a natural person.

To do so, please contact us by e-mail at info@heyblockslabs.com, stating the relevant case.

Legal basis: Art. 6(1)(f) GDPR (legitimate interest in the security and integrity of the application as well as protection against unlawful content).

A data protection officer has not been appointed pursuant to Art. 37 GDPR, since the conditions for the appointment obligation are not met (no extensive processing of special categories of data, no extensive systematic monitoring).

16. Newsletter

We currently do not offer a newsletter. Should a newsletter be offered in the future, it will be sent exclusively on the basis of your express consent. The optional flashcard reminder e-mails (Section 7.8) are not a newsletter; they too are sent exclusively on the basis of your express consent.

---

17. Changes to this Privacy Policy

We reserve the right to amend this Privacy Policy in order to adapt it to changed legal requirements or new functions. The current version is always available in the application.