सरकारी अनुरोध नीति (Government Requests Policy)

ashoka ritual — वैश्विक कलाकार नेटवर्क

8 अगस्त 2026

यह नीति बताती है कि artist ritual GmbH सरकारों, न्यायालयों, कानून-प्रवर्तन एजेंसियों, खुफिया/सुरक्षा सेवाओं, नियामकों और अन्य सार्वजनिक प्राधिकरणों द्वारा ashoka ritual नेटवर्क से संबंधित उपयोगकर्ता जानकारी या कार्रवाई माँगने वाले अनुरोधों, माँगों और आदेशों को कैसे संभालता है। इसका उद्देश्य कलाकारों और उनके डेटा की कानूनन अधिकतम रक्षा करना है, जबकि यह स्वीकार किया जाता है कि बाध्यकारी कानूनी दायित्व निजी नीति द्वारा समाप्त नहीं किए जा सकते।

1. प्रदाता और दायरा

1.1 यह नीति artist ritual GmbH, Hofrichterstrasse 32, 51067 Cologne, Germany और ashoka ritual से संबंधित उसके कब्जे या नियंत्रण वाले डेटा पर लागू होती है।

1.2 इसमें account data, identity/registration data, content, हमारे लिए उपलब्ध messages, metadata, IP/access logs, device/security information, billing, data preservation, content restriction और account action के अनुरोध शामिल हैं।

1.3 कानूनन अनुमत सीमा तक यह नीति ashoka ritual Terms में users के प्रति contractual privacy commitment के रूप में शामिल है।

2. मूल सिद्धांत: कोई स्वैच्छिक सरकारी सहयोग नहीं

2.1 artist ritual एक निजी, सीमापार सांस्कृतिक नेटवर्क है और कलाकारों की पहचान, communities का विश्लेषण, relationships की निगरानी, opinions evaluate करने या सरकारी उद्देश्यों के लिए user datasets उपलब्ध कराने हेतु राज्य संस्थाओं से स्वेच्छा से सहयोग नहीं करता।

2.2 हम ashoka ritual user data से संबंधित intelligence-sharing, surveillance partnerships, political influence programmes, population profiling, government data pools या standing law-enforcement access programmes में स्वेच्छा से भाग नहीं लेते।

2.3 केवल अंतिम और enforceable legal obligation के कारण किया disclosure “compelled compliance” है, voluntary collaboration नहीं।

3. राज्य संस्थाएँ प्रतिभागी के रूप में नेटवर्क का उपयोग नहीं कर सकतीं

3.1 State institutions और सरकारी उद्देश्य से कार्य करने वाले व्यक्ति participants, data collectors, research accounts या institutional observers के रूप में ashoka ritual में register/use नहीं कर सकते। Terms की definition और genuine private-capacity exception लागू है।

3.2 Applicable law और redress rights के अधीन, यदि कोई account covert state collection या official purpose के लिए उपयोग होता प्रतीत हो तो हम उसे suspend/close कर सकते हैं।

3.3 यह contractual rule authorities को खुले internet पर user द्वारा जानबूझकर public की गई content देखने से नहीं रोकता।

4. सरकारी या निजी रूप से commission किया opinion research निषिद्ध

4.1 हम public-opinion polling, political/ideological research, election analytics, propaganda measurement, social-control research, psychometric profiling, sentiment mapping या comparable government/private commissioned opinion research के लिए voluntarily user data नहीं देंगे।

4.2 हम ऐसे उद्देश्यों के लिए user data बेचते, किराये पर देते या license नहीं करते। Academic, statistical, policy या commercial research के रूप में प्रस्तुत request भी इस निषेध में आने पर reject होगा, जब तक binding law independently disclosure न माँगे।

5. Special access, backdoors या standing interfaces नहीं

5.1 हम governments को direct database access, dashboards, special search tools, bulk feeds, privileged APIs, hidden accounts, persistent taps, backdoors या preferential user-data access नहीं देते।

5.2 हम जानबूझकर security कमजोर या government key escrow नहीं बनाते। हम सभी data के end-to-end encrypted होने का वादा नहीं करते; निषेध intentional government-access mechanisms पर है।

6. आवश्यक request channel और authentication

6.1 Government requests mail@artist-ritual.com पर subject “Government Request” के साथ भेजे जाएँ और requesting authority, responsible official, official contact तथा legal basis बताएँ।

6.2 हम official government domain, authenticated electronic channel, formal service route, mutual legal assistance channel या authenticity verify करने वाला अन्य तरीका माँग सकते हैं।

6.3 Request भेजना jurisdiction, consent to service, request recognition या objections के waiver को उत्पन्न नहीं करता।

7. न्यूनतम कानूनी आवश्यकताएँ

7.1 Request competent authority द्वारा valid legal power पर जारी, properly served, artist ritual GmbH पर binding, sufficiently specific और applicable constitutional, fundamental-rights, data-protection और procedural safeguards के अनुरूप होना चाहिए।

7.2 Request specific account/person, exact information categories, relevant period, purpose/legal basis और available remedies बताए। "All data", user classes या broad cultural communities की vague requests सुविधा मात्र के लिए स्वीकार नहीं की जाएँगी।

7.3 EU DSA के अधीन orders में applicable law द्वारा अपेक्षित elements, including authority identification, legal basis, specific recipient/content और जहाँ आवश्यक necessity/proportionality reasons अपेक्षित हैं।

8. Jurisdiction और cross-border requests

8.1 Foreign authorities जहाँ direct extraterritorial enforcement valid न हो, Germany/EU में recognized legal mechanism, including mutual legal assistance, judicial cooperation या अन्य recognized channels का उपयोग करें।

8.2 EU law से protected personal data के लिए GDPR Article 48 और अन्य transfer rules पर विचार किया जाता है। Foreign judgment/administrative decision केवल विदेश में जारी होने से automatically enforceable नहीं माना जाता।

8.3 हम conflicts of law, international comity, fundamental rights और transfer restrictions evaluate करते हैं और competent German/EU authority का order माँग सकते हैं।

9. Necessity, proportionality और data minimisation

9.1 Requests को संकीर्ण रूप से interpret किया जाता है। केवल specifically covered, service के लिए पहले से collected, हमारे possession/control में और legally required information disclose की जाती है।

9.2 केवल request satisfy करने के लिए नए data categories, new monitoring, profiles, opinion inference, facial recognition, social graphs या future collection नहीं बनाते, जब तक binding law specific/validly ऐसा न माँगे और कोई lawful challenge शेष न हो।

9.3 कम information, shorter period, pseudonymous identifier या non-content data से request पूरी हो सकती हो तो हम उसे narrow करने का प्रयास करते हैं।

10. Rejection, narrowing और legal challenge

10.1 Unauthenticated, formally required होने पर informal, legally defective, overbroad, disproportionate, outside jurisdiction, applicable data-protection law से inconsistent या insufficiently specific requests को reject, return या clarify किया जाता है।

10.2 Reasonable legal grounds होने पर narrowing, protective conditions, judicial review या अन्य remedies माँगे जाते हैं; उचित होने पर independent counsel लिया जा सकता है।

10.3 हर request पर litigation का वादा नहीं है। निर्णय legal merit, urgency, user risk, available remedies, cost और challenge द्वारा disclosure कम/रोकने की lawful संभावना पर निर्भर है।

11. User notice

11.1 Default रूप से disclosure से पहले affected user को requesting authority, request nature और data categories सहित notice दिया जाता है, सिवाय जहाँ notice legally prohibited हो, imminent serious safety risk पैदा करे या legitimate investigation को unlawfully compromise करे।

11.2 Temporary prohibition होने पर जहाँ संभव हो उसकी अवधि सीमित करने और समाप्ति के बाद user को notice देने का प्रयास किया जाता है, जब तक कानून आगे भी रोकता न हो।

11.3 DSA या अन्य law जहाँ order और उसके effect की notice माँगता है वहाँ required information और available redress दिया जाता है।

12. Preservation requests

12.1 Preservation request अपने-आप disclosure authorize नहीं करता। Specified existing data केवल valid law की आवश्यकता पर, या credible formal request के बाद proper legal process की प्रतीक्षा में short period के लिए voluntary preservation lawful होने पर ही preserve किया जाता है।

12.2 Preservation identified accounts, categories और periods तक सीमित है और expanded surveillance/new collection का आधार नहीं बनता।

13. Emergency requests

13.1 Ordinary process के बिना limited information केवल तब disclose की जा सकती है जब applicable law अनुमति दे, imminent death या serious physical injury का genuine emergency risk यथोचित माना जाए और disclosure उसे address करने के लिए necessary हो।

13.2 Emergency request व्यक्ति at risk, threat nature/immediacy, sought information, ordinary process समय पर क्यों नहीं मिल सकता और verification हेतु official contact बताए।

13.3 Independent binding legal basis के बिना political activity, protests, reputation, property-only concerns, general crime prevention, immigration enforcement, opinion research या intelligence gathering के लिए emergency disclosure उपलब्ध नहीं है।

14. गंभीर खतरों संबंधी mandatory reports

14.1 यह नीति express legal reporting duties को नहीं रोकती। विशेष रूप से DSA लागू होने पर जीवन या व्यक्तियों की सुरक्षा को threat देने वाले suspected criminal offence की जानकारी मिलने पर statutory notification duties लागू हो सकती हैं।

14.2 ऐसा report केवल legal purpose और law-required information तक सीमित होगा और ashoka ritual को voluntary surveillance partner नहीं बनाता।

15. Content restriction और account-action orders

15.1 Removal, disabling, geo-restriction, preservation या account restriction के orders को legal basis, competent authority, specificity, territorial scope, necessity, proportionality और available redress के लिए review किया जाता है।

15.2 Lawful order territorial होने पर worldwide restriction से बचने का प्रयास और जहाँ law अनुमति दे least restrictive effective measure का उपयोग किया जाता है।

15.3 जहाँ legally permitted/required हो users को covered orders और remedies की जानकारी दी जाती है।

16. Bulk, class और dragnet requests

16.1 Individualised legal authority और strict necessity के बिना bulk access, indiscriminate datasets, किसी location के सभी users, artistic movement के सभी members, व्यक्ति के सभी contacts, broad keyword content या अन्य dragnet information की requests का हम विरोध करते हैं।

16.2 हम voluntarily “community maps”, artist-network graphs, political/cultural affiliation inferences या movements, dissidents, activists/social groups identify करने के datasets नहीं देते।

17. Service providers और subprocessors

17.1 User data handle करने वाले providers को confidentiality protect करने और contractual/legal रूप से संभव हो तो ashoka ritual data के government requests हमें refer करने के लिए कहते हैं, direct response के बजाय।

17.2 हम contractual commitments चाहते हैं कि law द्वारा prohibited न हो तो disclosure से पहले हमें notice मिले और disclosure valid binding process तक सीमित रहे।

17.3 Infrastructure/data locations security, data-protection law और disproportionate state-access risk को देखकर चुने जाते हैं। कोई hosting choice सभी sovereign legal powers समाप्त नहीं कर सकती।

18. Data localisation और jurisdictional exit

18.1 हम केवल authorities के access को आसान बनाने के लिए किसी country में data voluntarily localise नहीं करते।

18.2 यदि jurisdiction में operation के लिए routine state access, government backdoor, systematic political monitoring, state access से जुड़ा broad localisation या policy से materially incompatible अन्य measure आवश्यक हो, तो artist ritual कानूनन अनुमत सीमा तक वहाँ service न देने या बंद करने का निर्णय ले सकता है।

18.3 Short term में exit legally/practically impossible हो तो data, access और retention minimise कर lawful technical/organisational safeguards तलाशे जाते हैं।

19. Documentation, access control और confidentiality

19.1 Government requests/disclosures authorised personnel संभालते हैं और उचित रूप से document होते हैं। Internal access need-to-know और role के अनुसार सीमित है।

19.2 Request records legal compliance, audits, security, transparency reporting और rights defence हेतु reasonably necessary अवधि तक, applicable retention law के अधीन, रखे जाते हैं।

20. Transparency reporting

20.1 Lawful और operationally feasible सीमा तक requests received, jurisdictions, types, challenges और disclosures पर aggregated information publish की जा सकती है।

20.2 ऐसी information publish नहीं की जाती जो users को unlawfully identify करे, security compromise करे या valid confidentiality order violate करे।

20.3 यदि "warrant canary" जैसा mechanism misleading या law-conflicting हो सकता है तो उसे legally accurate reporting के substitute के रूप में उपयोग नहीं किया जाता।

21. अधिकारों का voluntary waiver नहीं; असंभव secrecy promise नहीं

21.1 Requesting authority की सुविधा के लिए हम legal objections या data-protection safeguards voluntarily waive नहीं करते।

21.2 कोई private company सत्यतापूर्वक यह guarantee नहीं दे सकती कि user information किसी भी परिस्थिति में राज्य को "कभी नहीं" दी जाएगी; courts/authorities के binding powers contract से समाप्त नहीं हो सकते। इसलिए हमारा commitment maximum lawful protection है: no voluntary state collaboration, strict validation, minimum disclosure, reasonably available challenge, lawful user notice, no backdoors और feasible होने पर incompatible jurisdictions से withdrawal।

22. बदलाव, भाषा संस्करण और संपर्क

22.1 Law, technology, security या operations बदलने पर policy update हो सकती है। User protections की material reduction जहाँ required हो notify की जाएगी और पहले के binding commitment के अधीन disclosures को retroactively नहीं बदलेगी।

22.2 भाषा संस्करणों का substantive meaning समान रखने का उद्देश्य है। Mandatory local law अलग परिणाम माँगे तो वही प्राथमिक होगा।

22.3 Government requests के लिए संपर्क:

artist ritual GmbH

Hofrichterstrasse 32

51067 Cologne

Germany

ईमेल: mail@artist-ritual.com

विषय: Government Request