Personal Data Processing Policy - SEAL

Introduction

SEAL is a platform created by Santiago Viana, Juan Pablo Vesga, Miguel Santamaría, Julio Cesar Arango, and Oscar Riojas, dedicated to certifying participants' attendance at courses and academic events through blockchain technology. As part of its activities, it collects, stores, and processes participants' personal data to issue secure and immutable digital certificates via NFTs.

To comply with the current data protection legislation, especially Law 1581 of 2012, Decree 1377 of 2013, and any other laws that modify, complement, or develop these regulations, this document outlines relevant aspects of the collection, use, and transfer of personal data performed by the Data Controllers based on the authorization provided by the Data Subject for such management and processing.

This Personal Data Processing Policy establishes the guidelines under which the Data Controllers will perform data processing, their purposes, the rights of the Data Subjects, and the internal and external procedures for exercising these rights.

Objectives

To establish the criteria applicable to the collection, storage, use, dissemination, and deletion of personal data collected and processed by the Data Controllers as part of SEAL’s activities.

This policy includes guidelines for all natural persons who are clients, users, suppliers, contractors, or any third party associated with the Data Controllers concerning the SEAL platform.

Scope

This Policy applies to all personal information registered in SEAL's databases, a platform created by Santiago Viana, Juan Pablo Vesga, Miguel Santamaría, Julio Cesar Arango, and Oscar Riojas, who act as Data Controllers for personal data processing.

This Policy applies to the Data Controllers, their collaborators, and any individual who has agreed to accept it.

Definitions

- **Authorization:** Prior, explicit, and informed consent of the Data Subject to process personal data.
- **Database:** An organized collection of personal data that is subject to processing.
- **Personal Data:** Any information linked to or that can be associated with one or more identified or identifiable natural persons.
- **Private Data:** Data that, by its intimate or reserved nature, is only relevant to the Data Subject.
- **Public Data:** Data that is neither semi-private, private, nor sensitive. Examples of public data include information related to a person's marital status, profession, occupation, or status as a public servant. Public data may be found in public records, official gazettes, or judicial decisions that are not confidential.
- **Sensitive Personal Data:** Data that affects the Data Subject's privacy or whose misuse could lead to discrimination. Examples include data revealing racial or ethnic origin, political orientation, religious or philosophical beliefs, union membership, health information, sexual life, and biometric data.
- **Data Processor:** A natural or legal person, public or private, who, alone or in association with others, processes personal data on behalf of the Data Controller.
- **Data Controller:** A natural or legal person, public or private, who, alone or in association with others, decides on the database and/or personal data processing.
- **Data Subject:** A natural person whose personal data is subject to processing.
- **Transfer:** The act of sending personal data from the Data Controller and/or Processor in Colombia to a recipient who also acts as a Data Controller within or outside the country.
- **Transmission:** The act of communicating personal data within or outside Colombia to allow for processing by the Processor on behalf of the Data Controller.
- **Processing:** Any operation or set of operations performed on personal data, such as collection, storage, use, dissemination, or deletion.
- **Blockchain:** A digital recording system that enables the creation and certification of immutable and transparent transactions.
- **Encryption:** The process of converting data into a secure format that is inaccessible to unauthorized individuals.

Principles for the Processing of Personal Data

The processing of personal data shall adhere to the following principles:

1. **Legality in Data Processing:** Processing is a regulated activity that must comply with the provisions of applicable laws and regulations.
2. **Purpose:** Processing must have a legitimate purpose under the Constitution and the law, which must be informed to the Data Subject.
3. **Freedom:** Processing may only be conducted with the Data Subject's prior, explicit, and informed consent. Personal data may not be obtained or disclosed without prior authorization or a legal or judicial mandate that waives the requirement for consent.

4. **Accuracy:** Information subject to processing must be truthful, complete, accurate, up-to-date, verifiable, and understandable. The processing of partial, incomplete, or misleading data is prohibited.
5. **Transparency:** Data Subjects have the right to access information about the existence of their data held by the Data Controller or Processor at any time and without restrictions.
6. **Restricted Access and Circulation:** Processing is subject to limitations based on the nature of personal data and legal and constitutional provisions. Only authorized individuals and entities may access and process personal data.
7. **Security:** Data Controllers and Processors must implement the necessary technical, human, and administrative measures to ensure data security, preventing unauthorized alteration, loss, consultation, or access.
8. **Confidentiality:** All individuals involved in the processing of personal data that is not public are required to maintain the confidentiality of the information, even after the conclusion of their relationship with the processing activities. Personal data may only be disclosed or communicated when necessary for authorized activities under the law.

Purposes of Processing

- To create and register participants in SEAL's internal databases as part of its community of interest.
- To verify the identity of attendees at events and academic activities.
- To issue digital attendance certificates for events and academic activities using blockchain technology.
- To send notifications and updates about the issuance of attendance certificates.
- To securely store encrypted data.
- To investigate and respond to complaints from clients and users.
- To conduct customer satisfaction surveys.
- To send promotional messages about SEAL's services.
- To fulfill all activities necessary to achieve SEAL's objectives.

Once data is stored on the blockchain as part of SEAL's services, it becomes publicly accessible and beyond SEAL's control.

If the need for data processing ceases, the data may be deleted from the Data Controllers' databases or securely archived for lawful use.

Personal Data Collected

The Data Controllers process personal data in compliance with this Policy, Law 1581 of

2012, Decree 1377 of 2013, and other applicable regulations. To this end, they collect, store, use, organize, update, and delete information as required for each specified purpose.

Any individual with access to SEAL's data containing personal information must comply with this Policy, applicable regulations, and any other data protection-related documents issued by SEAL.

Processing of Public Data

Under Article 19 of Law 1581 of 2012, the Data Controllers may process public data without prior authorization. However, they will adopt necessary measures to ensure compliance with obligations under applicable regulations.

Processing of Sensitive Data

The Data Controllers only process sensitive data when strictly necessary and in compliance with general requirements established by applicable data protection laws and the specific requirements for sensitive data.

Processing of Data of Minors

The Data Controllers process personal data of minors only when strictly necessary and in compliance with the general requirements established by applicable data protection laws and the specific requirements for data of minors. This processing prioritizes the best interests of minors and guarantees the protection of their fundamental rights.

For the processing of minors' personal data, authorization will be obtained from their legal representatives. The minors' opinion will be considered, considering their maturity, autonomy, and ability to understand the content of the authorization and the nature of the data processing.

Data Security

The Data Controllers adopt technical, administrative, and technological measures to ensure the security of personal data. These include:

- Encrypting personal data before storing it on the blockchain.
- Storing data in immutable databases inaccessible to unauthorized third parties.
- Using digital certificates for authentication during issuance.
- Protecting against unauthorized access and modification of stored data.

Visual data for certificates is stored using the InterPlanetary File System (IPFS), a decentralized storage network that segments and distributes information across

interconnected nodes. Since there is no central server for data storage, once a file is uploaded to IPFS, it is assigned a unique identifier based on its content (hash or CID), ensuring the file remains immutable.

Rights of Data Subjects

In accordance with Article 8 of Law 1581 of 2012, Data Subjects have the following rights:

a) To know, update, and correct their personal data with the Data Controllers or Processors. This includes addressing partial, inaccurate, incomplete, or misleading data, or data whose processing is explicitly prohibited or unauthorized.
b) To request proof of the authorization provided to the Data Controller, except when authorization is not required by law.
c) To be informed by the Data Controller or Processor, upon request, about the use of their personal data.
d) To file complaints with the Superintendence of Industry and Commerce for violations of the law or other applicable regulations.
e) To revoke authorization and/or request the deletion of data when its processing does not comply with constitutional and legal principles, rights, or guarantees.
f) To access their personal data free of charge, provided it has been processed.

Data Retention

Personal data will only be retained for as long as necessary to fulfill the purposes for which it was processed. However, blockchain-issued certificates, being permanent and immutable, will remain indefinitely recorded.

Transfer and Transmission of Personal Data

The Data Controllers may subcontract third parties to perform specific functions or process data. When personal data is shared with third parties, these entities will be informed of their obligation to protect the data using at least the same security standards as those employed by the Data Controllers.

Unless authorized by the Data Subject, personal data cannot be processed or disclosed for unrelated purposes. These third parties will assume the role of Data Processors, and the relationship will be formalized in a data transmission agreement.

The Data Controllers may transfer or transmit personal data to other entities abroad for reasons of security, administrative efficiency, or improved service, provided the Data Subjects authorize such actions. Measures will be taken to ensure that the receiving entities implement equivalent data protection measures under their jurisdiction.

Policy Modifications
The Data Controllers reserve the right to modify this Policy at any time. Any updates will be communicated to Data Subjects by publishing the revised version on SEAL's website.

Procedure for Exercising Data Protection Rights (Habeas Data)
To comply with personal data protection laws, the Data Controllers outline the following procedure and minimum requirements for exercising rights:

Requests must be submitted to **info@sealweb3.com** and include the following information:

1. Full name.
2. Contact details: phone number, physical address, and/or email.
3. Reason(s) for the request, including a description of the right the Data Subject wishes to exercise.
4. Signature and identification number.

The maximum timeframes for responding to requests are:

- **Consultations:** Ten (10) business days from the date of receipt.
- **Complaints:** Fifteen (15) business days from the date of receipt.

If a response cannot be provided within the established timeframe, the Data Controllers will inform the Data Subject of the reasons for the delay and provide a resolution date. This new date will be at most five (5) business days for consultations or eight (8) business days for complaints.

If the Data Subject's rights to access, update, rectify, revoke, or delete data are denied, wholly or partially, they may report the case to the Personal Data Protection Division of the Superintendence of Industry and Commerce.

Effective Date
This Policy is effective as of October 1, 2024. Amendments to this Policy will take effect from the date of publication on SEAL's website.

Databases containing personal data will remain active for as long as necessary to achieve the purposes described in this Policy.