

Government Requests Policy

ashoka ritual - global artist network

8 August 2026

This Policy explains how artist ritual GmbH handles requests, demands and orders from governments, courts, law-enforcement agencies, intelligence or security services, regulators and other public authorities seeking user information or action concerning the ashoka ritual network. It is designed to maximise lawful protection of artists and their data while recognising that binding legal duties cannot be excluded by private policy.

1. Provider and scope

1.1 This Policy applies to artist ritual GmbH, Hofrichterstrasse 32, 51067 Cologne, Germany, and to data under its possession or control in connection with ashoka ritual.

1.2 It covers requests for account data, identity or registration data, content, messages where available to us, metadata, IP and access logs, device or security information, billing information, preservation of data, content restriction and account action.

1.3 The Policy is incorporated into the ashoka ritual Terms as a contractual privacy commitment to users to the extent legally permissible.

2. Core principle: no voluntary state collaboration

2.1 artist ritual is a private, transnational cultural network and does not voluntarily collaborate with state institutions to identify artists, analyse communities, monitor relationships, evaluate opinions or make user datasets available for governmental purposes.

2.2 We do not voluntarily participate in intelligence-sharing, surveillance partnerships, political influence programmes, population profiling, government data pools or standing law-enforcement access programmes involving ashoka ritual user data.

2.3 A disclosure made solely because a final and enforceable legal obligation compels it is “compelled compliance” and is not treated by us as voluntary collaboration.

3. State institutions may not use the network as participants

3.1 State institutions and persons acting for governmental purposes may not register for or use ashoka ritual as participants, data collectors, research accounts or institutional observers. The definition and private-capacity exception in the Terms apply.

3.2 We may suspend or close accounts reasonably believed to be used covertly for state collection or official purposes, subject to applicable law and redress rights.

3.3 This contractual rule does not prevent authorities from viewing content a user deliberately makes publicly accessible on the open internet.

4. No state or privately commissioned opinion research

4.1 We will not voluntarily provide user data for public-opinion polling, political or ideological research, election analytics, propaganda measurement, social-control research, psychometric profiling, sentiment mapping or comparable governmental or privately commissioned opinion research.

4.2 We do not sell, rent or license user data for such purposes. Requests framed as academic, statistical, policy or commercial research are rejected where their purpose falls within this prohibition, unless disclosure is independently required by binding law.

5. No special access, backdoors or standing interfaces

5.1 We do not provide governments with direct database access, dashboards, special search tools, bulk feeds, privileged APIs, hidden accounts, persistent taps, backdoors or preferential access to user data.

5.2 We do not deliberately weaken security or create government key escrow to facilitate access. We do not promise that all data are end-to-end encrypted; the prohibition concerns deliberate government access mechanisms.

6. Required request channel and authentication

6.1 Government requests should be sent to mail@artist-ritual.com with the subject “Government Request” and identify the requesting authority, responsible official, official contact information and legal basis.

6.2 We may require transmission through an official government domain, authenticated electronic channel, formal service route, mutual legal assistance channel or other method sufficient to verify authenticity.

6.3 Sending a request to us does not create jurisdiction, consent to service, recognition of the request or waiver of any objection.

7. Minimum legal requirements

7.1 We require a request to be issued by a competent authority, based on a valid legal power, properly served, binding on artist ritual GmbH, sufficiently specific and consistent with applicable constitutional, fundamental-rights, data-protection and procedural safeguards.

7.2 A request should identify the specific account or person, the precise categories of information sought, the relevant time period, the purpose and legal basis, and available remedies. Vague requests for “all data”, classes of users or broad cultural communities are not accepted merely for convenience.

7.3 For orders governed by the EU Digital Services Act, we expect the elements required by applicable law, including identification of the authority, legal basis, specific recipient or content, and, where required, reasons addressing necessity and proportionality.

8. Jurisdiction and cross-border requests

8.1 Foreign authorities should use a legal mechanism recognised in Germany or the European Union where direct extraterritorial enforcement is not valid, including applicable mutual legal assistance, judicial-cooperation or other recognised channels.

8.2 For personal data protected by EU law, we take account of GDPR Article 48 and other transfer rules. A foreign judgment or administrative decision is not treated as automatically enforceable merely because it was issued abroad.

8.3 We evaluate conflicts of law, international comity, fundamental rights and transfer restrictions and may require the requesting authority to obtain an order from the competent German or EU authority.

9. Necessity, proportionality and data minimisation

9.1 We interpret requests narrowly. We disclose only information that is specifically covered, already collected for the service, within our possession or control, and legally required.

9.2 We do not create new categories of data, conduct new monitoring, build profiles, infer opinions, run facial recognition, generate social graphs or collect future information merely to satisfy a request unless a binding law specifically and validly requires such action and no lawful challenge remains.

9.3 Where a request can be satisfied with less information, a shorter period, a pseudonymous identifier or non-content data, we seek to narrow it accordingly.

10. Rejection, narrowing and legal challenge

10.1 We reject, return or seek clarification of requests that are unauthenticated, informal where formal process is required, legally defective, overbroad, disproportionate, outside jurisdiction, inconsistent with applicable data-protection law or insufficiently specific.

10.2 Where reasonable legal grounds exist, we seek narrowing, protective conditions, judicial review or other remedies. We may engage independent counsel where appropriate.

10.3 We do not promise to litigate every request. The decision depends on legal merit, urgency, risk to users, available remedies, cost and the likelihood that a challenge can lawfully reduce or prevent disclosure.

11. User notice

11.1 Our default is to notify the affected user before disclosure, including the requesting authority, nature of the request and categories of data, unless notice is legally prohibited, would create an imminent serious safety risk or would unlawfully compromise a legitimate investigation.

11.2 If notice is temporarily prohibited, we seek to limit the duration where possible and notify the user after the restriction expires, unless law continues to prohibit notice.

11.3 Where the DSA or other law requires notice of an order and the effect given to it, we provide that information and available redress as required.

12. Preservation requests

12.1 A preservation request does not itself authorise disclosure. We preserve specified existing data only where required by valid law or where we voluntarily choose to preserve it for a short period in response to a credible formal request while awaiting proper legal process and such preservation is lawful.

12.2 Preservation is limited to identified accounts, data categories and time periods. We do not use preservation as a basis for expanded surveillance or new collection.

13. Emergency requests

13.1 We may disclose limited information without ordinary process only where applicable law permits it and we reasonably believe there is a genuine emergency involving an imminent risk of death or serious physical injury and disclosure is necessary to address that risk.

13.2 Emergency requests should identify the person at risk, describe the nature and immediacy of the threat, specify the information sought, explain why ordinary legal process cannot be obtained in time and provide an official contact for verification.

13.3 Emergency disclosure is not available for political activity, protests, reputation, property-only concerns, general crime prevention, immigration enforcement, opinion research or intelligence gathering absent an independently binding legal basis.

14. Mandatory reports concerning serious threats

14.1 This Policy does not prevent reports that the law expressly requires. In particular, where the EU Digital Services Act applies and we become aware of information giving rise to suspicion of a criminal offence involving a threat to the life or safety of persons, statutory notification duties may apply.

14.2 Any such report is limited to the legal purpose and information required by law and does not convert ashoka ritual into a voluntary surveillance partner.

15. Content restriction and account-action orders

15.1 Orders seeking removal, disabling, geo-restriction, preservation or account restriction are reviewed for legal basis, competent authority, specificity, territorial scope, necessity, proportionality and available redress.

15.2 We seek to avoid worldwide restriction where a lawful order is territorially limited. We may use the least restrictive effective measure where law permits.

15.3 Users are informed of covered orders and remedies where legally permitted or required.

16. Bulk, class and dragnet requests

16.1 We oppose requests seeking bulk access, indiscriminate data sets, all users in a location, all members of an artistic movement, all contacts of a person, keyword-wide content or other dragnet information without individualised legal authority and strict necessity.

16.2 We do not voluntarily provide “community maps”, artist-network graphs, political or cultural affiliation inferences or datasets designed to identify movements, dissidents, activists or social groups.

17. Service providers and subprocessors

17.1 We require service providers handling user data to protect confidentiality and, where contractually and legally possible, to refer government requests concerning ashoka ritual data to us rather than respond directly.

17.2 We seek contractual commitments requiring notice to us before disclosure unless prohibited by law and limiting disclosures to valid, binding process.

17.3 We choose infrastructure and data locations with regard to security, data-protection law and the risk of disproportionate state access. No hosting choice can eliminate all sovereign legal powers.

18. Data localisation and jurisdictional exit

18.1 We do not voluntarily localise data in a country solely to make it easier for that country’s authorities to obtain access.

18.2 If operating in a jurisdiction would require routine state access, a government backdoor, systematic political monitoring, broad localisation tied to state access or another measure materially incompatible with this Policy, artist ritual may choose not to offer or to discontinue the service there, to the extent legally permitted.

18.3 Where withdrawal from a jurisdiction is legally or practically impossible in the short term, we minimise data, access and retention and seek lawful technical and organisational safeguards.

19. Documentation, access control and confidentiality

19.1 Government requests and disclosures are handled by authorised personnel and documented as appropriate. Internal access is limited according to need-to-know and role.

19.2 We retain request records only as long as reasonably needed for legal compliance, audits, security, transparency reporting and defence of rights, subject to applicable retention law.

20. Transparency reporting

20.1 To the extent legally permitted and operationally feasible, we may publish aggregate information about government requests, including numbers received, jurisdictions, request types, challenges and disclosures.

20.2 We do not publish information that would unlawfully identify users, compromise security or violate a valid confidentiality order.

20.3 We do not use a “warrant canary” or similar mechanism as a substitute for legally accurate reporting where such a mechanism could mislead users or conflict with law.

21. No voluntary waiver of rights; no promise of impossible secrecy

21.1 We do not voluntarily waive legal objections or data-protection protections for the convenience of a requesting authority.

21.2 At the same time, no private company can truthfully guarantee that user information will “never” be disclosed to a state under any circumstances. Courts and authorities may have binding powers that cannot be contracted away. Our commitment is therefore the maximum lawful one: no voluntary state collaboration, strict validation, minimum disclosure, challenge where reasonably available, user notice where lawful, no backdoors and withdrawal from incompatible jurisdictions where feasible.

22. Changes, language versions and contact

22.1 We may update this Policy for changes in law, technology, security or operations. Material reductions in user protections will be notified where legally required and will not retroactively alter disclosures already governed by an earlier binding commitment.

22.2 Language versions are intended to have the same substantive meaning. Mandatory local law prevails where it requires a different result.

22.3 Contact for government requests:

artist ritual GmbH

Hofrichterstrasse 32

51067 Cologne

Germany

Email: mail@artist-ritual.com

Subject: Government Request