

LeasePlan Employee Privacy Statement

LeasePlan Corporation N.V. and its affiliated entities (together “**LeasePlan**”) value the trust of their employees and are committed to protecting the personal data of employees. LeasePlan operates in many different countries. Some of these countries have laws related to the collection, use, transfer and disclosure of the personal data of individuals, including our employees. We take these obligations very seriously, and we are committed to protecting the privacy of our current and former employees. The purpose of this Employee Privacy Statement (the “**Statement**”) is to give you information about what personal data we collect, use, transfer and disclose, and why.

1. What Information About You We Collect, Use, Transfer And Disclose, And Why

In the course of your employment with a LeasePlan company (the “**Company**”), the Company collects information about you and your working relationship with the Company, or your family, domestic/civil partner or dependents (“**Dependents**”). We refer to such information as “**Personal Data**”. For more specific information regarding what Personal Data about you the Company collects, uses, transfers and discloses, and the purposes for which they are collected, used, transferred and disclosed, please see the end of this Statement. Local employee handbooks, and notices provided in your local office provide additional details or information.

We collect and process information about you for a variety of reasons. For more detail regarding the reasons and purposes for which we process Personal Data please see the end of this Statement. Where none of these reasons apply, your decision to provide Personal Data to the Company is voluntary. If we collect or process Personal Data based on your consent, you may withdraw your consent at any time.

We receive Personal Data from you as well as from other sources as described at the end of this Statement.

2. Transfer And Joint Use Of Personal Data

Due to the global nature of LeasePlan’s operations, the Company shares overall HR data throughout all entities but personal data is not included, unless this is needed for the corporate headquarters in NL to fulfill the purposes as described at the end of this statement.

Access to Personal Data within LeasePlan will be limited to those who have a need to know the information for the purposes described at the end of this Statement, and will include your managers and their designees, personnel in HR, IT, Compliance, Legal, Finance and Accounting and Internal Audit.

All personnel within LeasePlan will generally have access to your business contact information such as name, position, telephone number, work location address and email address.

From time to time, LeasePlan will need to make Personal Data available to other unaffiliated third parties. Please see the end of this Statement for a list of the categories of unaffiliated third parties. Some of the unaffiliated third parties will be located outside of your home jurisdiction, including in any country in which we or they have operations.

3. Security

The Company will take appropriate measures to protect Personal Data that are consistent with applicable privacy and data security laws and regulations, including requiring service providers to use appropriate measures to protect the confidentiality and security of Personal Data.

4. Data Integrity and Retention

The Company will take reasonable steps to ensure that the Personal Data processed are reliable for their intended use, and are accurate and complete for carrying out the purposes described in this Statement. The Company will retain Personal Data for the period necessary to fulfill the purposes outlined in this Statement unless a longer retention period is required or permitted by law. For information on the criteria used please see the end of this Statement.

5. Access and Correction Requests, Questions And Complaints

Please contact your local Human Resources Representative if you have any questions or concerns about how the Company processes Personal Data; if you would like to request to access, correct, suppress or delete Personal Data about you or request that we cease using it as permitted by applicable law; or if you would like to request a copy or portability of your Personal Data. We will respond to your request consistent with applicable law. Please note, however, that certain Personal Data may be exempt from requests pursuant to applicable data protection laws or other laws and regulations.

6. Employee's Obligations

Please keep Personal Data up to date and inform us of any significant changes to Personal Data. You agree to inform your Dependents whose Personal Data you provide to the Company about the content of this Statement, and ensure you have the right to provide that information to the Company. You further agree to follow applicable law and both the Company's and LeasePlan's policies, standards and procedures that are brought to your attention when handling any Personal Data to which you have access in the course of your relationship with the Company. In particular, you will not access or use any Personal Data for any purpose other than in connection with and to the extent necessary for your work with the Company. You understand that these obligations continue to exist after termination of your relationship with the Company.

7. Local Data Protection Officer Contact Information and Complaints

The local Privacy Officer is Samantha Carlin, to be reached via email on LPGB-Privacy or privacy@leaseplan.com.

You can contact LeasePlan's Data Protection Officer by email at Corp-Group-Privacy-Officer or Group.Privacy.Officer@leaseplancorp.com.

You also may lodge a complaint with a Data Protection Authority for your country or region or in the place of the alleged misconduct via this hyperlink to the list of Data Protection Authorities: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080.

8. Monitoring of communications

Subject to applicable laws, we will monitor and record calls, email, text messages on company smartphones, social media messages, personal use of Leaseplan's systems and devices by employee and other staff, and other communications. We will do this for compliance with regulatory rules, self-regulatory practices or procedures relevant to our business, to prevent or detect crime, in the interests of protecting the security of our communications systems and procedures, and for quality control and staff training purposes.

This means that our lawful reasons under data protection laws for the processing involved in this use of your personal information is compliance with legal obligations and processing necessary for our legitimate interests.

In particular, telephone calls may be recorded for these purposes where they are between us and customers/individuals applying to be customers in connection with the application and/or the customer account. If you work in a customer facing role, distinct from a back office role, this will be relevant to you.

9. For how long is your personal information retained by us

We need to keep your personal information for as long as necessary to fulfil the purposes for which it was collected (and those purposes are as described above). This includes retaining it during the period of your employment or other services arrangement with us and then, after this ends, for as long as necessary in order to comply with our legal and regulatory requirements and in case of claims. This means we may keep some categories of personal information about you for longer than others.

The criteria we currently use to determine data retention periods for your personal information is set out below. You should note that the retention periods we mention may change from time to time. Always look at our Information Management Policy for the most up to date information. It is incorporated by reference into this privacy notice.

- Retention in case of queries. If you are an employee or other member of staff we will retain it in case of queries from you (for instance, if you apply unsuccessfully for a promotion). We will keep this personal information as part of your HR record for the length of your employment or other services arrangement with us. We may also have to keep it for a longer period (see directly below).
- Retention in case of claims. We will retain certain of your personal information for the period in which you might legally bring claims against us. This means your personal information will

usually be held by us for a period of just over 6 years after the end of the employment or other relationship with us. We may have to keep it for a longer period (see directly below).

- Retention in accordance with legal and regulatory requirements. We will retain your personal information for longer than 6 years where we are required to do so by laws or regulations (e.g. some health and safety laws).
- Other retention periods relevant to employee/staff records: Certain employee/staff related records have a different time frame to those set out above.
- Retention of CCTV images. We retain CCTV images for three months and after that they will be erased because we will not need to retain them for the purposes listed (above).
- In addition, any personal information contained in any work related correspondence (such as emails) or other records may be retained for longer periods dependent on the retention period of the file that your personal data is held.

If you have any questions or queries about Leaseplan's policy about periods for retention specifically in relation to your personal information you can contact our DPO (details as above).

Types Of Personal Data We Collect, Use, Transfer And Disclose:

- **Personal Details:** Name, employee identification number, work and home contact details (email, phone numbers, physical address) language(s) spoken, gender, date of birth, national identification number, social security number, marital/civil partnership status, domestic partners, dependents, disability status, emergency contact information and photograph.
- **Official Documentation and Documentation Required under Immigration Laws:** Registration of availability of Certificate of conduct , citizenship, passport data, details of residency or work permit.
- **Compensation and Payroll:** Base salary, bonus, benefits, compensation type, salary step within assigned grade, details on stock options, stock grants and other awards, currency, pay frequency, effective date of current compensation, salary reviews, banking details, working time records (including vacation and other absence records, leave status, hours worked and department standard hours), pay data and termination date.
- **Position:** Description of current position, job title, corporate status, management category, job code, salary plan, pay grade or level, job function(s) and sub function(s), company name and code (legal employer entity), branch/unit/department, location, employment status and type, full-time/part-time, terms of employment, employment contract, work history, hire/re-hire and termination date(s) and reason, length of service, retirement eligibility, promotions and disciplinary records, date of transfers, and reporting manager(s) information.
- **Talent Management Information:** Details contained in letters of application and resume/CV (previous employment background, education history and current trainings, professional qualifications, language and other relevant skills, certification, certification expiration dates), information necessary to complete a background check, details on performance management ratings, development programs planned and attended, e-learning programs, performance and development reviews, willingness to relocate, driver's license information, and information used to populate employee biographies.
- **Management Records:** Details of any shares of common stock or directorships.
- **System and Application Access Data:** Information required to access company systems and applications such as System ID, LAN ID, email account, instant messaging account, mainframe ID, previous employee ID, previous manager employee ID, system passwords, employee status reason, branch state, country code, previous company details, previous branch details, and previous department details, and electronic content produced using Company systems.

The Purposes For Which We Collect, Use, Transfer And Disclose Personal Data

We collect, use, transfer and disclose Personal Data for the purposes listed below based on one or more of the following reasons: (i) because we are required to do so by local applicable law; (ii) because such information is necessary to fulfill the employment contract; (iii) because such information is of particular importance to us and we have a specific legitimate interest under law to process it; or (iv) where necessary to protect the vital interests of any person.

Regarding (iii) above, we have a legitimate interest in collecting and processing Personal Data, for example: (1) to ensure that our networks and information are secure; (2) to administer and generally conduct business within Company and across the organization; and (3) to prevent fraud.

- **Managing Workforce:** Managing work activities and personnel generally, including recruitment, appraisals, performance management, promotions and succession planning, rehiring, administering salary, and payment administration and reviews, wages and other awards such as stock options, stock grants and bonuses, healthcare, pensions and savings plans, training, leave, managing sickness leave, promotions, transfers, secondments, honoring other contractual benefits, providing employment references, loans, performing workforce analysis and planning, performing employee surveys, performing background checks, managing disciplinary matters, grievances and terminations, reviewing employment decisions, making business travel arrangements, managing business expenses and reimbursements, planning and monitoring of training requirements and career development activities and skills, workforce reporting and data analytics/ trend analysis, and creating and maintaining one or more internal employee directories. We will engage in these activities to manage our contractual relationship with you, based on our legitimate interests and/or to comply with a legal obligation.
- **Workforce Analytics:** We use workforce analytics for succession planning, workforce management, data security. For instance, we use workforce analytics to assist in planning succession and to ensure business continuity, to design employee retention programs and diversity initiatives, to offer training opportunities and to identify patterns in the use of technology systems to information entrusted to us as well as to protect LeasePlan's people and property. We will engage in these activities based on our legitimate interests.
- **Communications, Facilities and Emergencies:** Facilitating communication with you, ensuring business continuity and crisis management, providing references, protecting the health and safety of employees and others, safeguarding and maintaining IT infrastructure, office equipment, facilities and other property, facilitating communication with you and your nominated contacts in an emergency. We will engage in these activities to manage our contractual relationship with you, based on our legitimate interests and/or to comply with a legal obligation.
- **Business Operations:** Operating and managing the IT, communications systems and facilities, managing company assets, allocating company assets and human resources, strategic planning, project management, business continuity, compilation of audit trails and other reporting tools, maintaining records relating to business activities, budgeting, financial management and reporting, communications, managing mergers, acquisitions, sales, re-organizations or disposals and integration with purchaser. We will engage in these activities based on our legitimate interests and/or to comply with a legal obligation.
- **Monitoring:** Monitoring compliance with the Code of Conduct and internal policies, including pursuant to the Company's policies and procedures with regard to monitoring of telephone, email, Internet and other company resources, and other monitoring activities as permitted by local law. We will engage in these activities based on our legitimate interests and/or to comply with a legal obligation.
- **Compliance:** Complying with legal and other requirements applicable to our businesses in all countries in which we operate, such as income tax and national insurance deductions, record-keeping and reporting obligations, conducting audits, compliance with government inspections and other requests from government or other public authorities, responding to legal process such as subpoenas, pursuing legal rights and remedies, defending litigation, and managing any internal complaints or claims (including those received through the Global Whistleblowing Policy), conducting investigations including employee reporting of allegations of wrongdoing, policy violations, fraud, or financial reporting concerns, and complying with internal policies and

procedures. We will engage in these activities to manage our contractual relationship with you, based on our legitimate interests and/or to comply with a legal obligation.

Employee Screening Checks

Leaseplan is required to undertake checks on employees and other staff. These include criminal record checks, credit checks, fraud checks and (if you are a director) adverse media checks. In addition, they include financial services regulatory checks, companies house checks, qualification checks, regulatory reference checks, performance evaluation checks (in each case as relevant to your role/the role for which you have applied).

These checks happen usually only after candidates have signed employment contracts. Leaseplan performs assessments using the outcomes of these checks (more details below). We will undertake some of these checks on a five year cycle. All this is explained in more detail below.

What are criminal record checks?

DBS (Disclosure Barring Service) checks are performed for Leaseplan by third party agencies. In this way we can find out information about criminal records and unspent convictions (depending on whether a basic or enhanced check is performed). They involve us sharing your personal information with third party agencies who perform these checks for us.

You can find out more here:

<https://www.gov.uk/government/organisations/disclosure-and-barring-service/about>

What are credit reference checks?

CRA (credit reference agency) checks involve us sharing your personal information with the UK's CRAs. They also involve us sharing your personal information with third party agencies who perform these checks for us.

The CRAs will give us information about you including about your financial situation and financial history. CRAs will supply us with both public (including the electoral register) information and shared credit, financial situation and financial history information and fraud prevention information. We will use this information to assess your financial position, to verify the accuracy of the data you have provided to us, and to meet our regulatory expectations in respect of financial crime and conduct risk management.

We are required to tell you that the identities of the CRAs, their role also as fraud prevention agencies, the data they hold, the ways in which they use and share personal information, data retention periods and your data protection rights with the CRAs are explained in more detail within the Credit Reference Agencies Information Document (CRAIN). The CRAIN can be found at the links below. You have a right to apply to the CRAs for a copy of your file. The information they hold may not be the same and there is a small fee that you may need to pay to each agency.

Callcredit Limited	Post: Callcredit Information Group, One Park Lane, Leeds, West Yorkshire LS3 1EP. Web Address: http://www.callcredit.co.uk/consumer-solutions/contact-us Email: consumer@callcreditgroup.com Phone: 0330 024 7574 Crain: www.callcredit.co.uk/crain
Equifax Limited	Post: Equifax Ltd, Customer Service Centre PO Box 10036, Leicester, LE3 4FS. Web Address: https://www.equifax.co.uk/Contact-us/Contact Us Personal Solutions.html Email: www.equifax.co.uk/ask Phone: 0333 321 4043 or 0800 014 2955 Crain: www.equifax.co.uk/crain
Experian Limited	Post: Experian, PO BOX 9000, Nottingham, NG80 7WF Web Address: http://www.experian.co.uk/consumer/contact-us/index.html Email: consumer.helpservice@uk.experian.com Phone: 0344 481 0800 or 0800 013 8888 Crain: www.experian.co.uk/crain

What are fraud checks?

The personal information we have collected from you will be shared with Fraud Prevention Agencies (including CIFAS) who will use it to prevent fraud and money-laundering and to verify your identity. If fraud is detected, you could be refused employment or have your employment or other relationship with us terminated. Further details of how your information will be used by us and these fraud prevention agencies, and your data protection rights, can be found at the end of this privacy notice. These checks involve us sharing your personal information with third party agencies who perform these checks for us.

What are adverse media checks?

These checks involve us sharing your personal information with third party agencies who perform these checks for us. Adverse media checks are only relevant to director level roles.

What is a Financial Services Register Check?

This is a check of the FCA Register to check that there have been no issues with your FCA registrations (if relevant to your role). These are performed when you are appointed and regularly after that.

What is a Companies House Check?

This is a check at Companies House to ensure the individual has not been disqualified/there have been no issues with companies for which the individual has been a director. These are performed when you are appointed as a director and regularly after that.

What is a Qualification Check?

This is a standard reference check that will be undertaken for all relevant staff on joining.

What is a Sanctions check?

Sanctions checks are searches that include a number of government sanction databases that identify individuals who are prohibited from certain activities or industries. For relevant roles, these checks will be carried out on joining or appointment and regularly after that.

What is a Performance Evaluation?

These are our standard performance reviews that all staff will complete annually with their line manager.

Using and processing your personal information: the legal basis and purposes

We process your personal information for particular purposes in connection with your employment relationship with us, or your other relationship with us for your services, and for the management and administration of our business. Data protection laws require us to explain the legal grounds to justify this processing.

Please refer to **The LeasePlan Privacy Policy for Employee Data (available on the Global Dashboard)** for full details about the legal basis and purposes.

In addition please note our lawful reasons under data protection laws for the processing of your personal information relevant to the credit reference fraud and other checks (described above) which are specific to the UK are as follows. Fraud checks and related processing is for compliance with our legal obligations. Credit checks and related processing are for our legitimate interests. The other checks described above are for compliance with legal obligations and for our legitimate interests.

Types Of Sensitive Personal Data We Collect, Use, Transfer And Disclose:

We use sensitive Personal Data under one (or more) of the following circumstances:

- as required for the performance of a task carried out to comply with a legal obligation or sectorial recommendation to which LeasePlan is subject;
- by or allowed under applicable local law;
- for the establishment, exercise or defense of a legal claim;
- to protect a your vital interests , but only where it is impossible to obtain your consent first; or
- to the extent necessary to comply with an obligation of international public law (e.g., treaties).

Besides the circumstances mentioned above, we may collect and use the following types of sensitive Personal Data for the following purposes:

- **Racial or ethnic data:**
 - in some countries photos and video images qualify as racial or ethnic data. LeasePlan may process photos (e.g., a copy of a passport containing a photo) and video images for the protection of LeasePlan's and others' assets, including the pre-and in-employment screening and monitoring of employees, to verify and confirm advice in the course of business (e.g., when you participate in video conferencing which is recorded), for site access and security reasons and for inclusion in employee directories; and
- **Health data** (including data relating to disabilities and absence due to illness or pregnancy, excluding details):
 - providing health services to you, provided that the relevant health data are processed by or under the supervision of a health professional who is subject to professional confidentiality requirements;
 - administering pensions, health and welfare benefit plans, maternity, paternity or family leave programs, or collective agreements (or similar arrangements) that create rights depending on your state of health;
 - reintegrating or providing support for employees entitled to benefits in connection with illness or work incapacity;
 - for the pre-and in-employment screening and monitoring of employees and for assessing and making decisions on (continued) eligibility for positions, projects or scope of responsibilities; and
 - providing facilities in the workplace to accommodate health problems or disabilities.
- **Criminal data** (including data relating to criminal behavior, criminal records or proceedings regarding criminal or unlawful behavior):
 - assessing an application by you, to make a decision about you, or to provide a service to you; and
 - protecting the interests of LeasePlan or its employees and clients, including the safeguarding of the security and integrity of the financial sector with respect to criminal offences that have been or, given the relevant circumstances are suspected

to be or have been, committed against LeasePlan or its employees and clients and further for pre- and in-employment screening and monitoring of employees.

- **Sexual preference** (including data relating to partners of employees):
 - to administer employee pensions and benefits programs; and
 - to administer employee memberships.
- **Religious or philosophical beliefs:**
 - to accommodate religious or philosophical practices, dietary requirements or religious holidays.

The Categories Of Unaffiliated Third Parties With Whom LeasePlan Shares Personal Data

- **Professional Advisors:** Accountants, auditors, lawyers, insurers, bankers, and other outside professional advisors in the country of your LeasePlan entity or at the Corporate office in the Netherlands. Example given: an Enneagram consultant with whom we share the names of employees and years in service at LeasePlan, a local data specialist with whom we share a country's employee file (birth date, role, department & working hours) to gather facts and figures on strategic workforce planning.
- **Service Providers:** Companies that provide products and services to LeasePlan such as payroll, pension scheme, benefits providers; human resources services, performance management, training, expense management, IT systems suppliers and support; third parties assisting with equity compensation programs, credit card companies, medical or health practitioners, trade bodies and associations, and other service providers.
- **Public and Governmental Authorities:** Entities that regulate or have jurisdiction over LeasePlan such as regulatory authorities, law enforcement, public bodies, and judicial bodies.
- **Corporate Transaction:** A third party in connection with any proposed or actual reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of LeasePlan business, assets or stock (including in connection with any bankruptcy or similar proceedings).

Other Sources From Whom We Receive Personal Data

- Colleagues;
- Managers;
- References you provide;
- Your use of Leaseplan assets, systems and platforms
- Security control systems and IT systems
- Your dependents and beneficiaries;
- Prior employers or schools;
- Clients
- Background check providers;
- Publicly available directories and online resources;
- Recruitment agencies, employment agencies and recruitment consultants (if you are a temporary or agency worker);
- Other third parties where lawful to do so;

- Health care provider; and
- Local Authority.

Transfers of Personal Data

- For a list of the LeasePlan affiliates that jointly process and use Personal Data (and their locations), see the LeasePlan Global Dashboard. The Company and LeasePlan will remain jointly responsible for Personal Data about you that is transferred and jointly used.
- Some of these countries are recognized by the European Commission as providing an adequate level of protection according to EEA standards (the full list of these countries is available via this hyperlink to EU Commission's adequacy list online: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en). With regard to transfers from the EEA to other countries, we have put in place adequate measures, such as standard contractual clauses adopted by the European Commission and binding corporate rules to protect your information. Employees in the EEA may obtain a copy of these measures by contacting your local Data Privacy Officer.

Criteria Used To Determine Our Retention Periods

- The duration of your employment;
- As long as we have an ongoing relationship with you or your Dependents;
- As required by a legal obligation to which we are subject; and
- As advisable in light of our legal position (such as in regard of applicable statutes of limitations, litigation, or regulatory investigations).