verifiable LEI (vLEI) Ecosystem Governance Framework
vLEI Ecosystem Information Trust Policies

Document Name:	vLEI Ecosystem Information Trust Policies
Document DID:	
Version Number:	0.7
Version Date:	
Governance Authority:	Global Legal Entity Identifier Foundation (GLEIF)
Governance Authority DID:	
Copyright:	

1 Introduction

This is a Controlled Document of the GLEIF vLEI Ecosystem Governance Framework (vLEI Ecosystem Governance Framework). The document defines the information security, privacy, availability and confidentiality policies that apply to all vLEI Ecosystem Members regardless of their particular role or the particular type of vLEI Credential being exchanged. Policies that apply to the issuance, holding, or verification of a specific type of vLEI Credentials are defined in the vLEI Credential Governance Framework for that credential type. For an overview of the vLEI Ecosystem Governance Framework, please see the following section on the GLEIF website [INSERT URL HERE].

2 Terminology

All terms in First Letter Capitals are defined in the vLEI Glossary.

3 Regulatory Compliance

vLEI Ecosystem Members MUST comply with any governmental regulations for information security to which their activities within the vLEI Ecosystem will be subject. This includes International or trans-national governance authorities (e.g., ISO/IEC 27001 – Information Security Management, EU General Data Protection Regulation (GDPR).

4 vLEI Ecosystem Member Privacy Policies

1. Legal Entities that receive vLEI Legal Entity Credentials SHOULD ensure that their privacy policies adequately protect the persons to whom the Legal Entity requests Legal Entity Official Organizational Role vLEI Credentials and Legal Entity Engagement Context Role vLEI Credentials.

2. The vLEI Ecosystem Credential Governance Frameworks MUST specify the information to be protected by the applicable privacy policy in the jurisdiction of the Legal Entity.

5 vLEI Ecosystem Member Data Protection Policies

1. vLEI Ecosystem Members MUST confirm that they respect and comply with data protection legislation as applicable and in force.

2. Where no such legislation is in force, and as a material minimum standard, vLEI Ecosystem Members MUST comply with the provisions of the Swiss Federal Data Protection Act specified in the Appendix to this policy document.

3. vLEI Ecosystem Members MAY use Personal Data for the purpose of performing their obligations and rights under this Agreement. vLEI Ecosystem Members MUST comply with:
    a. the material applicability of the provisions of the Swiss Federal Data Protection Act or
    b. about local data protection legislation applicable to the vLEI Ecosystem Member if such legislation is equivalent or more rigorous.

4. Qualified vLEI Issuers MUST annually review and document that the provisions are implemented and enforced. Other vLEI Ecosystem Members SHOULD undertake to regularly review and ensure that the provisions of this Section 5 are implemented and enforced.

5. When a privacy breach is suspected, the involved vLEI Ecosytem Members MUST inform each other about actual or potential disclosure(s) of Personal Data and promptly take appropriate measures to address the situation and to limit the risk of such disclosure(s) from reoccurrence. For Qualified vLEI Issuers, privacy breaches MUST be documented in an Incident Report.

6. Qualified vLEI Issuers MUST document privacy breaches in an Incident Report .

6 vLEI Ecosystem Member Security Policies

1. vLEI Ecosystem Members MUST publish, review annually, maintain, and comply with IT security policies and practices sufficient to protect all services that a vLEI Ecosystem Member provides in conformance with this Ecosystem Governance Framework and meets the minimum elements of the following recommendations: https://resources.infosecinstitute.com/topic/key-elements-information-security-policy/#gref

2. These policies MUST be mandatory for all employees of the vLEI Ecosystem Member involved with vLEI Data. The vLEI Ecosystem Member MUST designate its Information Security Manager or another officer to provide executive oversight for such policies, including formal governance and revision management, employee education, and compliance enforcement.

3. vLEI Ecosystem Member employment verification policies and procedures MUST include, but may not be limited to, criminal background check and proof of identity validation.

4. Qualified vLEI Issuers MUST recertify annually that they maintain a law abiding and ethical status in the business community as evidenced in the Annual vLEI Issuer Qualification.

5. If a Qualified vLEI Issuer performs handling of vLEI Data in its own data center, the Qualified vLEI Issuer's security policies MUST also adequately address physical security and entry control according to industry best practices.

6. If a Qualified vLEI Issuer uses third-party providers in functions that involve the handling of vLEI Data, the Qualified vLEI Issuer MUST ensure that the security, privacy, and data protection policies of the third-party providers meet the requirements in this document.

7. Qualified vLEI Issuers MUST make available evidence of stated compliance with these policies and any relevant accreditations held by the Qualified vLEI Issuer during Annual vLEI Issuer Qualification, including certificates, attestations, or reports resulting from accredited third-party audits, such as ISO 27001, Statement on Standards for Attestation Engagements Service Organization Controls 2 (SSAE SOC 2), or other industry standards.

7 Security Incidents Policies

1. Qualified vLEI Issuers MUST maintain and follow documented incident response procedures and guidelines for computer security incident handling and will comply with data breach notification terms of the vLEI Issuer Qualification Agreement. ITIL (Information Technology Infrastructure Library) Incident Management is followed by GLEIF and is certified as part of GLEIF's ISO 20000 certification.

2. Qualified vLEI Issuers MUST define and execute an appropriate response plan to investigate suspected unauthorized access to vLEI Data. GLEIF and the Qualified vLEI Issuers will handle through the Incident Management process.

8 Availability Policies

1. GLEIF and Qualified vLEI Issuers MUST maintain defined availability targets as part of the vLEI Ecosystem Governance Framework.

2. GLEIF and Qualified vLEI Issuers MUST maintain records to evidence the availability of their services.

9 Developer Security Policies

1. GLEIF MUST provide technical changes/upgrades to the GLEIF-supplied vLEI software to Qualified vLEI Issuers.

2. Qualified vLEI Issuers MUST successfully install, test and implement the GLEIF-supplied vLEI software within stated timeframes.

3. Developers of Qualified vLEI Issuers SHOULD follow the security recommendations in section 8 of the W3C Verifiable Credentials Data Model 1.0 specification and the Trust over IP Authentic Chained Data Containers (ACDC) specification when designing software or services for use with vLEI Credentials and the vLEI Ecosystem.

Appendix

Applicable Provisions of the Swiss Data Protection Act (DPA) including the pertaining Ordinance (DPO)

Note: The following is an excerpt of the Swiss Federal Act on Data Protection of 19 June 1992 ("DPA", Status as of 1 January 2014 and of the pertaining Ordinance ("DPO", Status as of 14 June 2010)

Swiss Federal Act on Data Protection (DPA)

Chapter 1: Aim, Scope and Definitions

Art. 1 Aim

This Act aims to protect the privacy and the fundamental rights of persons when their data is processed.

Art. 2 Scope

1. This Act applies to the processing of data pertaining to natural persons and legal persons by:
    a. private persons; [note: this includes private legal entities]
    b. federal bodies.
2. It does not apply to: [note: not relevant in the context of GLEIF- Qualified vLEI Issuer]

Art. 3 Definitions

The following definitions apply:

a. personal data (data): all information relating to an identified or identifiable person;
b. data subjects: natural or legal persons whose data is processed;
c. sensitive personal data: data on:
    i. religious, ideological, political or trade union-related views or activities,
    ii. health, the intimate sphere or the racial origin,
    iii. social security measures,
    iv. administrative or criminal proceedings and sanctions;
d. personality profile: a collection of data that permits an assessment of essential characteristics of the personality of a natural person;
e. processing: any operation with personal data, irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, disclosure, archiving or destruction of data;
f. disclosure: making personal data accessible, for example by permitting access, transmission or publication;
g. data file: any set of personal data that is structured in such a way that the data is accessible by data subject;
h. federal bodies: [note: not relevant in the context of GLEIF-Qualified vLEI Issuer]

i. controller of the data file: private persons or federal bodies that decide on the purpose and content of a data file;
j. formal enactment: [note: not relevant in the context of GLEIF- Qualified vLEI Issuer]

Chapter 2: General Data Protection Provisions

Art. 4 Principles

1. Personal data may only be processed lawfully.

2. Its processing must be carried out in good faith and must be proportionate.

3. Personal data may only be processed for the purpose indicated at the time of collection, that is evident from the circumstances, or that is provided for by law.

4. The collection of personal data and in particular the purpose of its processing must be evident to the data subject.

5. If the consent of the data subject is required for the processing of personal data, such consent is valid only if given voluntarily on the provision of adequate information. Additionally, consent must be given expressly in the case of processing of sensitive personal data or personality profiles.

Art. 5 Correctness of the data

1. Anyone who processes personal data must make certain that it is correct. He must take all reasonable measures to ensure that data that is incorrect or incomplete in view of the purpose of its collection is either corrected or destroyed.

2. Any data subject may request that incorrect data be corrected.

Art. 6 Cross-border disclosure

1. Personal data may not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular due to the absence of legislation that guarantees adequate protection.

2. In the absence of legislation that guarantees adequate protection, personal data may be disclosed abroad only if:
    a. sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad;
    b. the data subject has consented in the specific case;
    c. the processing is directly connected with the conclusion or the performance of a contract and the personal data is that of a contractual party;
    d. disclosure is essential in the specific case in order either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts;
    e. disclosure is required in the specific case in order to protect the life or the physical integrity of the data subject;

f. the data subject has made the data generally accessible and has not expressly prohibited its processing;
g. disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules that ensure an adequate level of protection.

3. [note: not relevant in the context of GLEIF- Qualified vLEI Issuer]

Art. 7 Data security

1. Personal data must be protected against unauthorised processing through adequate technical and organisational measures.

2. The Federal Council issues detailed provisions on the minimum standards for data security.

Art. 8 Right to information

1. Any person may request information from the controller of a data file as to whether data concerning them is being processed.

2. The controller of a data file must notify the data subject:
   a. of all available data concerning the subject in the data file, including the available information on the source of the data;
   b. the purpose of and if applicable the legal basis for the processing as well as the categories of the personal data processed, the other parties involved with the file and the data recipient.

3. The controller of a data file may arrange for data on the health of the data subject to be communicated by a doctor designated by the subject.

4. If the controller of a data file has personal data processed by a third party, the controller remains under an obligation to provide information. The third party is under an obligation to provide information if he does not disclose the identity of the controller or if the controller is not domiciled in Switzerland.

5. The information must normally be provided in writing, in the form of a printout or a photocopy, and is free of charge. The Federal Council regulates exceptions.

6. No one may waive the right to information in advance.

Art. 9 Limitation of the duty to provide information

1. The controller of a data file may refuse, restrict or defer the provision of information where:
   a. a formal enactment so provides;
   b. this is required to protect the overriding interests of third parties.

2. [note: not relevant in the context of GLEIF- Qualified vLEI Issuer]

3. As soon as the reason for refusing, restricting or deferring the provision of information ceases to apply, the federal body must provide the information unless this is impossible or only possible with disproportionate inconvenience or expense.

4. The private controller of a data file may further refuse, restrict or defer the provision of information where his own overriding interests so require and he does not disclose the personal data to third parties.

5. The controller of a data file must indicate the reason why he has refused, restricted or deferred access to information.

Art. 10 [note: not relevant in the context of GLEIF- Qualified vLEI Issuer]

Art. 10a Data processing by third parties

1. The processing of personal data may be assigned to third parties by agreement or by law if:
    a. the data is processed only in the manner permitted for the instructing party itself; and
    b. it is not prohibited by a statutory or contractual duty of confidentiality.

2. The instructing party must in particular ensure that the third party guarantees data security.

3. Third parties may claim the same justification as the instructing party.

Art. 11 [note: not relevant in the context of GLEIF- Qualified vLEI Issuer]

Art. 11a [note: not relevant in the context of GLEIF- Qualified vLEI Issuer]

Chapter 3: Processing of Personal Data by Private Persons

Art. 12 Breaches of privacy

1. Anyone who processes personal data must not unlawfully breach the privacy of the data subjects in doing so.

2. In particular, he must not:
    a. process personal data in contravention of the principles of Articles 4, 5 paragraph 1 and 7 paragraph 1;
    b. process data pertaining to a person against that person's express wish without justification;
    c. disclose sensitive personal data or personality profiles to third parties without justification.

3. Normally there is no breach of privacy if the data subject has made the data generally accessible and has not expressly prohibited its processing.

Art. 13 Justification

1. A breach of privacy is unlawful unless it is justified by the consent of the injured party, by an overriding private or public interest or by law.

2. An overriding interest of the person processing the data shall in particular be considered if that person:
    a. processes personal data in direct connection with the conclusion or the performance of a contract and the personal data is that of a contractual party;
    b. is or intends to be in commercial competition with another and for this purpose processes personal data without disclosing the data to third parties;
    c. process data that is neither sensitive personal data nor a personality profile in order to verify the creditworthiness of another, and discloses such data to third parties only if the data is required for the conclusion or the performance of a contract with the data subject;
    d. processes personal data on a professional basis exclusively for publication in the edited section of a periodically published medium;
    e. processes personal data for purposes not relating to a specific person, in particular for the purposes of research, planning and statistics and publishes the results in such a manner that the data subjects may not be identified;
    f. collects data on a person of public interest, provided the data relates to the public activities of that person.

Art. 14 Duty to provide information on the collection of sensitive personal data and personality profiles

1. The controller of the data file is obliged to inform the data subject of the collection of sensitive personal data or personality profiles; this duty to provide information also applies where the data is collected from third parties.

2. The data subject must be notified as a minimum of the following:
    a. the controller of the data file;
    b. the purpose of the processing;
    c. the categories of data recipients if a disclosure of data is planned.

3. If the data is not collected from the data subject, the data subject must be informed at the latest when the data is stored or if the data is not stored, on its first disclosure to a third party.

4. The duty of the controller of the data file to provide information ceases to apply if the data subject has already been informed or, in cases under paragraph 3, if:
    a. the storage or the disclosure of the data is expressly provided for by law; or
    b. the provision of information is not possible or possible only with disproportionate inconvenience or expense.

5. The controller of the data file may refuse, restrict or defer the provision of information subject to the requirements of Article 9 paragraphs 1 and 4.

[note: the remainder of the Act (Articles 15-39) is not relevant in the context of GLEIF- Qualified vLEI Issuer]

Ordinance to the Federal Act on Data Protection (DPO)

Chapter 1: Processing of Personal Data by Private Persons

Section 1: Right of Access

Art. 1 Modalities

1. Anyone who requests information from the controller of a data file on whether data concerning them is being processed (Art. 8 DPA) must normally request the information in writing and provide proof of their identity.
2. Requests for information as well as the provision of information may also be made online if the controller of the data file expressly arranges for this and takes appropriate measures to:
    a. guarantee the identification of the data subject; and
    b. protect the personal data of the data subject when providing information against unauthorised access by third parties.
3. With the agreement of the controller of the data file or at his suggestion, the data subject may inspect their data in situ. The information may also be provided verbally if the data subject has consented and has been identified by the controller.
4. The information or the substantiated decision on the restriction of the right of access (Art. 9 and 10 DPA) is provided within 30 days of receipt of the request for information. If the information cannot be provided within 30 days, the controller of the data file must notify the applicant of this and of the date by which the information will be provided.
5. If one or more data files are jointly held by two or more controllers, the right of access may be asserted against each controller, unless one of them is responsible for processing all requests for information. If the controller of the data file is not authorised to provide information, he shall pass the request on to the person responsible.
6. If the request for information relates to data that is being processed by a third party on behalf of the controller of the data file, the controller shall pass the request on to the third party for processing if the controller is not able to provide the information himself.
7. If information is requested on data relating to deceased persons, it must be provided if the applicant proves an interest in the information that is not countered by the overriding interests of relatives of the deceased or third parties. Close relatives and persons who have been married to the deceased have a justified interest.

Art. 2 Exceptions to the exemption from costs

1. The payment of an appropriate share of the costs may by way of exception be requested if:
    a. the applicant has already been provided with the requested information in the twelve months prior to the application and no legitimate interest in the further provision of information can be proven. A legitimate interest is constituted in particular if the personal data has been modified without notice being given to the data subject;
    b. the provision of information entails an exceptionally large amount of work.

2. The share of the costs amounts to a maximum of 300 francs. The applicant must be notified of the amount of the share before the information is provided and may withdraw his request within ten days.

Section 2: [note: not relevant in the context of GLEIF- Qualified vLEI Issuer]

Section 3: Transborder Disclosure

Art. 5 Publication in electronic form

If personal data is made generally accessible by means of automated information and communications services for the purpose of providing information to the general public[1], this is not deemed to be transborder disclosure.

Art. 6 Duty to provide information

1. [note: not relevant in the context of GLEIF- Qualified vLEI Issuer]
2. [note: not relevant in the context of GLEIF- Qualified vLEI Issuer]
3. The duty to provide information is [...] regarded as fulfilled if data is transmitted on the basis of model contracts or standard contract clauses that have been drawn up or approved by the Commissioner, and the Commissioner has been informed about the use of these model contracts or standard contract clauses by the controller of the data file. The Commissioner shall publish a list of the model contracts and standard contract clauses that he has drawn up or approved. [note: the Model Clauses of the European Union are approved].
4. The controller of the data file shall take appropriate measures to ensure that the recipient complies with the safeguards and the data protection rules.
5. [note: not relevant in the context of GLEIF- Qualified vLEI Issuer]

Art. 7 [note: not relevant in the context of GLEIF- Qualified vLEI Issuer]

Section 4: Technical and organisational measures

Art. 8 General measures

1. Anyone who as private individual processes personal data or provides a data communication network shall ensure the confidentiality, availability and the integrity of the data in order to ensure an appropriate level of data protection. In particular, he shall protect the systems against the following risks:
    a. unauthorised or accidental destruction;
    b. accidental loss;
    c. technical faults;
    d. forgery, theft or unlawful use;
    e. unauthorised alteration, copying, access or other unauthorised processing.

[*]For the avoidance of doubt, "general public" in Art. 5 DPO is the English translation of the term in the three national languages of Switzerland, i.e. of the German "die Öffentlichkeit", of the equivalent French "le public" and of the equivalent Italian "il pubblico", respectively. This term, as used in the DPO, is (legally, contractually) unrelated to the definition of "General Public" in the Master Agreement.

2. The technical and organisational measures must be adequate. In particular, they must take account of the following criteria:
    a. the purpose of the data processing;
    b. the nature and extent of the data processing;
    c. an assessment of the possible risks to the data subjects;
    d. the current state of the art.
3. These measures must be reviewed periodically.

Art. 9 Special measures

1. The controller of the data file shall, in particular for the automated processing of personal data, take the technical and organisational measures that are suitable for achieving the following goals in particular:
    a. entrance control: unauthorised persons must be denied the access to facilities in which personal data is being processed;
    b. personal data carrier control: unauthorised persons must be prevented from reading, copying, altering or removing data carriers;
    c. transport control: on the disclosure of personal data as well as during the transport of data carriers, the unauthorised reading, copying, alteration or deletion of data must be prevented;
    d. disclosure control: data recipients to whom personal data is disclosed by means of devices for data transmission must be identifiable;
    e. storage control: unauthorised storage in the memory as well as the unauthorised knowledge, alteration or deletion of stored personal data must be prevented;
    f. usage control: the use by unauthorised persons of automated data processing systems by means of devices for data transmission must be prevented;
    g. access control: the access by authorised persons must be limited to the personal data that they required to fulfilment their task;
    h. input control: in automated systems, it must be possible to carry out a retrospective examination of what personal data was entered at what time and by which person.
2. The data files must be structured so that the data subjects are able to assert their right of access and their right to have data corrected.

Art. 10 Records

1. The controller of the data file shall maintain a record of the automated processing of sensitive personal data or personality profiles if preventive measures cannot ensure data protection. Records are necessary in particular if it would not otherwise be possible to determine subsequently whether data has been processed for the purposes for which it was collected or disclosed. [note: remainder of para.1 not relevant in the context of GLEIF- Qualified vLEI Issuer]
2. The records must be stored for one year in a state suitable for auditing. They are accessible only to those bodies or private persons whose duty it is to supervise compliance with the data protection regulations, and may be used only for this purpose.

Art. 11 Processing policy

1. The controller of an automated data file subject to registration (Art. 11a para. 3 DPA) that is not exempted from the registration requirement in terms of Article 11a paragraph 5 letters b–d DPA shall issue a processing policy that describes in particular the internal organisation and the data processing and control procedures and contain documents on the planning, realisation and operation of the data file and the information technology used.
2. The controller of the data file shall update the processing policy regularly. He shall make it available to the Commissioner or the data protection officer under Article 11a paragraph 5 letter e DPA on request in a form that is comprehensible to them.

Art. 12 Disclosure of data

The controller of the data file shall notify the data recipient as to how up-to-date and reliable the personal data that he has disclosed is, unless this information is evident from the data itself or from the circumstances.

[note: the remainder of the Ordinance (Articles 13-38) is not relevant in the context of GLEIF-Qualified vLEI Issuer]