Sesh Space Legal & Trust Center

Sesh Space Law Enforcement Request Policy

Legal Process • Limited Data • Encryption Limits

Effective Use	Platform policies for app and web
Retention	Feeds 14 days / Messages 24 hours
Support	support@seshspace.com

Important: Sesh Space is privacy-first. Short retention and end-to-end encryption reduce what can be reviewed after content expires. Users should preserve screenshots for reports.

1. Scope of This Policy

This Policy explains how Sesh Space responds to requests for user information from law enforcement, regulators, courts, and other government authorities. It reflects the technical realities of a privacy-first service with limited retention, optional location features, business listings, ad records, and end-to-end encrypted messaging.

2. What Sesh Space May Have

Sesh Space may have limited operational information such as account identifiers, basic registration details, limited authentication/session records, profile information, report metadata, admin action logs, business profile records, ad campaign records, listing suggestion records, push subscription records, approximate location settings if enabled, and other narrowly scoped service data necessary to operate the platform. Because content is temporary, some information may no longer exist by the time a request is received.

3. What Sesh Space May Not Have

Sesh Space does not ordinarily have readable access to end-to-end encrypted private message content. Feed posts may expire automatically after approximately fourteen (14) days, and private messages may expire automatically after approximately twenty-four (24) hours. If content has expired, been deleted, or is not accessible because of encryption, Sesh Space may be unable to produce it.

4. Valid Legal Process Required

Sesh Space generally requires valid and legally binding process before disclosing user information, unless disclosure is permitted or required by law in an emergency involving imminent risk of death or serious physical harm, or in another legally recognized urgent circumstance.

5. Review of Requests

Requests are reviewed for jurisdiction, facial validity, scope, specificity, legal basis, and consistency with applicable law. Sesh Space may object to, narrow, reject, or seek clarification on requests that are overbroad, legally deficient, unsupported, inconsistent with the platform's technical capabilities, or seek data that does not exist or cannot be decrypted by Sesh Space.

6. Notice to Users

Where permitted by law and appropriate under the circumstances, Sesh Space may notify affected users before disclosing information. Sesh Space may delay or withhold notice where notice is prohibited by law, would create risk of harm, would compromise an investigation, or is otherwise inappropriate.

7. Emergency Requests

If an authority asserts that there is an emergency involving imminent danger of death or serious physical injury, Sesh Space may consider emergency disclosure requests to the extent allowed by law. Even in emergency situations, disclosure is limited by what data Sesh Space actually has. Sesh Space cannot provide a backdoor to encrypted messages or recreate expired content.

8. Preservation Requests

Where legally valid and technically feasible, Sesh Space may preserve limited records for a defined period. Preservation does not create new data, restore expired content, extend ordinary retention for already-deleted content, or defeat end-to-end encryption. Content that has already expired or is not accessible cannot be recreated.

9. Ad, Business, Listing, and Demo Records

Where available and legally required, Sesh Space may be able to provide limited records associated with business accounts, sponsored content, campaign configuration, listing suggestions, advertiser contacts, demo links, or admin actions. Availability depends on retention, system configuration, and legal validity of the request.

10. International and Cross-Border Requests

Authorities making requests should use the process legally recognized in the relevant jurisdiction. Sesh Space may require requests to comply with applicable cross-border data access rules, mutual legal assistance requirements, or other lawful mechanisms.

11. No Informal Voluntary Access to Encrypted Content

Sesh Space cannot provide a backdoor to encrypted message content and does not guarantee that encrypted material can be made readable. This technical limit applies regardless of the requesting party.

12. Contact

Government and law enforcement requests should be directed to support@seshspace.com with appropriate legal documentation.