Cloud Services Privacy Policy

Last Updated: June 24, 2024

This LensLock Cloud Services Privacy Policy (“**Policy**”) applies only to the information that LensLock, Inc. (“**LensLock**”) collects, and you or your employer (collectively, “**Customer**”) provide to LensLock in connection with Customer’s use of LensLock Cloud Services (as defined below). LensLock’s marketing sites and other public websites are governed by the LensLock Privacy Policy.

Except as provided elsewhere in this Policy, it is governed by the terms of the Master Services Purchasing Agreement or similar agreement between LensLock and the Customer ("**Agreement**"). Any concept or principle outlined in this Policy is applicable to and becomes part of all relevant provisions of the Agreement, even without specific cross-references. All capitalized terms in this Policy not defined herein shall have the meanings ascribed to them in the Agreement.

By using LensLock Cloud Services, the Customer acknowledges having read and understood this Policy. LensLock may update this Policy periodically. When changes are made, LensLock will update the "last updated" date at the top of this page. The Customer's continued use of LensLock Cloud Services indicates acknowledgment, and to the extent permitted by law, agreement and acceptance of these changes.

Definitions

“**LensLock Cloud Services**” means LensLock's web services hosted on the LensLocker Portal including, without limitation, interactions between LensLock Cloud Services and LensLock Products (as defined below).

“**LensLock Products**” means:
(1) LensLock Cloud Services;

(2) devices sold by LensLock (including, without limitation, cameras, digital video recorders, sensors, and docking systems) (collectively, "**LensLock Devices**");
(3) other software offered by LensLock (including, without limitation, LensLock BITS, LensLock Evidence Offloader, LensLock MDT App, LensLock Mobile App, LensLock Device Manager, LensLock LiveView, LensLock Interrogation Room, and LensLock DSMS) (collectively, "**LensLock Client Applications**"); and
(4) ancillary hardware, equipment, software, services, cloud-based services, documentation, and software maintenance releases and updates. LensLock Products do not include any third-party applications, hardware, warranties, or the "**LensLocker Portal**" services.

"**Customer Data**" means:
(1) "**Customer Content**", which means data uploaded into, ingested by, or created in LensLock Cloud Services within Customer's tenant, including, without limitation, media or multimedia uploaded into LensLock Cloud Services by Customer ("**Evidence**"); and
(2) "**Non-Content Data**", which means:
(a) "**Customer Entity and User Data**", which means Personal Data and non-Personal Data regarding Customer's LensLock Cloud Services tenant configuration and users;
(b) "**Customer Entity and User Service Interaction Data**" which means data regarding Customer's interactions with LensLock Cloud Services and LensLock Client Applications;
(c) "**Service Operations and Security Data**", which means data within service logs, metrics and events and vulnerability data, including, without limitation: (i) application, host, and infrastructure logs; (ii) LensLock Device and LensLock Client Application logs; (iii) service metrics and events logs; and (iv) web transaction logs;
(d) "**Account Data**", which means information provided to LensLock during sign-up, purchase, or administration of LensLock Cloud Services, including, without limitation, the name, address, phone number, and email address Customer provides, as well as aggregated usage information related to Customer's account and administrative data associated with the account; and
(e) "**Support Data**", which means the information LensLock collects when Customer contacts or engages LensLock for support, including, without limitation, information about hardware, software, and other details gathered related to the support incident, such as contact or authentication information, chat session personalization, information about the condition of the machine and the application when the fault occurred and during

diagnostics, system and registry data about software installations and hardware configurations, and error-tracking files.

For purposes of clarity, Customer Content does not include Non-Content Data, and Non-Content Data does not include Customer Content.

"**Data Controller**" means the natural or legal person, public authority, or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data (as defined below).

"**Data Processor**" means a natural or legal person, public authority or any other body which processes Personal Data on behalf of the Data Controller.

"**Personal Data**" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

"**Processing**" refers to any operation or series of operations carried out on Personal Data or sets of Personal Data, whether or not by automated means. This includes activities such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment, combination, restriction, erasure, or destruction.

LensLock's Role

LensLock acts as a Data Processor for Customer Content. The Customer, as the Data Controller, holds all rights, titles, and interests in the Customer Content, while LensLock does not obtain any rights to it. The Customer is solely responsible for uploading, sharing, withdrawing, managing, and deleting Customer Content. The Customer grants LensLock limited access to the Customer Content exclusively to provide and support LensLock Cloud Services for the Customer and the Customer's end-users. The Customer represents and warrants to LensLock that: (1) the Customer owns the Customer Content; (2) the Customer Content and the Customer's end-users' use of the Customer Content and LensLock Cloud Services comply with this Policy and applicable data protection laws and

regulations. LensLock is not responsible for the Customer's privacy practices as a Data Controller. For these practices, you should consult the Privacy Policy of the relevant customer.

LensLock may also collect, control, and process Non-Content Data as a Data Controller. This data is collected, controlled, and processed to provide LensLock Cloud Services and to support the overall delivery of LensLock Products, including for business, operational, and security purposes. LensLock may analyze and report anonymized and aggregated Non-Content Data to communicate with both external and internal stakeholders. For Customer Entity & User Data, LensLock acts as an independent Data Controller, with the Customer also acting as an independent Data Controller, not a joint Data Controller.

Data Collection Purposes and Processing Activities

Customer Content

LensLock will use Customer Content solely to provide LensLock Cloud Services to the Customer. It will not use Customer Content for advertising or any similar commercial purposes.

LensLock periodically upgrades or modifies its Cloud Services to offer new features and enhancements, following the LensLock Engineering Maintenance Schedule. Customers are notified of such upgrades or changes within a reasonable timeframe before their release. These changes may enhance the service's capabilities and expand the ways in which Customer Content can be processed.

Non-Content Data

Non-Content Data encompasses data, configuration, and usage information related to the customer's LensLock Cloud Services tenant, LensLock Devices, LensLock Client Applications, and users, which is transmitted or generated during the use of LensLock Products. Non-Content Data includes the following:

Customer Entity and User Data

Customer Entity and User Data includes both personal and non-personal information regarding the Customer's LensLock Cloud Services tenant configuration and users.

LensLock uses this data to: (1) provide LensLock Cloud Services, including user authentication and authorization functionality; (2) improve the quality of LensLock Products and offer enhanced features; (3) contact the Customer with information about their account, tenant, subscriptions, billing, and updates to LensLock Cloud Services, including details about new features, security, and technical issues; and (4) market our products or services to the Customer via email, by sending promotional communications, including targeted advertisements, or presenting relevant offers.

Customers cannot unsubscribe from non-promotional communications but may opt out of promotional communications at any time by clicking the unsubscribe button at the bottom of such communications.

Customer Entity and User Service Interaction Data

Customer Entity and User Service Interaction Data includes information about how Customers interact with LensLock Cloud Services and LensLock Client Applications. LensLock uses this data to enhance the quality of its products and provide improved functionality and features.

Service Operations and Security Data

LensLock uses Service Operations and Security Data to provide service operations and monitoring.

Account Data

LensLock utilizes Account Data to provide LensLock Cloud Services, management of Customer accounts, marketing to, and communication with the Customer.

Support Data

LensLock uses Support Data to resolve Customer support incidents and to operate, enhance, and personalize LensLock Products. If Customer shares Customer Content with LensLock in a support scenario, the Customer Content will be treated as Support Data but will only be used for resolving support incidents.

LensLock may provide support via phone, email, or online chat. With Customer's consent, LensLock may use Admin Access (“AA”) to temporarily navigate Customer's LensLock Cloud Service tenant to view data for resolving a support incident. Phone conversations, online chat sessions, or AA sessions with LensLock support professionals may be recorded and/or monitored for purposes such as training, future support, and evidentiary purposes.

Server and Data Location

Customer Content

LensLock offers LensLock Cloud Services in numerous geographic regions. Before creating an account in LensLock Cloud Services, Customer determines where LensLock will store Customer Content by designating an economic area.

LensLock ensures that all Customer Content in LensLock Cloud Services remains within the selected economic area, including, without limitation, all backup data, replication sites, and disaster recovery sites. Customer selected economic areas can be determined through review of Customer's LensLock Cloud Services URL.

Non-Content Data

Customer Entity and User Data

Customer Entity and User Data is located in Customer's selected economic area for Customer Content.

Customer Entity and User Service Interaction Data

Customer Entity and User Service Interaction Data is located in Customer's selected economic area for Customer Content and the United States.

Service Operations and Security Data

Service Operations and Security Data is located in Customer's selected economic area for Customer Content and the United States.

Account Data and Support Data

Account and Support Data is located in the United States and may be located in Customer's selected economic area for Customer Content.

Information Sharing

LensLock may share data with its subsidiaries, service providers and other partners to help us operate, including for providers to facilitate: (1) user account management, authentication, analytics, and communication, (2) product features, e.g. geolocation services, product development, and error analytics, (3) customer service and support, and (4) security monitoring and investigation.

For more information about the sharing of Personal Data by LensLock, please contact legal@lenslock.com.

Required Disclosures

LensLock will not disclose Customer Content except as required by any law or regulation. If permitted, LensLock will notify Customer if any disclosure request is received for Customer Content so Customer may challenge or object.

Customer's Access and Choice

Customer Content

Customer can access Customer's tenant to manage Customer Content.

LensLock will collaborate with Customers to facilitate access to Personal Data held by LensLock. LensLock will also take reasonable measures to allow Customers to correct, amend, or delete Personal Data that is proven to be inaccurate.

Non-Content Data

If you wish to update the Personal Data you've shared with us, change your mind about sharing Personal Data, cancel your Customer account, or request that LensLock no longer use your Personal Data to provide you services after registering an account on LensLock Cloud Services, please contact us at legal@lenslock.com.

Certain data processing can be adjusted by the Customer based on LensLock Product usage, Customer network or device configuration, and administrative settings available with LensLock Cloud Services or LensLock Client Applications:

LensLock Eagle 13 WiFi Positioning

LensLock Eagle 13 cameras provide customers with a feature that enhances location services in environments where GPS/GNSS signals are not available, such as within buildings or underground. Customer administrators can manage the use of this service within the administrative features of LensLock Cloud Services.

Data Security Measures

LensLock is dedicated to safeguarding the security of Customer Data. We have established and implemented policies, programs, and procedures that are commercially reasonable and comply with applicable industry practices. These include administrative, technical, and physical safeguards to protect the confidentiality, integrity, and security of Customer Content and Non-Content Data against unauthorized access, use, modification, disclosure, or other misuse.

LensLock will take appropriate steps to ensure that its employees and contractors comply with the data security measures, as applicable to their respective scopes of performance.

Confidentiality

Customer Content and Non-Content Data are encrypted when transmitted over public networks. Customer Content is also encrypted at rest in all LensLock Cloud Service regions.

LensLock ensures the protection of all Customer Content and Non-Content Data through robust logical access control mechanisms, ensuring that only users with relevant business needs have access to the data. Access control mechanisms are periodically validated by third-party specialized security firms, and access control lists are regularly reviewed by LensLock.

Integrity

When Evidence is uploaded to LensLock Cloud Services, a Secure Hash Algorithm (SHA) checksum is generated on the upload device and again upon ingestion into LensLock Cloud Services. If the SHA checksums do not match, the upload process is reinitiated. Once the upload is successful, the SHA checksum is retained by LensLock Cloud Services and can be viewed by users with access to the Evidence audit trail for that specific piece of Evidence. Tamper-proof audit trails are automatically created by LensLock Cloud Services upon ingestion of any Evidence.

Availability

LensLock employs a comprehensive strategy to maintain the availability of LensLock Cloud Services. Customer Content is replicated across multiple systems to safeguard against accidental destruction or loss. The architecture of LensLock Cloud Services is designed to reduce single points of failure. LensLock has developed and routinely tests its business continuity planning and disaster recovery programs.

Isolation

LensLock ensures logical isolation of Customer Content, meaning that the content of one authenticated customer is not displayed to another customer, unless explicit sharing relationships are established. Centralized authentication systems are employed across LensLock Cloud Service regions to enhance uniform data security.

Additional role-based access control is applied within each Customer's LensLock Cloud Service tenant to manage user interactions with or access to Customer Content. Customers have sole control over these role-based access control mechanisms within their LensLock Cloud Services tenants.

Access to the supporting infrastructure of LensLock Cloud Services is governed by the principle of least privilege. All access must be approved by system owners and undergoes at least quarterly user access reviews. Shared computing or networking resources are thoroughly hardened and periodically validated to ensure the proper isolation of Customer Content.

Non-Content Data is also logically isolated within information systems, ensuring that only authorized LensLock personnel have access.

Personnel

LensLock employees are expected to comply with applicable laws and the company's guidelines on confidentiality, business ethics, acceptable usage, and professional standards. Upon hire, employees must complete security training, with additional annual and role-specific security training required.

To the extent permitted by law and in compliance with local labor regulations, LensLock conducts thorough background checks on its personnel. Employees supporting LensLock Cloud Services undergo additional role-specific security clearances or adjudication processes, which may include Criminal Justice Information Services background screening and national security clearances and vetting.

Data Breach

Notification

If LensLock discovers that Customer Data has been accessed, disclosed, altered, or destroyed by an unlawful or unauthorized party, LensLock will notify the relevant authorities (where required) and affected customers.

LensLock will notify Customer administrators registered on LensLock Cloud Services within 48 hours of confirming an incident. Authorities will be notified through LensLock's established channels and within specified timelines. The notification will include known facts, actions taken, and commitments regarding future updates. Additional information can be found in the LensLock Cloud Services Security Incident Handling and Response Statement.

Data Portability, Migration, and Transfer Back Assistance

Data Portability

Evidence uploaded to LensLock Cloud Services is stored in its original format. Customers can retrieve and download Evidence from LensLock Cloud Services to transfer data to an

alternative information system. Additionally, Evidence audit trails and system reports can be downloaded in various industry-standard, non-proprietary formats.

Data Migration

In the event a Customer's access to LensLock Cloud Services is terminated, LensLock will retain all Customer Content for at least 90 days following termination. During this period, Customer can retrieve their content if all outstanding amounts have been paid. However, LensLock Cloud Services will not be fully functional during this time, except for the ability to retrieve Customer Content. There will be no additional fees for downloading Customer Content during this 90-day period.

LensLock is not obligated to maintain or provide any Customer Content after the 90-day period. Unless legally prohibited, LensLock may delete Customer Content upon termination as part of its normal retention and data management procedures. Upon written request, LensLock will provide written confirmation that all Customer Content has been successfully deleted and removed from LensLock Cloud Services.

Post-Termination Assistance

LensLock will offer Customer the standard post-termination data retrieval assistance available to all customers. Any requests for additional assistance from Customer in downloading or transferring Content will incur additional fees. LensLock cannot guarantee or warrant data integrity or readability in external systems.

Data Retention, Restitution, and Deletion

LensLock follows internal disaster recovery and data retention policies in accordance with relevant laws and regulations. These policies cover LensLock's data, including LensLock Cloud Services and Customer Content. Data retention policies specifically address LensLock's Non-Content Data, ensuring its secure disposal when it is no longer needed for delivering and supporting LensLock products and services, in line with applicable regulations. Non-Content Data is retained as long as necessary to provide services, comply with legal obligations, resolve disputes, and enforce agreements. Customers are responsible for adhering to their own retention policies and procedures.

Evidence Retention

Customer determines Evidence retention periods according to their internal retention policies and procedures. Within LensLock Cloud Services, Customer can establish and manage these retention policies, thereby controlling the retention and deletion of their Evidence. LensLock Cloud Services can automate weekly notifications to all Customer administrators, summarizing upcoming agency-wide deletions. Additionally, individual Customer users can receive weekly messages regarding Evidence uploaded to their user accounts to prevent accidental deletions. Customers can recover Evidence up to seven days after it has been queued for deletion. After this seven-day grace period, LensLock Cloud Services will initiate the deletion of the Evidence. Data deletion processing may occur asynchronously across storage systems and data centers. During and after this process, the Evidence will not be recoverable by any party.

Accountability

As outlined, LensLock is dedicated to maintaining compliance with relevant security and privacy standards to ensure the ongoing security, availability, integrity, confidentiality, and privacy of LensLock Cloud Services and Customer Data stored within.

Insurance

LensLock will maintain, during the term of the Agreement, a cyber-insurance policy and will furnish certificates of insurance following Customer's written request.

How to Contact Us

LensLock commits to resolve complaints about Customer privacy and use of LensLock Products. Complaints surrounding this Policy can be directed to Customer's local LensLock representative or legal@lenslock.com. If Customer has any questions or concerns regarding privacy and security of Customer Content or LensLock's handling of Customer's Personal Data, please contact legal@lenslock.com.com.