

Data Protection

How Lixis approaches vehicle data, privacy and permitted use. Last updated: 7 October 2026

Lixis uses only the data required for a defined purpose, and the network operator keeps control of its infrastructure and its data. Financial institutions receive an answer to one specific question, never access to the underlying network data.

How a query works

1. **A declared purpose.** A financial institution submits a request tied to a specific, permitted purpose, such as verifying an insurance claim or supporting a credit decision.
2. **A narrow scope.** Each query covers a specified vehicle, a defined geographic scope and a defined time window. There is no open-ended searching or browsing.
3. **Processing where the data sits.** The query runs within the operator's environment or under the controls agreed for that deployment.
4. **Only a result leaves.** The requester receives a purpose-specific signal or verdict, such as "Consistent" or "Contradicted", with a short explanation.
5. **A record of every query.** Each request is logged with its requester, purpose and scope, so the operator can audit how its network is used.

What we do not do

- We do not own, install or operate cameras.
- We do not retain video or images.
- We do not build a central database of vehicle movements or offer general-purpose surveillance capabilities.
- We do not sell or license raw camera data.
- We do not answer requests that lack a permitted purpose or fall outside the agreed scope.

Network control

The camera-network operator retains control over its infrastructure and over the data for which it is responsible. A partnership with Lixis does not transfer ownership of the underlying network data. Specific access and processing rights are set out in a written agreement for each deployment.

Roles and responsibilities

Under the LGPD or other applicable data protection principle, depending on the country of application, a controller decides the purposes and essential elements of processing, and an operator (processor) processes personal data on a controller's behalf. In a typical deployment the network operator remains controller of its camera data. The exact roles of the operator, Lixis and the financial institution are determined for each deployment based on the actual processing arrangement, not assumed from commercial labels.

Legal and contractual restrictions

Vehicle-data deployments may be subject to privacy law, sector-specific rules, concession agreements, municipal requirements, existing contracts governing the network and restrictions set by the infrastructure operator. Lixis evaluates each deployment within those constraints rather than assuming one model fits every market.

In Brazil, this includes the LGPD (Lei nº 13.709/2018). In other markets, it includes the relevant local data-protection law, data-residency requirements and international-transfer rules. Data from a network is used for decisions in the market it serves, and the technical and commercial structure may differ by country.

Retention

Operational data is not retained indefinitely. Retention periods are set for each deployment according to the permitted purpose, contractual requirements and applicable regulation. Data that is no longer required is deleted or anonymized.

Security

Safeguards for each deployment include role-based access, authentication and authorization controls, encryption in transit and at rest where appropriate, logging and monitoring, restricted processing environments, retention limits, contractual confidentiality obligations and incident-response procedures. Specific controls depend on the architecture and risk profile of each deployment.

Rights of individuals

Individuals may exercise the rights provided by applicable data-protection law. Under the LGPD, these include confirmation of processing, access, correction, certain forms of deletion and objection, and review of decisions made solely on automated processing. Where a Lixis result contributes to a decision about a person, the financial institution making that decision remains responsible for it and for handling any review request.

Requests about processing for which Lixis is responsible can be sent to compliance@lixis.ai. Where another organization is the controller, we will refer the request to it or cooperate with it as appropriate.

Partnership review

Before any operational deployment, Lixis works with the network partner to agree, in order:
purpose → permitted data → processing model → output → retention → commercial access
→ termination controls. The aim is a product that fits both the commercial opportunity and
the network's legal and contractual obligations.

Contact

Data protection, privacy and compliance: compliance@lixis.ai