PRIVACY POLICY

Last updated: 2026-10-20

Article 1 — Introduction, Controller and Scope

1.1 This Privacy Policy (the "Policy") forms part of the legal documentation of the Service and describes how Fabiola Serralunga (the "Operator", "we", "us" or "our"), established in Argentina, processes Personal Data in connection with the website published at https://testpages-simple.pages.dev (the "Site"). The Site, together with the claim and delivery functions it embeds, is referred to as the "Service". Enquiries relating to this Policy or to the processing of Personal Data may be directed to the Operator at any time at curses.trinity426@slmails.com.

1.2 The Service is a demonstration page through which a Visitor may claim (mint) a non-transferable token — a "Soulbound Token" or "SBT" — on the Base Sepolia Testnet and, following an automated verification of entitlement, obtain the delivery of the digital asset file linked to that token. The Service forms part of the MellonKeyfs documentation system maintained by the Operator; a companion edition of that system is published at https://mellonkeyfs.pages.dev and the Operator's development profile is published at https://github.com/fabiola-serralunga. The project is maintained for technical, demonstrative and educational purposes and has no commercial purpose.

1.3 This Policy applies to all individuals who visit the Site or interact with its claim and delivery features (each, a "Visitor" or "you"). It does not apply to third-party websites, products or services that are not operated by us, including the wallet provider you select, the RPC providers described in Article 4, the blockchain and storage networks on which the Service relies, and the gateways through which content hosted on the Arweave network is delivered. Those third parties process data under their own privacy policies, which we encourage you to review independently.

1.4 The legal documentation of the Service consists of this Policy, the Terms and Conditions and the Cookie and Local Storage Notice. This Policy governs all matters relating to privacy and the processing of Personal Data. In the event of any

conflict between this Policy and the remaining parts with respect to the processing of Personal Data, this Policy prevails.

1.5 This Policy is published with the effective date and version recorded in the document control table of this documentation. Amendments will be announced in accordance with Article 18.

Article 2 — Definitions

2.1 “Personal Data” means any information relating to an identified or identifiable natural person, in particular by reference to an identifier such as an IP address, a wallet address or another online identifier.

2.2 “Processing” means any operation or set of operations performed upon Personal Data, whether or not by automated means, including the collection, recording, storage, transmission, disclosure and erasure thereof.

2.3 “Wallet” means the software or hardware means by which a person controls cryptographic keys and through which a public address (a string beginning with “0x” followed by forty hexadecimal characters) is used to interact with a blockchain network. A Wallet does not, by itself, contain off-chain information supplied to the Service.

2.4 “Wallet Provider” means the third party whose wallet software you choose to connect to the Site in order to sign messages or transactions. The Operator does not develop, host or control the Wallet.

2.5 “RPC Provider” means the remote procedure call service through which a browser queries the state of the Base Sepolia Testnet. For the Service, the RPC Provider is Alchemy Insights, Inc. (“Alchemy”) and, as an automatic fallback, the public Base Sepolia endpoint operated through the infrastructure of Base and published at sepolia.base.org.

2.6 “SBT” means a Soulbound Token: a token issued on the Base Sepolia Testnet by a smart contract deployed by the Operator, which is non-transferable by design and whose metadata incorporates a reference to the digital asset file to which it is linked.

2.7 “Base Sepolia Testnet” means the public test network of the Base protocol. It is a testing and development environment: assets recorded on it have no economic value and the network may be subject to resets outside the control of the Operator.

2.8 “Gateway” means an HTTP endpoint that indexes and serves content stored on the Arweave network, including the canonical gateway arweave.net and, as fallback, gateways of the AR.IO network, whose technology is developed by Permanent Data Solutions, Inc. and supported by the AR.IO Foundation.

2.9 “Arweave Network” means the decentralised permanent storage network based on a blockweave data structure, on which the Operator publishes the imagery displayed by the Site. Files published on the Arweave Network are public and immutable by design.

2.10 “Verification Data” means the minimum set of data that the delivery function of the Service receives and processes in memory for a few seconds in order to verify an entitlement: the wallet address, a cryptographic signature produced by the Wallet over a message containing a date and time, the token number and the edition requested.

2.11 “Local Session Storage” means the entry that the Site writes to the local storage of your browser in order to keep the Wallet connected during your navigation session, as described in the Cookie and Local Storage Notice.

2.12 “GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).

2.13 “CCPA” means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, together with its implementing regulations.

2.14 “LGPD” means the Lei Geral de Proteção de Dados (Law No. 13,709/2018) of the Federative Republic of Brazil, together with its implementing regulations.

2.15 “Argentine PDPA” means Law No. 25,326 on the Protection of Personal Data of the Argentine Republic, together with its regulatory and implementing provisions.

Article 3 — Overview of Data Processing

3.1 The Service has been designed so that the Processing of Personal Data is reduced to the technical minimum. The Service does not offer user accounts, registration,

login, contact forms, newsletters, payments or any other feature that would require a Visitor to identify himself or herself; it performs no know-your-customer procedure and it does not maintain any off-chain database of visitors, claimants or downloads.

3.2 The Personal Data processed in connection with the Service is limited to: technical data — principally IP addresses and associated request metadata — processed by the infrastructure provider in the course of hosting, delivery and security; the ephemeral Verification Data described in Article 4; the records that the requested minting transaction itself writes to the Base Sepolia Testnet; the technical disclosures that your browser makes directly to the RPC Provider and to the Gateways; and the Local Session Storage entry, which never leaves your browser.

3.3 We do not sell or rent Personal Data, we do not share Personal Data with advertising networks or data brokers, and we do not use Personal Data for behavioural profiling or targeted advertising.

3.4 Table 1 below summarises the processing activities described in this Policy. The table is provided for convenience of reading and does not replace the detailed provisions of Articles 4 to 12.

Table 1 — Summary of processing activities

Category of data	Source / actor	Principal purposes	Legal basis	Retention
IP address and request metadata	Cloudflare, Inc. (hosting, CDN, bot management, security clearance, Workers execution)	Delivery of the Site; security; anti-bot protection; DDoS mitigation; execution of the delivery function	Legitimate interest (Art. 6(1)(f) GDPR)	Under the standard policies of Cloudflare, Inc. (security logs approximately 30 days; Workers logs 3 to 7 days)
Wallet address and Verification Data (signature, token number, edition)	Delivery function of the Service (memory only)	Verification of the entitlement to the linked digital asset before delivery	Performance of a contract (Art. 6(1)(b) GDPR)	A few seconds; memory only; no persistence, no logs

Category of data	Source / actor	Principal purposes	Legal basis	Retention
On-chain records (wallet address, contract address, transaction hash, timestamp, call data)	Base Sepolia Testnet (public network)	Registration of the minting transaction requested by the Visitor; provenance of the SBT	Performance of a contract (Art. 6(1)(b) GDPR)	Permanent (immutable by design of the network)
Wallet address, contract address and IP address	RPC Provider (Alchemy; fallback public Base Sepolia endpoint)	On-chain verification of token ownership performed by your browser	Performance of a contract (Art. 6(1)(b) GDPR)	Under the provider's own policies (Alchemy: IP retained approximately 90 days through its infrastructure providers)
IP address and asset identifier	Gateways of the Arweave Network (arweave.net; AR.IO fallback gateways)	Delivery of imagery hosted on the Arweave Network	Legitimate interest (Art. 6(1)(f) GDPR)	Under each gateway operator's own policy
Wallet connection state	Visitor's browser (local storage, first party)	Maintains the Wallet connected during the navigation session	Strictly necessary functional storage	Until deleted by the Visitor or cleared by the browser
Contact data (if you write to us)	Operator mailbox	Handling enquiries and requests to exercise rights	Legitimate interest (Art. 6(1)(f) GDPR)	Up to two (2) years from the last interaction, or earlier upon erasure request

Article 4 — Categories of Information Processed

4.1 IP addresses and related technical data processed by Cloudflare, Inc. The Site is hosted on Cloudflare Pages. Cloudflare acts as proxy, content delivery network and security layer, and imposes bot management and security clearance challenges on incoming traffic; the delivery function of the Service is executed through Cloudflare Workers. In that context Cloudflare processes the Visitor's IP address together with standard technical request metadata such as timestamps, the requested resource, the user-agent transmitted by the browser and the response status. Cloudflare, Inc. determines the retention of its own security logs (approximately 30 days) and Workers logs (3 to 7 days) in accordance with its own policies, which are published on its website and form no part of this documentation.

4.2 Verification Data processed in memory by the delivery function. To deliver a linked digital asset, the Service must verify that the wallet address presenting the request owns the SBT of the asset concerned. For that purpose the delivery function receives, for a few seconds and exclusively in memory: the wallet address, a cryptographic signature that the Wallet itself produces over a message containing a date and time, the token number and the edition requested. The signature is verified locally by the Service; the ownership of the token is then confirmed through an on-chain query. Once the verification is completed, the Verification Data is discarded: it is not written to disk, is not recorded in logs, is not shared and is not sold. The Wallet is never contacted by third parties through the Site, and the delivered file is served with explicit instructions that prevent the browser from storing it in cache.

4.3 On-chain records created by the minting transaction. When an SBT is minted at your request, the following data are recorded on the Base Sepolia Testnet: (a) the wallet address that mints the token; (b) the address of the smart contract that emits it; (c) the transaction hash; (d) the timestamp of the block that includes the transaction; and (e) the call data of the smart contract function. These records are public, permanent and immutable by design of the network, as described in Article 8.

4.4 Technical disclosures made by your browser to the RPC Provider. To verify whether a wallet address holds specific tokens, your browser communicates directly with Alchemy or, when Alchemy is unavailable, with the public Base

Sepolia endpoint. During this communication the following information is transmitted directly to the RPC Provider: the wallet address, the address of the SBT smart contract being queried, and your IP address, which the RPC Provider uses for security and abuse-prevention purposes. According to the public documentation of Alchemy, the IP address of API requests is retained by its infrastructure providers for approximately ninety (90) consecutive days and is then automatically deleted. The Operator does not transmit Personal Data to the RPC Provider, does not intervene in that communication and has no access to the logs of the RPC Provider.

4.5 Requests to the Gateways. The imagery displayed by the Site is hosted on the Arweave Network. To display it, your browser requests the content from a Gateway — by default the canonical gateway arweave.net and, as a configurable fallback, gateways of the AR.IO network. Gateway operators are central service operators, unlike the underlying Arweave Network, and in serving your request they may process your IP address, the identifier of the requested asset and the timestamp, under their own terms of service and privacy policies. The Arweave Network itself does not receive your IP address, and the download of content hosted on it does not generate any on-chain transaction.

4.6 Local Session Storage. The Site keeps the Wallet connected during your navigation session by means of an entry in the local storage of your browser. The Operator does not access, store or track that information on its own systems; the entry remains under the exclusive control of your browser and may be deleted at any time, as described in Cookie and Local Storage Notice.

4.7 Contact data. If you write to the contact address published in this documentation, the Operator processes the content of that correspondence and the address from which it was sent, exclusively in order to handle your enquiry or request.

4.8 Information we do not collect. We do not collect, and the Service provides no mechanism to collect, names, postal addresses, telephone numbers, dates of birth, government identifiers, payment or financial information (the Testnet involves no payment of any kind), precise geolocation, biometric or health data, or any other special categories of Personal Data within the meaning of Article 9 GDPR. The Operator maintains no accounts and no database of visitors, claimants or downloaders.

Article 5 — Legal Bases for Processing

5.1 Where the GDPR applies, the Processing of IP addresses and associated technical data rests on legitimate interest within the meaning of Article 6(1)(f) GDPR. That interest consists in operating, securing and delivering a free, public technical service and in protecting the claim and delivery functions against malicious traffic, abuse and excessive automated requests. We have weighed that interest against the rights and reasonable expectations of Visitors and have concluded that the impact on Visitors is minimal, given the technical nature of the data, the absence of tracking technologies and the absence of any identifiable visitor record.

5.2 The Processing of Verification Data and the on-chain registration described in Clause 4.3 rest on the performance of a contract within the meaning of Article 6(1)(b) GDPR: they are technical acts strictly necessary to execute the claim and delivery service that you request. The registration of the minting transaction on the Base Sepolia Testnet is an inherent and disclosed consequence of that service and is not carried out for any separate purpose; the Operator complies with its transparency obligations under Articles 13 and 14 GDPR by describing that registration in this Policy before the Processing takes place.

5.3 The transmissions that your browser makes directly to the RPC Provider and to the Gateways, as described in Clauses 4.4 and 4.5, are necessary technical steps for the delivery of the service you requested and for the display of the content of the Site, and are accordingly covered by the bases described in Clauses 5.1 and 5.2, as applicable to each transmission.

5.4 The storage of the Local Session Storage entry constitutes technical storage that is strictly necessary for the delivery of an information society service expressly requested by the Visitor, and accordingly falls within the recognised exceptions to the consent requirements applicable to cookies and similar technologies.

5.5 Under the CCPA, the data described in Article 4 is limited to internet or other electronic network activity information and technical identifiers processed by our service providers for the operational and security purposes described in this Policy. We do not sell and do not share Personal Data as those terms are defined by the CCPA, because no consideration is received for any disclosure described in this Policy. Under the LGPD, the Processing rests on the necessity of the Processing for

the performance of a contract to which you are party (Article 7, item V), on the exercise of rights in judicial or administrative proceedings where applicable (Article 7, item VI) and on the legitimate interests of the Operator in securing its infrastructure (Article 7, item IX). Under the Argentine PDPA, which is based on informed consent, the Processing rests on the consent evidenced by the Visitor's voluntary initiation of the claim after having been informed by this Policy, limited to the minimum data described herein; requests to exercise rights are answered within ten (10) business days, consistent with Article 16 of the Argentine PDPA.

5.6 We do not process Personal Data on the basis of consent for any other purpose, and consequently no consent-withdrawal mechanism is required. Should we ever introduce Processing that requires consent under applicable law, we will obtain and document such consent before that Processing begins, and this Policy will be amended accordingly.

Article 6 — Purposes of Processing

6.1 We and the Providers process the technical data described in Article 4 for the following purposes only: (a) delivering and displaying the Site and operating its claim and delivery functions; (b) verifying the entitlement of a claimant to the linked digital asset; (c) securing the Service against abuse, bots, attacks and excessive automated traffic; (d) producing aggregate statistics that assist us in understanding general usage patterns and improving the Service; and (e) complying with the legal obligations applicable to us.

6.2 We do not use Personal Data for any purpose incompatible with those described in Clause 6.1. The verification of a cryptographic signature and of on-chain token ownership is a technical act performed at your request in order to deliver the service, and does not constitute automated decision-making, including profiling, producing legal effects concerning you or similarly significantly affecting you within the meaning of Article 22 GDPR.

Article 7 — Information Relating to Wallet Addresses and On-Chain Records

7.1 A wallet address is a pseudonymous identifier. Where a wallet address can be related to an identifiable natural person — for instance through the claim

interaction itself, or through linkage performed by third parties such as Wallet Providers, exchanges or public explorers — it constitutes Personal Data within the meaning of Article 4(1) GDPR, in accordance with the relative-identifiability standard developed in the case-law of the Court of Justice of the European Union.

7.2 On-chain records are public by design. Any participant of the network, and any member of the public through block explorers such as sepolia.basescan.org, can inspect the transactions, wallet addresses and metadata recorded on the Base Sepolia Testnet. The Operator publishes no additional index that links wallet addresses to identities: the Service performs no know-your-customer procedure, maintains no accounts and does not request any e-mail address in connection with a claim.

7.3 The Operator does not control the Base Sepolia Testnet, the Arweave Network or the AR.IO network. The European Data Protection Board has recognised, in its guidelines on the processing of Personal Data through blockchain technologies, that the tension between the immutability of distributed ledgers and erasure rights is a structural feature of the technology. As a mitigation, the Service writes to the chain only the data strictly necessary for the minting service requested, and no off-chain association between wallet addresses and identities is created by the Operator.

7.4 Because the Service operates on a test network with no economic value, no expectation of financial or patrimonial interest attaches to the records described in this Article, and the network itself may be subject to resets or deprecations outside the control of the Operator. No promise of erasure of on-chain records is made, as further described in Article 14.

Article 8 — Processing on Blockchain and Permanent Storage Networks

8.1 The Base Sepolia Testnet is a public, decentralised test network. Any transaction performed on it is recorded permanently, publicly and immutably. These characteristics are inherent to blockchain technology and cannot be modified by the Operator or by any other actor.

8.2 The data recorded on the network by a minting transaction are listed in Clause 4.3. The blockchain does not record IP addresses: your IP address is visible only to the

RPC Provider and to Cloudflare in the circumstances described in this Policy, is not written to the blockchain and cannot be reconstructed from a transaction hash.

8.3 The Arweave Network is a permanent, decentralised storage network based on a blockweave data structure. The files published on it by the Operator — principally the imagery displayed by the Site — are public and immutable by design, together with the metadata of their initial upload transactions, such as the transaction identifier, the owner address, the timestamp and the tags recorded on the underlying layer. The Operator has no technical ability to modify or remove them once the initial upload has been confirmed.

8.4 The Arweave Network does not register the IP addresses of users who consult or download files. The download of content hosted on it, as performed through the Gateways described in Clause 4.5, does not generate on-chain transactions or on-chain metadata.

8.5 By using the Service, you acknowledge the characteristics described in this Article. If you do not agree with them, you should abstain from minting an SBT and from displaying or downloading content hosted on the Arweave Network through the Site.

Article 9 — Cookies and Similar Technologies

9.1 The code of the Site sets no HTTP cookies for any purpose. The only HTTP cookies that may be stored in your browser are the strictly necessary security cookies imposed by the Cloudflare security layer in the exercise of its bot management and clearance functions, described in Clause 4.1. The only first-party client-side storage deployed by the Site is the Local Session Storage entry described in Clause 4.6.

9.2 The complete inventory of cookies and similar technologies used by the Service, together with the applicable management options, is set out in the Cookie and Local Storage Notice, which forms an integral part of this Legal Documentation.

Article 10 — Processors, Sub-Processors and Recipients

10.1 Cloudflare, Inc., with registered offices in San Francisco, California, United States, provides the hosting of the Site through Cloudflare Pages, the content delivery and security services, the bot management and clearance functions, the execution of the delivery function through Workers and the hosting of the downloadable assets in a managed bucket, and the cookieless analytics feature described in Clause 4.1. Cloudflare acts in the capacity of processor with respect to those services, and as an independent controller solely with respect to its own security and abuse-prevention records.

10.2 The Wallet Provider is selected by you and acts as an independent controller of the data it processes in the course of the connection, including the wallet address, the transactions you sign and your IP address, under its own privacy policy. The Operator does not control that processing and has no visibility over it.

10.3 Alchemy acts as the service provider that answers the on-chain ownership queries issued by your browser. Because the communication is established directly from your browser, the Operator transmits no Personal Data to Alchemy and has no access to its logs. When the public Base Sepolia endpoint is used as fallback, the equivalent processing is performed through the infrastructure of Base, under its own published privacy documentation.

10.4 Gateway operators are unrelated third parties. They process your IP address, the identifier of the requested asset and the timestamp in serving your requests, under their own terms of service and privacy policies.

10.5 The Base Sepolia Testnet and the Arweave Network are public registers and decentralised networks, and are not recipients of Personal Data in the traditional sense; the records described in Article 8 are incorporated into public registers that any person may consult.

10.6 To the extent that any Personal Data is within our effective control, we will disclose it to public authorities only where we are legally compelled to do so and, where lawfully permitted, we will inform the affected Visitor of such disclosure. Given the architecture described in this Policy, the Operator holds no visitor database that could be subject to such disclosure. Table 2 identifies the infrastructure providers of the Service.

Table 2 — Infrastructure providers and third parties

Provider / third party	Principal role	Data processed	Reference
Cloudflare, Inc.	Hosting of the Site (Cloudflare Pages); CDN; bot management and clearance; Workers execution of the delivery function; managed bucket hosting of downloadable assets; cookieless web analytics	IP address; request metadata; aggregated metrics	Privacy policy published at cloudflare.com
Wallet Provider (selected by you)	Wallet connection; message and transaction signing	Wallet address; signed transactions; IP address, under its own policy	Published by the provider you select
Alchemy Insights, Inc.	RPC queries on token ownership, issued directly by your browser	Wallet address; contract address; IP address (retained approximately 90 days through its infrastructure providers)	Privacy documentation published at legal.alchemy.com
Base public RPC endpoint (sepolia.base.org)	Fallback RPC infrastructure	Wallet address; contract address; IP address	Privacy policy published at docs.base.org
Gateway operators (arweave.net; AR.IO network)	Delivery of imagery hosted on the Arweave Network	IP address; asset identifier; timestamp	Published by each gateway operator
Base Sepolia Testnet; Arweave Network	Public, decentralised networks; not recipients in the traditional sense	On-chain and published records (public by design)	Block explorers such as sepolia.basescan.org

Article 11 — International Transfers

11.1 Cloudflare, the RPC Providers, the Wallet Providers, the Gateways and the nodes of the Base Sepolia Testnet and of the Arweave Network operate through infrastructure distributed globally. Consequently, the data described in Article 4 may be processed in servers located in various jurisdictions and be subject to international transfers.

11.2 Where the GDPR applies and Personal Data is transferred to a country not covered by an adequacy decision of the European Commission, the transfer is subject to appropriate safeguards, in particular the Standard Contractual Clauses adopted or approved by the European Commission, together with such supplementary technical and organisational measures as each provider implements. Information about the transfer mechanisms adopted by each provider is available in the respective privacy documentation of that provider.

11.3 The records incorporated into the Base Sepolia Testnet and the files published on the Arweave Network are, by their nature, public and globally accessible from any node. That incorporation constitutes the making available of information in a public register rather than a traditional transfer to an identified recipient, and is disclosed and limited as described in Articles 7 and 8.

11.4 Visitors who wish to obtain further information about the safeguards applied to international transfers may contact us at curses.trinity426@slmails.com.

Article 12 — Retention

12.1 We do not operate any database of Visitor Personal Data and, as a matter of design, retain no visitor records of our own beyond the correspondence described in Clause 12.7 and the aggregate dashboards exposed by the analytics feature.

12.2 Verification Data is held in memory for the few seconds required by the verification and is then discarded; it is never written to disk and never logged.

12.3 The technical data described in Clause 4.1 is retained, if at all, by Cloudflare, Inc. pursuant to its standard retention and logging policies — approximately 30 days for security logs and 3 to 7 days for Workers logs — which are determined by Cloudflare, Inc. and not by the Operator.

12.4 The IP address processed by the RPC Provider is retained by Alchemy for approximately ninety (90) consecutive days through its infrastructure providers, in accordance with its own published documentation; the fallback public endpoint applies the retention described in the privacy documentation of Base.

12.5 The Local Session Storage entry is retained in your browser only until you delete it or clear it through the browser settings.

12.6 The on-chain records described in Clause 4.3 and the files published on the Arweave Network are permanent and cannot be deleted or modified, as described in Articles 8 and 14.

12.7 Contact data provided voluntarily by a Visitor is retained for a maximum of two (2) years counted from the last interaction, unless an earlier erasure request is received.

12.8 In the event of a verified erasure request, we will action it directly where the relevant data is within our control and will otherwise provide the Visitor with reasonable assistance in directing the request to the relevant provider.

Article 13 — Your Rights

13.1 Under the GDPR, where applicable, Visitors have the rights of access, rectification, erasure, restriction of Processing, data portability and objection, as well as the right to lodge a complaint with a competent supervisory authority, in each case subject to the conditions and exceptions established by that regime and to the limitations described in Article 14.

13.2 Under the CCPA, California residents have the rights to know, to delete, to correct and to limit the use and disclosure of their Personal Data, as well as the right to opt out of its sale or sharing. We do not sell and do not share Personal Data as those terms are defined by the CCPA, and Visitors who exercise any right under the CCPA will not be discriminated against in any way.

13.3 Under the LGPD, data subjects have, among others, the rights of confirmation of Processing, access, correction, anonymisation, blocking or deletion of unnecessary or excessive data, data portability, information on third parties with whom data has been shared, and review of decisions taken solely on the basis of automated Processing, in each case subject to the conditions established by that regime and by

the Brazilian supervisory authority (Autoridade Nacional de Proteção de Dados – ANPD).

13.4 Under the Argentine PDPA, data subjects are entitled to access, rectify, update and, where applicable, delete (suppress) Personal Data contained in registers or databases within our control, and may address the competent enforcement authority (Agencia de Acceso a la Información Pública – AAIP) in accordance with the applicable procedures.

13.5 To exercise any of the rights described in this Article, please send a request to curses.trinity426@slmails.com, indicating clearly the right you wish to exercise. Because the Service does not collect or store direct identifying data and does not maintain user accounts, the Operator cannot verify identity against pre-existing records. Consequently, where a request concerns data linked to a wallet address, the Operator may require the requester to demonstrate control of that wallet by means of a cryptographic signature over a message issued by the Operator, or by another equivalent means. Where a request concerns contact data provided voluntarily, the Operator may verify identity by matching the e-mail address of origin. Requests are answered within ten (10) business days of receipt, consistent with Article 16 of the Argentine PDPA; in complex cases this period may be extended to a maximum of thirty (30) business days, with notice of the extension and of its reasons.

13.6 Nothing in this Article limits any right that cannot be limited by law, including the mandatory consumer protections of the Visitor’s place of residence.

Article 14 — Limitations on Erasure Arising from Immutable Technologies

14.1 The right to erasure cannot be exercised in full over the records registered on the Base Sepolia Testnet or over the files stored on the Arweave Network, owing to the immutability inherent in those technologies. This limitation is technical, not legal, and affects any service that uses blockchain or decentralised permanent storage. The regulatory community has acknowledged this conflict, notably in the guidelines of the European Data Protection Board on blockchain technologies.

14.2 Upon receiving an erasure request, the Operator: (a) confirms in writing that no off-chain data associated with the wallet address exists — the Service keeps no accounts, no databases, no claimant records and no download records — and erases

the correspondence data within its control; (b) cannot erase the on-chain records on the Base Sepolia Testnet, since they are immutable by design, and in consequence limits its Processing of those records to the purposes that justified their registration and does not use them for any additional purpose; and (c) cannot erase the files published by the Operator on the Arweave Network, since they are immutable by design.

14.3 Because the Service creates no off-chain association between wallet addresses and identities, there exists no profile, record or database that could be erased in substitution of the on-chain records. The architectural minimisation described in Article 3 is the Operator's principal means of giving effect to the spirit of erasure rights in an immutable environment.

Article 15 — Children

15.1 The Service is a technical demonstration project that is not directed to children. We do not knowingly collect Personal Data from children under the age of thirteen (13), nor from minors below the age at which the consent of the holder of parental responsibility is required under the law applicable to them. The use of a Wallet presupposes the technical capacity to manage cryptographic keys and transactions, which is presumed to correspond to an adult.

15.2 If a parent or guardian believes that a child has provided Personal Data through the Service, the parent or guardian may contact us at curses.trinity426@slmails.com, and we will take reasonable steps to delete such information where it is within our control.

Article 16 — Security

16.1 The Site is delivered exclusively over encrypted HTTPS connections and is protected by the Cloudflare security layer, including DDoS mitigation, a web application firewall and bot management. The delivery function is architecturally stateless: it processes Verification Data in memory only, writes nothing to disk and keeps no records. This minimisation by design constitutes the primary safeguard of the Service. The Operator handles no passwords and no payment instruments of any kind.

16.2 The Providers maintain industry-standard security programmes for their platforms. Nevertheless, no method of transmission or storage over the Internet is completely secure, and we cannot guarantee the absolute security of data processed by third parties.

16.3 In the event of a personal data breach affecting Personal Data within our control, we will notify the competent supervisory authority without undue delay and, where feasible, no later than seventy-two (72) hours after having become aware of it, in accordance with Article 33 GDPR, and we will communicate the breach to the affected Visitors without undue delay in accordance with Article 34 GDPR where the breach is likely to result in a high risk to their rights and freedoms.

Article 17 — Do Not Track and Opt-Out Signals

17.1 Some browsers offer a “Do Not Track” signal or equivalent opt-out preference signals. Since the Service does not engage in cross-site tracking, behavioural advertising or the sale of browsing information, no response to such signals is required or implemented. The setting therefore has no practical effect on the Service, because there is no tracking to disable.

Article 18 — Changes to this Policy

18.1 We may amend this Policy from time to time to reflect changes in the Service, in the technologies employed or in applicable law. The amended version will be published on the Site with a new effective date and version number recorded in the document control table of this documentation.

18.2 Because the Service is a static portfolio project, no material expansion is planned. Nevertheless, where an amendment materially affects the rights of Visitors — including, among others, the incorporation of new services that process Personal Data or a change in the purposes of Processing — a prominent notice will be published on the Site for a reasonable period in order to inform Visitors of the change.

18.3 Visitors are encouraged to review this Policy periodically. Continued use of the Service after the effective date of an amendment constitutes acknowledgement of the amended Policy.

Article 19 — Contact, Controller Identification and Complaints

19.1 The controller of the Processing described in this Policy is: Fabiola Serralunga, Buenos Aires, Argentina. Contact: curses.trinity426@slmails.com.

19.2 You have the right to lodge a complaint with a competent supervisory authority if you consider that the Processing of your Personal Data infringes applicable law. The competent authorities include, among others: in Argentina, the Agencia de Acceso a la Información Pública (AAIP); in the European Union, the data protection authority of the Member State of your residence; in the State of California (United States), the Attorney General of the State of California; and in Brazil, the Autoridade Nacional de Proteção de Dados (ANPD). You may address those authorities without prior contact with the Operator, although a direct approach to curses.trinity426@slmails.com is recommended in the first instance so that we may attempt to resolve the matter.