

ENTWURF — Rechtsverbindlichkeit erst nach anwaltlicher Prüfung.

Dieses Dokument ist ein KI-gestützter, sorgfältig recherchierter Entwurf für die EduKI GmbH. Es ersetzt **keine** Rechtsberatung. Vor dem Produktivgang ist es durch eine:n in Deutschland zugelassene:n Rechtsanwält:in bzw. eine:n Datenschutzbeauftragte:n zu prüfen und auf die tatsächlichen Verhältnisse der EduKI GmbH anzupassen.

DRAFT — legally binding only after review by qualified counsel.

This document is an AI-assisted, carefully researched draft for EduKI GmbH. It is **not** legal advice. Before production use it must be reviewed by a lawyer admitted in Germany and/or a data protection officer and adapted to EduKI GmbH's actual circumstances.

Dokument / Document: Cookie-Richtlinie & Einwilligung / Cookie Policy & Consent **Version:** 0.1 (Entwurf / draft) **Stand / As of:** 2026-06-03 **Verantwortlich / Owner:** EduKI GmbH

1. Controller and scope

The controller within the meaning of Art. 4(7) GDPR and the entity responsible for the use of cookies and comparable storage technologies under § 25 TDDDG (German Telecommunications Digital Services Data Protection Act; formerly TTDSG) is:

EduKI GmbH

{{EduKI GmbH — Anschrift / registered address}}

{{Registergericht + HRB-Nr. / register court + commercial-register no.}}

Represented by: {{Geschäftsführer:in / managing director(s)}}

Phone: {{Telefon}}

E-mail: {{E-Mail allgemein}}

Data-protection contact: {{datenschutz@... / privacy contact e-mail}}

Data protection officer: {{Datenschutzbeauftragte:r — Name+Kontakt ODER „nicht bestellt“}}

EduKI GmbH is an independent IT-training business and operates the AI-assisted operating platform "**Educas**," through which it runs its own business processes as an IT-training provider. It is the controller within the meaning of Art. 4(7) GDPR for the processing described below in the course of its training business. This Cookie Policy applies to all web interfaces of the Educas platform operated by EduKI GmbH, namely

- the public **landing pages** (marketing/course pages), and
- the internal **portal/staff interfaces** (login area for staff and authorised users).

It supplements EduKI GmbH's general Privacy Policy; in all other respects the statements made there apply (in particular regarding data-subject rights, retention, and recipients).

2. What cookies and client-side storage are

Cookies are small text files that your browser stores when you access a website and sends back to the server on subsequent requests. They make it possible to recognise a browser across multiple requests — for example to keep a signed-in session alive, or to associate a submitted form with the corresponding request.

In addition, web applications can store information in the browser via **local storage** (**localStorage/sessionStorage**). Unlike cookies, this data is not automatically transmitted to the server with every request, but is read only client-side via JavaScript.

§ 25(1) TDDDG covers both the **storing of information** in your terminal equipment (your device) and **access** to information already stored there. In principle, both are permitted only with your consent — unless the operation is exceptionally exempt from consent under § 25(2) TDDDG (see § 5).

Note on local storage: To provide its functions, the Educas platform uses exclusively the cookies listed in § 3. There is **no** use of **localStorage/sessionStorage** beyond this for measurement, tracking, or marketing purposes. {{TODO: confirm whether the frontend uses **localStorage/sessionStorage** for purely functional purposes (e.g. UI state); if so, identify it here as technically necessary.}}

3. Overview of all cookies used

The table below lists **every** cookie set by the Educas platform. All cookies are **first-party cookies** (set exclusively from EduKI GmbH's domain) and are delivered with the **Secure** attribute (transmission only over encrypted HTTPS connections). The **SameSite** attribute depends on the cookie: the three landing-page cookies (**__Host-lp_visitor**, **__Host-lp_at**, **__Host-lp_csrf**) are set with **SameSite=Strict** (no transmission on cross-site requests), whereas the session cookie **session_token** is set with **SameSite=Lax** (transmitted on cross-site top-level navigation, so that an existing sign-in is preserved when you follow a link into the protected area). With the exception of the CSRF cookie (see § 4), all cookies are additionally **HttpOnly** (not readable by client-side JavaScript). The exact attributes set for each cookie are shown per cookie in the "Attributes" column. The values stated here reflect the setting currently configured in code; the target **SameSite** value of the session cookie (**Lax** vs. **Strict**) is to be finalised before production use and aligned with the technical and organisational measures (**07-tom.md**) ({{confirm: target SameSite value of the session cookie}}).

Cookie	Purpose	Lifetime	Attributes	Category	Legal basis
session_token (name configurable via SESSION_COOKIE_NAME)	Authenticated session for staff/portal users; keeps the sign-in alive across multiple page views	24 hours (config SESSION_EXPIRY_HOURS)	Secure , HttpOnly , SameSite=Lax	Strictly necessary	§ 25(2) no. 2 TDDDG (no consent required); data processing: Art. 6(1)(b) and (f) GDPR (contract performance and legitimate interest in a secure sign-in mechanism)
__Host-lp_visitor	Pseudonymous visitor identifier for landing-page A/B-test assignment stickiness and for rate-limiting; the value is HMAC-signed, the raw/cleartext identifier is not stored (IP address and	30 days	Secure , HttpOnly , SameSite=Strict	Necessary for the requested page / also a measurement aspect — see § 5 (open assessment)	Function/stickiness & security: § 25(2) no. 2 TDDDG and Art. 6(1)(f) GDPR; insofar as the measurement aspect (A/B test) is to be classified as not strictly necessary: § 25(1) TDDDG in conjunction with Art. 6(1)(a) GDPR (consent) —

	user-agent are only inputs to the HMAC)				{{decision for EduKI/its lawyer}}
<code>__Host-lp_at</code>	Landing-page assignment token (binds interaction/lead-submit events to the respective A/B assignment, so that a submitted form is attributed to the correct assignment)	1 day	<code>Secure, HttpOnly, SameSite=Strict</code>	Strictly necessary	§ 25(2) no. 2 TDDDG (no consent required); data processing: Art. 6(1)(f) GDPR (integrity of the attribution of the action you triggered)
<code>__Host-lp_csrf</code>	CSRF token (double-submit) to protect the lead-submit form against cross-site request forgery	1 day	<code>Secure, NOT `HttpOnly` (must be read by JavaScript — see § 4), SameSite=Strict</code>	Strictly necessary (security)	§ 25(2) no. 2 TDDDG (no consent required); data processing: Art. 6(1)(f) GDPR (legitimate interest in defending against CSRF attacks)

"Lifetime" denotes the maximum validity period of the respective cookie from the time it is set; on a new session or page view the cookie may be re-set and the period re-started. Session/authentication cookies lose their validity at the latest when the configured period expires.

4. Note on the CSRF cookie `__Host-lp_csrf` (the only exception to `HttpOnly`)

The cookie `__Host-lp_csrf` is the **only** cookie of the Educas platform that is **not** set with the `HttpOnly` attribute. This is technically required and intentional from a security standpoint:

The lead-submit form is protected against cross-site request forgery (CSRF) using the **double-submit pattern**. Under this pattern, the client-side JavaScript must read the token stored in the cookie and additionally include it in the form's request body; the server accepts the form only if the value in the cookie matches the value in the request body. For the JavaScript to be able to read the token, the cookie **must not** be `HttpOnly`.

The remaining protective measures are unaffected: the cookie remains `Secure` (transmission only over HTTPS) and `SameSite=Strict` (no transmission on cross-site requests). The `__Host-` prefix additionally enforces, on the browser side, that the cookie may only be set with `Secure`, `Path=/`, and **without** a `Domain` attribute — it is thereby strictly bound to the serving domain and cannot be set or overwritten by subdomains.

5. Legal assessment under § 25 TDDDG

5.1 Principle

Under § 25(1) TDDDG, the storage of information in your terminal equipment and access to information already stored there are permitted only with your consent. By way of exception, consent is **not required** under § 25(2) TDDDG where

1. the sole purpose is carrying out the transmission of a message over a telecommunications
2. the storage or access is **strictly necessary** in order for the provider to make available

5.2 Consent-exempt, strictly necessary cookies

In EduKI GmbH's view, the cookies `session_token`, `__Host-lp_at`, and `__Host-lp_csrf` are **strictly necessary** within the meaning of § 25(2) no. 2 TDDDG and therefore require **no** consent:

- `session_token` is necessary to keep your signed-in session alive in the protected area you
- `__Host-lp_at` is necessary to reliably attribute a form submission you triggered to the
- `__Host-lp_csrf` is a security measure without which the lead-submit form cannot be operated

No consent banner is required for these cookies.

5.3 Special case `\_\_Host-lp\_visitor` — open assessment

The cookie `__Host-lp_visitor` serves **two** functions:

3. **Function/security (strictly necessary):** It stabilises the A/B assignment for the
4. **Measurement (assessment open):** The same pseudonymous identifier feeds into the

Whether the cookie, because of its **measurement aspect**, is to be classified as "strictly necessary" or requires **consent** in that respect is a matter of judgement under § 25 TDDDG. What is decisive is, in particular, whether the measurement is to be understood as an integral component of the service desired by the user or as a separate reach/success measurement that primarily serves the provider.

Because EduKI GmbH offers its services to **consumers** as well, it treats the measurement aspect of the `__Host-lp_visitor` cookie, as a precaution, as **requiring consent**: a separate A/B success measurement will, as a rule, not be "strictly necessary" within the meaning of § 25(2) no. 2 TDDDG. The safe default is therefore a **consent banner** for the measurement aspect (see § 8). Until consent is obtained, `__Host-lp_visitor` is used only for its strictly necessary functions (assignment stickiness, rate-limiting) and **not** for measurement purposes.

{{decision for EduKI/its lawyer}}: For the consumer context, EduKI GmbH proceeds on the basis that the measurement aspect **requires consent** and uses the consent banner from § 8. Its legal counsel confirms this classification, or departs from it only where the measurement aspect is exceptionally to be assessed as **strictly necessary**; in that case the banner does not apply and this policy is to be shortened accordingly (§ 8). Subject to that confirmation, the consent-based solution applies.

5.4 No third-party, advertising, or tracking cookies

EduKI GmbH confirms, as of the date of this policy (2026-06-03):

- **Only first-party cookies** are used; **no** third-party cookies.
- **No** advertising, marketing, or cross-device tracking cookies are set.
- **No** external web-analytics service (e.g. Google Analytics) and **no** external

6. Managing and withdrawing your consent

For the consent-requiring measurement aspect of the `__Host-lp_visitor` cookie (see § 5.3), consent is given purely voluntarily and can be **withdrawn at any time with effect for the future**, without any disadvantage to you. The lawfulness of processing carried out up to the point of withdrawal remains unaffected (Art. 7(3) GDPR).

Current status: Because EduKI GmbH treats the measurement aspect, as a precaution, as requiring consent (§ 5.3), consent is obtained and managed via the consent banner from § 8. {{TODO: Identify the specific consent-management mechanism — the tool or banner/CMP solution used, the option to re-open the settings (e.g. a "Cookie settings" button), and the mechanism for storing/logging the consent (demonstrability under Art. 7(1) GDPR).}}

You can withdraw your consent — to the extent given — or remove the relevant cookies as follows:

- Delete the cookies that have been set in your browser (see § 7), or
- contact the data-protection contact named in § 1.

7. Controlling cookies via your browser

Independently of any consent, you can control and restrict the setting and storage of cookies at any time via your browser settings, delete individual or all cookies, and enable automatic deletion when the browser is closed. The procedure differs from browser to browser; the vendors provide corresponding help pages (e.g. for Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari).

Important note: If you block or delete **strictly necessary** cookies (see § 5.2), core functions of the platform may be impaired — in particular, the sign-in cannot be maintained or the lead-submit form cannot be submitted. These cookies cannot be deselected via a consent banner, because the service does not function as intended without them.

8. Consent banner (sample text)

Application: Because EduKI GmbH treats the measurement aspect of the `__Host-lp_visitor` cookie, as a precaution, as requiring consent vis-à-vis consumers (§ 5.3), the banner text below is the **governing default** and is to be used. The banner must offer an ****equivalent reject option**** at the first level (a genuine "Reject all"); a pre-selection ("opt-in" pre-ticked) is not permitted. Should legal counsel exceptionally classify the measurement aspect as strictly necessary (§ 5.3): where only strictly necessary cookies are then used, **no consent banner** with "Accept/Reject" may appear; a mere cookie notice (without a consent request) suffices and is to be preferred.

German banner text (governing default for the consumer context; identical to § 8 of the German version):

Cookies und Messung

Wir verwenden technisch notwendige Cookies, damit diese Website funktioniert (Anmeldung, Formularabsendung, Sicherheit). Diese sind immer aktiv und benötigen keine Einwilligung.

Darüber hinaus möchten wir mit einem erstanbieterseitigen, pseudonymen Cookie messen, welche Variante unserer Landingpages besser funktioniert (A/B-Test). Dafür benötigen wir Ihre Einwilligung. Sie ist freiwillig und jederzeit mit Wirkung für die Zukunft widerrufbar.

[**Alle akzeptieren**] [**Alle ablehnen**] [**Einstellungen**]

Weitere Informationen finden Sie in unserer [Cookie-Richtlinie] und unserer [Datenschutzerklärung].

English banner text:

Cookies and measurement

We use strictly necessary cookies so that this website works (sign-in, form submission, security). These are always active and do not require consent.

In addition, we would like to use a first-party, pseudonymous cookie to measure which variant of our landing pages performs better (A/B test). This requires your consent. It is voluntary and can be withdrawn at any time with effect for the future.

[**Accept all**] [**Reject all**] [**Settings**]

For more information, see our [Cookie Policy] and our [Privacy Policy].

Notes on banner design (binding if used):

- "Reject all" must be reachable at the **first level, equivalent**, and with the same
- Consent-requiring cookies may be set/used for measurement purposes **only after** active
- The settings must be re-openable at any time, and withdrawal must be as easy as giving consent.
- {{TODO: When introducing a CMP, add the specific mechanism for storing/logging the consent

9. Changes to this Cookie Policy

EduKI GmbH will update this Cookie Policy as soon as the cookies used, their purposes, or the legal assessment change — in particular if a consent-requiring cookie, a consent-management platform, or an external service is added in the future. The version stated under "Stand / As of" applies in each case.

10. Contact

If you have questions about this Cookie Policy or wish to exercise your data-subject rights (in particular access, rectification, erasure, restriction, objection, withdrawal of consent, and lodging a complaint with a supervisory authority), please contact:

{{datenschutz@... / privacy contact e-mail}}

{{Datenschutzbeauftragte:r — Name+Kontakt ODER „nicht bestellt"}}

You also have the right to lodge a complaint with a data-protection supervisory authority (Art. 77 GDPR):
{{zuständige Aufsichtsbehörde / competent supervisory authority (depends on EduKI's seat)}}.