Recommended technical and functional requirements for an effective LER utility

A global utility layer for self-sovereign, verifiable, digital career and education credentials

Overview

Self-sovereign identity (SSI) represents a fundamentally new way to move and prove information in the digital world. In the process, individuals can benefit from enhanced agency and privacy and streamlined access to digital services, while organizations can benefit from more accurate data, better security, and vastly improved customer experiences.

An effective Learning and Employment Record (LER) infrastructure should empower individuals by providing them agency over their personal career records and reputation, allowing them to share it with relying party to prove their qualification, helping to unlock greater economic opportunity for everyone, everywhere.

On the employer side, the use such LER infrastructure across the job market accelerates recruitment, onboarding, and mobility, improves compliance, and unlocks innovative employment models.

Required Basic Flow

Organizations that have primary source authority to assert claims about the individual (e.g., institution, government, state board of nursing) should be able to use the LER infrastructure to issue the individual a digitally signed, tamper-proof and cryptographically secured credential.

The individual should be able to store the credential in their digital wallet and, when required, to share it via any digital conduit with any relying party (e.g., employer) to prove their qualifications.

Using advanced cryptography, the relying party should be able to instantly verify the credential can be trusted, without the need to connect with the original issuer.

Every credential should be signed by the issuing organizations, and when verified, to serve as immutable evidence for the source of the claims the appear on it.

Rigorous Verification Methods

The fundamental requirement of the LER infrastructure lies in enabling instantaneous verification of credentials when shared with a relying party. It is imperative that the relying party possesses a reliable mechanism to confirm several critical aspects. These include verifying that the credential was issued by a trusted source, and that this source has the authority to assert the claims included in the credentials. It also includes ensuring its integrity remains intact from the moment it leaves the issuer's systems, as well as validating that the credential has not been revoked by the issuer for any reason. Moreover, the relying party must be certain that the credential accurately attests to the identity of the individual presenting it. These essential functionalities ensure the utmost trust and credibility in the verification process, establishing a robust and seamless system for all stakeholders involved.

The Need for Global Interoperability and Compliance

Today’s trends of portfolio careers, lifelong learning, global workforce mobility and remote hiring will require the individual to curate credentials and certifications from multiple sources (education, training, licensing, employment, skills etc.) across multiple geographies, to prove their qualifications. Furthermore, for these credentials to have utility value, any relying party the individual shares their credentials with must be able to process, verify and make sense of them, regardless of industry or geography.

This is Interoperability, and the fragmented and global nature of the education ecosystem and the job market make it a monumental challenge.

The LER infrastructure should offer global reach and full interoperability across the global labor and education markets. This includes technical interoperability of course but also, unified user experience, global syntax, global semantic layer and global compliance.

A Utility Layer that No Single Entity Controls, Yet Anyone Can Use

A proprietary platform for facilitating the exchange of reliable career-related data inevitably carries the risk of vendor lock-in, affecting both the workforce and employers. The possibility of losing credentials arises if the vendor were to cease operations or impose restrictive policies on platform usage.

To mitigate these concerns, it is recommended that the LER infrastructure is built on open-source technology and remain independent of any single entity's control. It should be accessible to all, free from centralized governance, and instead governed by the community that benefits from its use. This approach ensures transparency and inclusivity, fostering a collaborative and sustainable environment for all stakeholders.

Trust Across Participating Parties

The modern internet has made it increasingly challenging to establish trust with others online, leading to issues such as spam, fraud, abuse, and misinformation.

In order to establish the critical trust needed to support the utility of LERs, all data transactions supported by the infrastructure must include authentication methods that produces rigorous proof required to confirm the identity of the parties involved in the communication and to validate the information being transferred. Individuals must be able to trust that the Issuer they claim their credentials from or the relying party they share their private information with are genuinely the entity they claim to be.

Recommended technical and functional requirements for an effective LER utility

1. Functional Requirements by Goal

1.1 Achieve Credential Utility Across All Sectors

In order for LERs to provide genuine utility to individuals, the LER infrastructure must be designed to ensure credential portability across all sectors and pertinent job markets. Labor market related interactions transcend borders and today's workforce frequently transitions between industries, geographies, and employment types (such as full-time, contingent, freelance, and platform work). Additionally, the increasing prevalence of remote hiring creates job opportunities that span different jurisdictions.

Individuals must be able to universally share their credentials with any relying party, without any restrictions or limitations.

Compliance with modern privacy regulations plays a critical role. Relying parties situated in jurisdictions governed by modern privacy regulations will consider engaging with an LER Infrastructure only if it is complying with regulations in their jurisdiction. 75% of the world's population will have its personal data covered under modern privacy regulations by year-end 2024[1]. In 2022, U.S. lawmakers in 29 states and the District of Columbia introduced data privacy bills[2].

Attribute	LER Requirement
Compliance with Modern Privacy Regulations	Must comply with the full set of requirements outlined in the section titled "Functional Requirements by Area - Compliance with Modern Privacy Regulations." While these requirements are not tailored to any particular jurisdiction, they address the core principles and requirements of modern privacy regulations.
Universal Utility	Individuals must be able to universally share their credentials with any relying party, without any restrictions or limitations.

1.2 Provide Real Utility for Relying Parties

From an employer's standpoint, verifying the career and education credentials of individuals before hiring them not only constitutes effective talent management but also holds significant implications for regulatory compliance, particularly in relation to the negligent hiring doctrine.

The recognition of the negligent hiring doctrine has been widely accepted across global legal systems. In the United States, this doctrine has gained widespread acceptance and has been applied in numerous cases.

Under the negligent hiring doctrine, employers are required to conduct comprehensive verifications of an individual's qualifications using primary source methods. This involves connecting directly with the authoritative entities that can confirm the claims related to the individual's credentials.

To provide substantial utility to employers on a larger scale, LERs must enable verification processes that are on par with the accuracy and reliability of primary source methods.

Attribute	LER Requirement
Individual authentication	Must include authentication methods that enable the issuer to obtain and document rigorous proof required to confirm that the individual is genuinely who they claim to be before issuing them credentials.
Source Verification	Must include authentication methods that enable the relying party to obtain and document rigorous proof required to confirm that the issuer of a credential is genuinely the entity they claim to be.
Source Authority Verification	Must include methods that enable the relying party to obtain and document rigorous proof required to confirm that the issuer has the authority to assert the claims included in the credential.
Data Integrity	Must include methods that enable the relying party to obtain and document rigorous proof required to confirm that the information included in the credential genuinely represents the claims made by the issuer.
Revocation Status Verification	Must include methods that enable the relying party to obtain and document rigorous proof required to confirm that the credential was not revoked by the issuer.
Person Binding	Must include methods that enable the relying party to obtain and document rigorous proof required to confirm that the credential was issued by the issuer to the individual presenting it.
Expiration	The LER infrastructure must clearly mark expired credentials as such.

[1] Top Five Trends in Privacy Through 2024, Gartner
[2] The International Association of Privacy Professionals (IAPP)

1.3 Protect Workforce Privacy

Consumers around the world are increasingly taking action to protect their data, by exercising their data rights under existing privacy laws or by no longer buying from organizations that don’t properly protect their data. Interestingly, the data shows that younger generations are more likely to be “privacy actives" than older ones.

79% of Americans now report being concerned, confused, and feeling lack of control about the way their personal information is being used by companies[1].

In this context, privacy encompasses the assurance that the decision to seek a new job remains confidential, shielded from the prying eyes of current employers or other entities that could potentially react unfavourably upon learning of such intentions.

For an LER ecosystem to be adopted at scale by individuals, the adherence to modern privacy regulations assumes a pivotal role. Ensuring compliance with these regulations not only safeguards individuals' sensitive information but also fosters an atmosphere of trust in the job market ecosystem.

However, equally significant is the sense of privacy that individuals experience while utilizing their newly acquired credentials. This sense of privacy is intrinsically tied to the assurance that their career pursuits, accomplishments, and aspirations remain confidential, granting them the freedom to explore opportunities without apprehensions.

Attribute	LER Requirement
Compliance with Modern Privacy Regulations	Must comply with the full set of requirements outlined in the section titled "Functional Requirements by Area - Compliance with Modern Privacy Regulations." While these requirements are not tailored to any particular jurisdiction, they address the core principles and requirements of modern privacy regulations.
Privacy	Individuals must retain control over who can access their credentials. Only when they choose to share specific credentials with a third party, such as a prospective employer or a school they apply to, will those selected credentials be disclosed to the third party.
Discretion	The LER infrastructure must ensure that privacy settings apply by default, without requiring manual input from the individual, so that Issuers will not have visibility into whether the individual shared their credentials or if they were verified by a relying party.

1.4 Safeguard Against Identity Theft and Phishing

In today's interconnected digital landscape, safeguarding against identity theft and phishing has become a paramount concern. The increasing reliance on online platforms for various aspects of life, including job searches and professional interactions, necessitates a proactive approach to protecting individuals' sensitive information. Identity theft and phishing threats can compromise personal data, career credentials, and professional reputations.

The LER infrastructure must include a robust cybersecurity measures, so that individuals can confidently engage in job-related activities while mitigating the risks associated with identity theft and phishing. Ultimately, safeguarding against these threats not only preserves personal integrity but also bolsters the overall health and resilience of the ecosystem.

Attribute	LER Requirement
Individual Authentication	Must include authentication methods that enable the issuer to obtain rigorous proof required to confirm that the individual is genuinely the who they claim to be before issuing credentials to this individual.
Issuer Authentication	Must include authentication methods that enable the individuals to obtain rigorous proof required to confirm that the issuer are genuinely the entity they claim to be before accepting credentials from this issuer.
Relying Party Authentication	Must include authentication methods that enable the individuals to obtain rigorous proof required to confirm that the relying party are genuinely the entity they claim to be before disclosing credentials to this relying party.

[1] Americans and Privacy: Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information, Pew Research Center

1.5 User-Centric Design

Adoption of user-centric design principles is paramount to achieving adoption of the LER infrastructure by individuals. This approach centres on aligning the functionality and features with the unique needs and preferences of job seekers.

In line with this user-centric design approach, individuals should possess the capability to centralize their credentials from various issuing entities into a single wallet.

From this consolidated repository, individuals should have the flexibility to seamlessly share a comprehensive selection of aggregated and curated credentials with any relying party, without encountering any constraints or limitations. This streamlined process aligns with the overarching objective of simplifying job seekers' interactions within the application, enhancing their ability to present a holistic representation of their qualifications to potential employers.

Attribute	LER Requirement
One Wallet	Individuals should have the ability to consolidate their credentials from all issuing bodies into a single wallet.
Batch Disclosure	Must enable the individual to disclose an entire set of aggregated/curated credentials in a single event.
Self-reporting	The LER infrastructure must enable the individual to self-report credentials. Self-reported credentials must be clearly marked as such yet adhere to the same technical standards and schemas as verifiable credentials and be shared as part of a disclosure, together with other credentials, verifiable or self-reported.
Wallet Recovery	Individuals should have the ability to recover their credentials if their wallet's device was broken, lost, stolen, or had its data wiped.

1.6 Drive Adoption at Scale by Employers

On the employer side of the equation, it is imperative that the LER infrastructure aligns seamlessly with the prevalent practices employed by organizations to manage their recruitment processes. Unless the infrastructure accommodates the established norms and methodologies of employers, widespread adoption is unlikely.

The successful integration of the LER ecosystem hinges on its compatibility with the tools, workflows, and protocols commonly used by employers to identify, assess, and onboard candidates.

By catering to these familiar practices, the LER infrastructure can effectively bridge the gap between innovative solutions and the real-world needs of employers, fostering a cohesive and mutually beneficial relationship between job seekers and hiring entities within the dynamic job market landscape.

Attribute	LER Requirement
Integrations	Must offer open-source tools to enable out-of-the-box integration with any relying party system of records (e.g., Applicant Tracking Systems, Admission Systems).
Batch Verification	Must enable the verification an entire set of aggregated/curated credentials shared by an individual in one event.
Availability and Monitoring	The LER infrastructure must achieve high availability for LER providers, holders and relying parties. The current availability status of the LER infrastructure must be viewable by all participants
Schemas	LER Infrastructure must support schemas for the common types of records required by issuers of high stakes credentials, and at minimum the following types: national ID, passport, CLR, vocational certification, license, employment record, right to work / I-9, skill/aptitude test, course completion, badge and skill.
Instant Verification	The LER infrastructure must enable instant verification of the credentials by a relying party, including verification of source identity, revocation status, source authority, person binding and data integrity (see definitions for these types of verification on the section titled "Functional Requirements by Area - A Robust Trust Framework section."
Semantic Layer	Must offer a standardized framework that assigns consistent meanings to the various credentials, so that regardless of industry, region, and institution the essence of qualifications remains universally understood by employers and other stakeholder in the labor market. This standardized framework must be machine readable to support adoption at scale.

1.7 Drive Adoption by Issuers of High-Stakes Credentials

For Issuers of high-stakes credentials, such as universities and licensing bodies, the widespread adoption of the LER infrastructure hinges on its alignment with their well-established practices for managing the issuance of critical qualifications. For this adoption to take place on a significant scale, the LER infrastructure must seamlessly integrate with the workflows, verification mechanisms, and protocols commonly employed by these entities. These include robust authentication methods to verify individuals' identities before issuing credentials. The infrastructure should support key record types like national ID, passport, CLR, vocational certification, license, and more. Issuers should have the ability to update or revoke credentials, with users promptly notified in either case.

Attribute	LER Requirement
Individual authentication	Must include authentication methods that enable the issuer to obtain rigorous proof required to confirm that the individual is genuinely the who they claim to be before issuing credentials to this individual.
Schemas	LER Infrastructure must support schemas for the common types of records required by issuers of high stakes credentials, and at minimum the following types: national ID, passport, CLR, vocational certification, license, employment record, right to work / I-9, skill/aptitude test, course completion, badge and skill.
Credential Updates	The LER infrastructure must enable the Issuer to force update the data on the credential held by the user. The user must be notified of such update.
Revocation	The LER infrastructure must enable the Issuer to revoke a credential held by the user. The user must be notified of such revocation.

1.8 Mitigate Workforce Vendor Lock-In Risks

In the context of LER's vendor lock-In risks assume a pivotal role, especially when considering the storage of career credentials within a single vendor's infrastructure. This scenario raises a crucial concern: the potential vulnerability stemming from the vendor's eventual discontinuation of the application or imposition of future usage restrictions. This could result in the abrupt loss of access to vital credentials, imperilling career advancement. The risk extends beyond technology dependence—it's also about safeguarding against the uncertainties, such as issuer shutdown, platform provider closure, cessation of operations, or even acquisition, that could undermine individuals' control over their credentials . To address these Vendor Lock-In Risks effectively, ensuring the individual's has perpetual access and control over their hard-earned credentials is imperative.

Attribute	LER Requirement
Survivability	Individuals should not rely on any single entity to share or verify their credentials. The utility of credentials must persist even if any individual entity, such as the issuer, wallet vendor, software vendor, storage vendor or platform provider, ceases to operate: • Credential data must continue to be accessible to the individual. • The individual must be able to continue and share their credentials universally. • Credentials must continue to be verifiable, including verification of source identity, revocation status, source authority, person binding and data integrity (see definitions for types of verification on the Trust section).
Portability	Individuals should not be confined to a specific wallet and should have the freedom to effortlessly transfer their credentials to other wallets that adhere to the same protocols without losing utility.
Back Up	Individuals should have the capability to back up and recover their credentials independently, without reliance on their wallet vendor.

Recommended technical and functional requirements for an effective LER utility

2. Requirements by Functional Area

2.1 Personal Sovereignty

Attribute	LER Requirement	Goal
Survivability	Individuals should not rely on any single entity to share or verify their credentials. The utility of credentials must persist even if any individual entity, such as the issuer, wallet vendor, software vendor, storage vendor or platform provider, ceases to operate: • Credential data must continue to be accessible to the individual. • The individual must be able to continue and share their credentials universally. • Credentials must continue to be verifiable, including verification of source identity, revocation status, source authority, person binding and data integrity (see definitions for types of verification on the Trust section).	Mitigate workforce vendor lock-in risks
One Wallet	Individuals should have the ability to consolidate their credentials from all issuing bodies into a single wallet.	User-centric design
Universal Utility	Individuals must be able to universally share their credentials with any relying party, without any restrictions or limitations.	Achieve credential utility across all sectors and pertinent job markets
Portability	Individuals should not be confined to a specific wallet and should have the freedom to effortlessly transfer their credentials to other wallets that adhere to the same protocols without losing utility.	Mitigate workforce vendor lock-in risks
Privacy	Individuals must retain control over who can access their credentials. Only when they choose to share specific credentials with a third party, such as a prospective employer or a school they apply to, will those selected credentials be disclosed to the third party.	Protect workforce privacy
Back Up	Individuals should have the capability to back up and recover their credentials independently, without reliance on their wallet vendor.	Mitigate workforce vendor lock-in risks
Discretion	The LER infrastructure must ensure that privacy settings apply by default, without requiring manual input from the individual, so that Issuers will not have visibility into whether the individual shared their credentials or if they were verified by a relying party.	Protect workforce privacy
Wallet Recovery	Individuals should have the ability to recover their credentials if their wallet's device was broken, lost, stolen, or had its data wiped.	User-centric design

2.2 Seamless Compatibility with Labor Market Practices

Attribute	LER Requirement	Goals
Integrations	Must offer open-source tools to enable out-of-the-box integration with any relying party system of records (e.g., Applicant Tracking Systems, Admission Systems).	Drive adoption at scale by employers
Batch Disclosure	Must enable the individual to disclose an entire set of aggregated/curated credentials in one event.	User-centric design
Batch Verification	Must enable the verification an entire set of aggregated/curated credentials shared by an individual in one event.	Drive adoption at scale by employers
Availability and Monitoring	The LER infrastructure must achieve high availability for LER providers, holders and relying parties. The current availability status of the LER infrastructure must be viewable by all participants	Drive adoption at scale by employers
Schemas	LER Infrastructure must support schemas for the common types of records required by issuers of high stakes credentials, and at minimum the following types: national ID, passport, CLR, vocational certification, license, employment record, right to work / I-9, skill/aptitude test, course completion, badge and skill.	Drive adoption by issuers of high-stakes credentials
Credential Updates	The LER infrastructure must enable the Issuer to force update the data on the credential held by the user. The user must be notified of such update.	Drive adoption by issuers of high-stakes credentials
Revocation	The LER infrastructure must enable the Issuer to revoke a credential held by the user. The user must be notified of such revocation.	Drive adoption by issuers of high-stakes credentials
Instant Verification	The LER infrastructure must enable instant verification of the credentials by a relying party, including verification of source identity, revocation status, source authority, person binding and data integrity (see definitions for these types of verification on the section titled "Functional Requirements by Area - A Robust Trust Framework section."	Drive adoption at scale by employers
Expiration	The LER infrastructure must clearly mark expired credentials as such.	Provide real utility for relying parties
Self-reporting	The LER infrastructure must enable the individual to self-report credentials. Self-reported credentials must be clearly marked as such yet adhere to the same technical standards and schemas as verifiable credentials and be shared as part of a disclosure, together with other credentials, verifiable or self-reported.	User-centric design
Semantic Layer	Must offer a standardized framework that assigns consistent meanings to the various credentials, so that regardless of industry, region, and institution the essence of qualifications remains universally understood by employers and other stakeholder in the labor market. This standardized framework must be machine readable to support adoption at scale.	Drive adoption at scale by employers

2.3 A Robust Trust Framework

Attribute	LER Requirement	Goal
Issuer Authentication	Must include authentication methods that enable the individuals to obtain rigorous proof required to confirm that the issuer are genuinely the entity they claim to be before accepting credentials from this issuer.	Safeguard against identity theft and phishing
Individual Authentication	Must include authentication methods that enable the issuer to obtain and document rigorous proof required to confirm that the individual is genuinely who they claim to be before issuing them credentials.	Drive adoption by issuers of high-stakes credentials
Relying Party authentication	Must include authentication methods that enable the individuals to obtain rigorous proof required to confirm that the relying party are genuinely the entity they claim to be before disclosing credentials to this relying party.	Safeguard against identity theft and phishing
Source Verification	Must include authentication methods that enable the relying party to obtain and document and document rigorous proof required to confirm that the issuer of a credential is genuinely the entity they claim to be.	Provide real utility for relying parties
Source Authority Verification	Must include methods that enable the relying party to obtain and document rigorous proof required to confirm that the issuer has the authority to assert the claims included in the credential.	Provide real utility for relying parties
Data Integrity	Must include methods that enable the relying party to obtain and document rigorous proof required to confirm that the information included in the credential genuinely represents the claims made by the issuer.	Provide real utility for relying parties
Revocation Status Verification	Must include methods that enable the relying party to obtain and document rigorous proof required to confirm that the credential was not revoked by the issuer.	Provide real utility for relying parties
Person Binding	Must include methods that enable the relying party to obtain and document rigorous proof required to confirm that the credential was issued by the issuer to the individual presenting it.	Provide real utility for relying parties

2.4 Compliance with Modern Privacy Regulations

This section in its entirety is critical to achieve two goals:

- Achieve credential utility across all sectors and pertinent job markets
- Protect workforce privacy

Attribute	LER Requirement
Lawfulness and Fairness	It is the responsibility of the governing body of the LER infrastructure to assure that all entities that participates in the credential exchange and storage, are liable to comply with the policies set by the LER infrastructure governing body, and all applicable laws and regulations, including, but not limited to, Data Protection Laws.
Transparency	All participants must be completely transparent to the individual in relation to processing their Personal Data. Their privacy statements, user agreements, transaction terms and conditions; all must require the individuals' consent.
Purpose Limitation	Disclosure Requests must specify the purpose for which the personal data is required and the duration that credentials will be retained as well as all related terms and conditions pertaining to the disclosure. Disclosure history must be logged on the individual's Wallet. The individual must be able to selectively mark credentials and/or Claims to share and approves terms and conditions.
Automated Decision-Making	The individual must be made aware of the existence of automated decision-making, including profiling. in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual, must be presented to the individual prior to disclosure, so they will be able to make an informed decision.
Data Minimization	It is the responsibility of the governing body of the LER infrastructure to assure that Relying Partys' are liable to limit requests to disclose credentials only to what is relevant strictly necessary in relation to the purpose for which it is being processed.
Limited Disclosure	The LER infrastructure must demonstrate a clear path to achieve zero knowledge proofs (ZKP) in 2-3 years.
Accuracy	The individual must be able to review credential data and selectively accept them. The individual must also consent to the Issuer's Terms and Conditions clearly presenting the Issuer's privacy statements, user agreement and all related terms and conditions pertaining to the issuing. The Issuer must be able to present evidence for such consent.
Rectification	The individual must be clearly notified of the way to contact the Issuer for data rectification if the credential contains errors in data. It is the responsibility of the governing body of the LER infrastructure to assure that the Issuers are liable to the rectification of inaccurate personal data within a reasonable time and implement Data Rectification processes as required under the GDPR and other modern privacy regulations.
Storage Limitation	The individual must consent to the relying party's Terms and Conditions clearly presenting the purpose for which the credentials are required and the duration that they will be retained, privacy statements, user agreement and all related terms and conditions pertaining to the disclosure. The relying party must be able to present evidence for such consent.
Storage Limitation	Personal data must be kept in a form which permits identification of Individuals for no longer than the duration necessary for the purposes for which the personal data is being processed.
Integrity and Confidentiality	It is the responsibility of the governing body of the LER infrastructure to assure that all entities that participates in the credential exchange and storage, are liable to provide appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.
Selective Disclosure by Default	individuals must have the ability to share only the specific credentials they choose, ensuring selective sharing of Credentials and/or Claims.
Consent Tracking	The individual's consents must be tracked and logged in a tamper-evident way.

Requirements by Functional Area

Attribute	LER Requirement
Privacy by Default	The LER infrastructure must ensure that the strictest privacy settings will apply by default, without any manual input from the individual.
Right of Portability	The LER infrastructure must allow the individual to move, copy or transfer credentials easily from one wallet to another in a safe and secure way, without affecting its usability.
Right of Access	The individual must have unrestricted access to their credentials.
Data Privacy Officer (DPO)	The governing body of the LER infrastructure must present an appointed DPO. The DPO is responsible for monitoring GDPR compliance, providing advice, and acting as a point of contact for individuals and supervisory authorities.
Record Keeping	All participants in the LER ecosystem must maintain detailed records of processing activities, including purposes, legal bases, categories of data, recipients, and retention periods.
Vendor Management	The governing body of the LER infrastructure must ensure that third-party vendors or processors also comply with modern privacy regulations when processing personal data on its behalf.
Data Breach Management	The governing body of the LER infrastructure must maintain a procedure for promptly identifying, reporting, and addressing data breaches and notifying relevant authorities and affected individuals within required timeframes.
Data Subject Rights	The governing body of the LER infrastructure must maintain mechanisms for handling individuals' requests to exercise their rights, such as access, rectification, erasure, and data portability.