Cookie, Analytics & SDK Consent Policy

Readu web and mobile privacy controls — EU/UK and broader deployment baseline

Language versions. This policy is available in Bulgarian and English. For consumers in Bulgaria, the Bulgarian text applies; elsewhere, the English text applies. [COUNSEL TO CONFIRM]

Implementation rule: Do not load non-essential analytics/advertising/device-access technologies before valid consent in jurisdictions where consent is required. There is no "accept by continuing to browse" shortcut for non-essential tracking.

1. Technology categories

Category	Examples	Default	Consent approach
Strictly necessary	Authentication token, security/session, load balancing, user-requested preference	On	No optional consent where legally strictly necessary; disclose
Functional optional	Remembering optional preferences beyond essential service	Off unless requested	Consent where PECR/ePrivacy requires
Analytics	Firebase Analytics or similar usage measurement [CONFIRM]	Off in EU/UK until consent where required	Separate clear choice; no pre-tick
Crash/performance	Crash reporting/diagnostics [CONFIRM]	Assess necessity; minimise identifiers	Consent if device-access rule applies and not strictly necessary
Marketing/advertising	Ad SDKs, cross-context behavioral tracking	Off / not used for student targeting	Separate opt-in where used; Readu policy is no targeted advertising using student data

2. Consent design

- Present Reject and Accept choices with comparable prominence where required.
- No pre-ticked optional categories.
- Do not condition core service on optional tracking unless genuinely necessary and legally permitted.
- Record consent version, categories, timestamp, and user/account/device identifier necessary to prove the choice.
- Make withdrawal/change at least as easy as giving consent.
- Re-prompt only when purposes/vendors materially change or consent has expired under the implemented compliance standard.

3. Child users

For child users, minimize tracking and use high-privacy defaults. Do not use manipulative nudges to obtain consent. Where consent is the legal basis and parental authorization is legally required for the child's age/jurisdiction, implement the appropriate parent/guardian flow.

4. Mobile SDK inventory

SDK / technology	Purpose	Essential?	Personal data	Consent required?	Status
[TO COMPLETE]		Yes/No		Jurisdiction-specific	Approved/blocked

5. Web cookie/local-storage inventory

Name/technology	Provider	Purpose	Expiry	Category	Consent
[TO COMPLETE]					

6. Analytics governance

- Do not send raw lesson answers, AI prompts, student names, emails, or message content into analytics event properties unless specifically justified and approved.
- Prefer pseudonymous event identifiers and aggregated reporting.
- Set retention to the shortest useful period.
- Disable advertising features/signals on student-focused analytics configurations.
- Review event schemas before release.

7. Registration consent separation

Acceptance of Terms/Privacy Notice is not consent to optional analytics. Keep optional consent distinct and off by default. AI/model-improvement consent, marketing consent, and analytics consent should not be collapsed into a single mandatory checkbox.

Legal reference note

This working document is designed to support Readu's compliance program. It should be reviewed against the exact production architecture, customer contract, and current law before execution or publication. Key legal sources include:

- Regulation (EU) 2016/679 (GDPR), in particular Articles 5, 6, 12-22, 24-25, 28, 30, 32-36, 44-49.
- Bulgarian Personal Data Protection Act and guidance of the Bulgarian Commission for Personal Data Protection (CPDP/KZLD).
- UK GDPR; Data Protection Act 2018; Privacy and Electronic Communications Regulations (PECR).
- ICO Age Appropriate Design Code (Children's Code), including the requirement to assess and mitigate risks to children through a DPIA.