ashoka ritual – Government-Requests Policy (English Translation)

Source: German version dated 13.02.2026 (unofficial translation for convenience).

Government-Requests Policy – “ashoka ritual”

Handling of official information and data surrender requests
Version: 13 February 2026

This policy describes how the provider of the “ashoka ritual” platform (X-Working GmbH) handles requests from government bodies. It supplements the GTC and the Privacy Policy and specifies the principle of the platform’s government-independent orientation.

1. Guiding principles

- No voluntary cooperation: We do not voluntarily cooperate with government institutions to identify, monitor or evaluate users or content.
- No privileged access: We do not provide special access, interfaces, backdoors or circumvention solutions.
- Legal review and minimisation principle: We respond only to legally valid and sufficiently specific orders and disclose only the mandatory minimum.
- Transparency towards users: Where legally permissible and not prohibited, we inform affected users.
- Documentation: We document official requirements and our responses in accordance with applicable law and internal compliance.

2. Scope

This policy applies to all official or quasi-official requests, including requests by law enforcement agencies, intelligence services, regulators, courts, ministries and state-controlled entities, regardless of the requesting country.

3. Principle: exclusion of government institutions from use

Government institutions are excluded from using the platform under the GTC. This exclusion also covers the collection of data by government actors for official purposes (e.g., covert research, monitoring, opinion research). Where such use is suspected, we reserve the right to suspend accounts and take further measures.

4. Requirements for the form of official requests

In principle, we process only requests that:

- originate from an identifiable, competent body and are submitted via verifiable communication channels,
- state a clear legal basis (e.g., court order) and are sufficiently specific,
- specify the purpose, the affected data categories and the time period,
- are proportionate and do not constitute impermissible “fishing expeditions”.

5. Review process and grounds for refusal

Each request is evaluated internally using a tiered review process (formal review, competence, legal basis, specificity, proportionality, territorial scope, conflict with protection obligations). We refuse, challenge or contest requests in particular where:

- no effective legal basis or competence is apparent,
- the request is too broad, vague or disproportionate,
- the request aims at privileged access, real-time surveillance or technical circumvention,
- the request conflicts with applicable data protection law or other mandatory law.

6. Scope of disclosure (minimisation principle)

Where we are legally obliged to disclose data, we limit this to the mandatory minimum. In particular, this includes:

- limiting to concrete identifiers/accounts rather than bulk requests,
- limiting to specific time periods,
- disclosing only the specifically ordered data categories,
- redacting/not disclosing non-required information where permissible.

7. User notification

We generally inform affected users about requests and disclosures as soon as and insofar as this is legally permissible and no statutory secrecy obligation or explicit notification ban exists. Where immediate notification is prohibited, we inform—where possible—after the prohibition expires.

8. Emergency requests (imminent danger)

In exceptional cases, authorities may submit emergency requests (e.g., imminent danger to life and limb). Such requests are also strictly reviewed. Where possible, we require a prompt subsequent formal order. Without sufficient evidence or in case of doubts, we may refuse emergency requests.

9. No use for governmental or private opinion research

We do not use data for governmental or private-sector opinion research, profiling research or political influence. We also do not provide data holdings for such purposes and exclude corresponding requests.

10. Transparency reports

Where legally permissible, we may publish aggregated transparency information (e.g., number and categories of official requests, share of refused/challenged requests). No personal data is published.

11. Data security and access controls

We use organisational and technical measures to minimise access to data (need-to-know principle, logging, access restrictions). Details cannot be fully disclosed for security reasons.

12. Contact point for authorities

Official requests must be sent exclusively to the following contact point:

Email: mail@artist-ritual.com
Postal address: X-Working GmbH, Hofrichterstrasse 32, 51067 Cologne, Germany

We do not process requests submitted via informal channels (e.g., social media) unless clear identification and verification are possible.

13. Changes to this policy

We may update this policy if the platform, legal situation or our processes change. The current version is published on the platform.