
# Information security

## How LeasePlan Nederland ensures information security

What's next?

17.00136.01

LeasePlan Nederland N.V. is committed to the security of information and data privacy. We continuously invest in our engineering, information security and proven technologies as well as our processes and people in order to ensure that we can always provide excellent quality and reliable services. This document step by step summarizes how LeasePlan ensures Information Security.

## 1. Policy and governance

Securing data starts with a clear view and strategy. Our governance structure is organised in a way that information security is positioned at every layer throughout our organisation. We describe hereinafter which departments and functions are involved.

**a. Information security policy**

Our global Information Security & Governance departments are responsible for defining our information security policies. Local LeasePlan entities adopt these policies and align them with the local requirements and regulations. Policies are based on best practices, e.g. ITIL, ISO 27001 and CobIT.

**b. Security team (local and global)**

At LeasePlan, we have a security team comprising highly skilled and educated employees. Our security team performs day-to-day information security activities and is responsible for aligning our security measures with:

- laws and regulations
- (internal) policies
- our risk management approach.

**c. Data breach protection team**

To secure your personal data and comply with the regulations (General Data Protection Regulation or GDPR), we have a data breach protection team. This team comprises employees with extensive knowledge from different professions, e.g. a Privacy Officer, an Information Security Officer, Information Security Administrators and a riskmanager.

**d. Internal audit (local and global)**

Our internal audit department is responsible for performing audits on the effectiveness of the implemented security measures. Internal audit also reviews the effectiveness of procedures/processes and policies.

## 2. Asset management

As a result of our asset management process, we have an overview of the data we receive, process and store.

The assets in our information asset inventory are classified based on the confidentiality level. Each asset is assigned to an owner. The responsibility of this owner is to ensure that proper measures are implemented effectively and perfectly aligned with the various policies and procedures for information security.

## 3. Human resources and culture (our staff)

Information security is as strong as its weakest link. Therefore, we have a strong focus on technical measures as well as the culture and security awareness of our employees.

**a. Awareness**

To ensure the needed and desired level of security awareness of our employees, we facilitate mandatory training activities, periodically inform our employees about information security and perform awareness tests.

**b. Employee checks**

Screening of individuals takes place during our onboarding process. All relevant employees are also obligated to take an oath on a moral-ethic statement ('bankierseed').

## 4. Access controls

**a. Physical access**

Access to the LeasePlan offices is secured by secure card reader access and a camera system covering all the entries into the buildings.

**b. Data centres**

Computer rooms are closed and secured by card reader access and only made accessible by authorised staff.

**c. Logical access**

i. Password policy

LeasePlan adheres to a password policy for all applications, databases, and operating systems. This policy includes, among others, password complexity, password lockout policies and password expiration.

ii. Network

1. Access to the wired network is continually monitored to ensure only LeasePlan systems are accessing the network.
2. Wi-Fi access to the internal network is only allowed by LeasePlan systems.

iii. Applications

Role based access control is implemented for most important applications. The access matrix is reviewed periodically.

iv. Monitoring, logging and alerting

Access to applications and operating systems are logged and monitored. Critical events are defined in applications and alerts are reviewed and followed up on.

## 5. Operational security

### a. Vulnerability management

i. Security tools are deployed to ensure all systems are regularly scanned for vulnerabilities.

ii. A patch management schema is used to ensure patches are deployed in a timely fashion. If required, patches are deployed the same day.

### b. Malware prevention

All Windows systems have anti-virus software installed. The IT team monitors the anti-virus software to ensure all scanners have up-to-date virus definitions. E-mail is scanned for viruses and spam. A web-filter is implemented to protect LeasePlan systems from malicious websites.

### c. IDS/IPS

The network is protected by several layers of firewalls, Intrusion Detection and Prevention Systems are in place and alerts are followed up on.

### d. Incident management

Security incidents are recorded and reviewed by the security team.

### e. Monitoring, logging and alerting

Logging and monitoring software is used to monitor access to facilities and systems.

f. **Network segregation**
The network is divided into network zones. Access between zones is mediated by a firewall allowing only the access that is required through the different network zones.

g. **Mobile Device Management**
Mobile phones, tablets and laptops are protected with security software to ensure the information on the devices is safe when used, stolen or lost. All the information on mobile devices is encrypted.

h. **Removable storage devices**
Access to USB and other removable storage media is restricted to read-only access. The few people who have write access to removable storage use encrypted USB sticks or have strict instructions on how to protect information on removable media.

## 6. Portals and websites

a. **OWASP**
All LeasePlan websites are built according to the OWASP guidelines.

b. **Penetration tests**
On each website of LeasePlan, a penetration test is performed by an independent company. All high findings are immediately solved and all medium and low findings are fixed in the normal release process. If there are a significant number of changes made to any website, a retest will be performed.

## 7. Data transfer/communication

a. **E-mail**
All email sent outside LeasePlan will be opportunistically encrypted with TLS. Enforced encryption is also possible on the request of the other party.

b. **ShareFile**
For the exchange of (large) files, LeasePlan provides a tool called ShareFile. This tool securely exchanges (large) files between the customer and LeasePlan. The exchange of these files is done over HTTPS and protected by a username and password. Files are stored on LeasePlan premises.

c. **Interfaces**
All exchange of data between LeasePlan and other parties will always be adequately secured, for example the exchange channel will be encrypted, the files exchanged will be encrypted, or both.

d. **Encryption (HTTPS/TLS, SMTPS)**
All websites that provide a login or provide ways of entering data will be protected by HTTPS/TLS.

## 8. Acquisition, development and management of software

Software as a Service (SaaS) is used by LeasePlan to optimise our online services for our customers. In addition to cloud applications, local hosted applications are also utilised. To safeguard the acquisition of software, we have implemented organisational and procedural measures. Information security risk assessment is performed by our security specialists for each application that is utilised.

In the case of in-house software development and management, we ensure information security in the development and software change management process. Before a change or developed piece of software is promoted to our live environment, our change manager approves the change after he has determined that all relevant measures are implemented and secured.

We are equipped with the latest information security updates and patches and we have implemented a patch management process.

## 9. Availability and continuity

**a. Load balancers**

All websites are behind a load balancer to assure a high level of availability. Most critical components are also redundant in order to ensure this availability or to provide the needed performance.

**b. Disaster recovery**

Every calendar year, a full disaster recovery test of all the critical servers is performed at an external location. All critical processes are tested by users and signed off by them.

**c. Back-up (external storage)**

Every system is backed up daily and the backup media is securely transported to an offsite location. There is also a copy available in our main office to provide for the fast recovery of deleted files.

## 10. Third-party suppliers

**a.** The confidentiality of personal data is in our internal policies. Our employees are bound by confidentiality and they are required to comply with the LeasePlan Code of Conduct. LeasePlan also enters into Data Processor Agreements with suppliers that process personal data for which LeasePlan is considered controller. Suppliers also agree to the LeasePlan Code of Conduct.

## 11. Regulation

**a.** To provide our services, we need to collect and maintain vast amounts of data regarding the cars and use of the cars. We base this on data privacy regulations and our collection methods which are reviewed by our data privacy officer. Our Privacy Policy is posted at www.leaseplan.nl or https://www.leaseplan.nl/privacy-beleid

**b.** In order to advance the integrity of the financial sector, there are international rules with which LeasePlan must comply. The rules are incorporated in the legislation and De Nederlandsche Bank (DNB - the Dutch central bank) exercises supervision over LeasePlan.

**Do you want to know more?**
If you have any further questions about data or information security, please feel free to contact LeasePlan.

LeasePlan

Contact information:

**Jasper Kroeger**
Information Security Officer
Tel: +31 36 527 1255
E-mail: jasper.kroeger@leaseplan.com

**Yvette Tienhooven**
Privacy Officer
Tel: +31 36 527 1320
E-mail: yvette.tienhooven@leaseplan.com

leaseplan.nl