lopital®

If caregivers have a choice, they choose Lopital

Privacy policy Lopital Nederland B.V.

Lopital Nederland B.V.
Laarakkerweg 9, 5061 JR Oisterwijk
Tel +31 (0)13 52.39.300, E-mail info@lopital.nl, www.lopital.nl

IBAN: NL50 INGB 0676 0858 22
BIC: INGBNL2A

BTW/Tax: NL005517692.B01
BTW/Tax: BE0896.717.884
KVK: 18023784

Lopital België B.V.
Antwerpsesteenweg 124, B-2630 Aartselaar
Tel +32 (0)3 870.51.60, E-mail info@lopital.be, www.lopital.be

Table of contents

Details

Document history

Published by: Iris Brans
Released by: Iris Brans
Date: 28-3-2025
Status: Concept
Version: 1.0

Version management

Date	Name	Change	Version
28-03-2025	Iris Brans	Document outline	1.0

1. Introduction

Lopital Nederland B.V. (hereinafter: Lopital) processes personal data of employees to ensure a safe, efficient and professional working environment. This privacy policy describes how Lopital handles the personal data of employees and how it complies with the General Data Protection Regulation (GDPR).

1.1 Period of validity

This policy has been established by the management of Lopital in collaboration with a Cybersecurity and Information Security Advisor. It will be reviewed at least once a year and updated if necessary.

1.2 Definitions

The definitions in Article 4 of the GDPR apply to this privacy policy.

1.3 Vision

Lopital strives for a strong privacy culture in which employees are aware of the importance of data protection. Responsible handling of personal data is essential for a safe working environment and contributes to the protection of employee rights. Privacy is a shared responsibility within the organization.

1.4 Purpose

This policy provides a framework for the careful processing of employees' personal data and sets out responsibilities in the area of data protection. The practical implementation of this policy is further elaborated in internal guidelines and procedures, such as:

- Data breach procedure in accordance with Article 33 of the GDPR.
- Privacy by Design & Default for internal systems and processes.
- Access and security policy for IT systems and physical documents.

Lopital also has a cyber hygiene policy and a cybersecurity policy in place to ensure the availability, integrity and confidentiality of personal data.

1.5 Responsibility of employees

Every employee is responsible for complying with this policy and handling personal data with care. Lopital expects employees to follow privacy rules and contribute to a privacy-conscious working environment.

1.6 Scope

This policy applies to all processing of personal data within Lopital relating to employees, including:

1. Personnel administration, such as payroll processing and leave registration.
2. IT and access management, including email use and workplace monitoring.
3. Data exchange with external service providers, such as payroll processors and occupational health and safety services.

Lopital processes personal data of employees exclusively for legitimate and necessary purposes and is committed to transparent and secure processing as set out in Articles 5 and 13 of the GDPR.

1.7 Responsible party

Lopital is the controller responsible for the personal data of employees. Questions about this policy can be directed to the Finance Manager.

2. Principles for the processing of personal data

The GDPR is based on a number of principles for the processing of personal data. Lopital endorses these principles and processes personal data of employees exclusively in accordance with these principles.

2.1 Lawful basis

Lopital processes employees' personal data exclusively in accordance with the law and in a careful manner. This means that data processing only takes place if there is a lawful basis for doing so, such as the performance of the employment contract, a legal obligation or a legitimate interest of Lopital.

2.2 Clear purposes

Personal data of employees are only processed for predetermined and legitimate purposes, such as payroll administration, personnel management, absence registration and security. No personal data that are not necessary for these purposes are processed.

2.3 Restriction of further processing

Personal data of employees will only be used for other purposes if this is compatible with the original purpose, there are no adverse consequences for the employee and additional safeguards have been put in place.

2.4 Minimum data processing

Lopital only processes personal data that is strictly necessary for the purpose in question. Where possible, processing with less data or pseudonymization is chosen.

2.5 Accurate and up-to-date data

Lopital ensures that employees' personal data is accurate and up to date. Employees are encouraged to report any changes to their data in a timely manner. Incorrect or outdated data will be corrected or deleted as soon as possible.

2.6 Retention periods

Employee personal data is not retained for longer than is necessary for the purpose for which it was collected or for as long as required by law. After the retention period has expired, data is deleted or anonymized. More information on this can be found in Chapter 6.

2.7 Integrity and confidentiality

Lopital takes technical and organizational measures to protect employees' personal data against loss, unauthorized access or unlawful processing. This policy is in line with the internal cyber hygiene and cyber security policy.

2.8 Privacy by Design & Default

When introducing new systems or processes, privacy is taken into account from the design stage onwards, so that personal data is optimally protected. Default settings are configured to be as privacy-friendly as possible.

2.9 Access to data

Only authorized employees have access to personnel data. Access rights are periodically evaluated and recorded in the access policy within the cybersecurity policy. Unauthorized access is actively prevented.

2.10 Personal data breaches

In the event of a data breach or unauthorized access to personal data, we will act in accordance with our internal data breach procedure. If necessary, a report will be made to the Data Protection Authority and the employees involved will be informed.

2.11 External processors

When Lopital engages external parties to process employee data (e.g. payroll administration), contractual agreements are laid down in processing agreements. External parties must guarantee an appropriate level of data protection.

2.12 Transparency

Employees are clearly informed about how Lopital processes their personal data and what rights they have. This is done via this privacy policy and additional information in the staff handbook or via internal communication channels.

2.13 Essential documentation

In order to comply with the GDPR and ensure privacy protection, Lopital has the following documentation in place:

- Processing register with personnel data;
- Processing agreements with external parties;
- Internal privacy policy for employees;
- Cybersecurity Risk Assessment;
- Cyber hygiene policy;
- Cybersecurity policy;
- Data breach register and protocol.

2.14 Supervision and advice

Lopital has no legal obligation to appoint a Data Protection Officer (DPO). However, an external advisor is called in where necessary to provide advice on information security and privacy. Internally, the Finance Manager supervises compliance with this policy.

3. What personal data do we process?

Lopital processes personal data of (potential) employees and former employees. We process the following personal data, among other things:

- Identification data (such as name, date of birth, national insurance number, copy of ID);
- Contact details (address, telephone number, email address);
- Financial data (bank account number, salary details, payroll taxes);
- Leave and absence data (registration of absences, reintegration files);
- Work-related data (job title, contact details, performance, appraisals, training details);
- Application details (CV, cover letter and other information provided during an application procedure);
- Other data that employees actively provide, for example in correspondence or by telephone;

4. Purposes of processing

Lopital processes personal data of employees exclusively for the following purposes:

- Entering into, executing and terminating employment contracts and other working relationships;
- Conducting personnel administration, payroll administration and absence registration;
- Complying with legal obligations (such as tax legislation, social security legislation and health and safety legislation);
- Ensuring a safe and efficient working environment (e.g. access control, IT security);
- Managing personnel files and assessing performance and development;
- Facilitating education, training and development programs;
- Recording leave and absences;
- Maintaining communication with employees on company-related matters;
- Handling complaints, disputes or legal proceeding involving employees;
- Archiving purposes, whereby data is used exclusively in legal proceedings or for historical, statistical or scientific purposes.

Lopital processes personal data through, among others, the HR department, payroll administration and IT systems. This is done on the basis of legal obligations, the execution of the employment contract or the legitimate interest of Lopital. Data is only processed for the relevant purpose and will not be used for other purposes without prior consent.

In some cases, data may be used in anonymized form for statistical analyses and reports.

5. Legal basis for processing

We process personal data on the basis of:

- Consent of the data subject (Artikel 6(1)(a) of the GDPR);
- Performance of a contract (Article 6(1)(b) of the GDPR);
- Legal obligation (Article 6(1)(c) of the GDPR);
- Legitimate interest (Article 6(1)(f) of the GDPR).

Lopital processes certain personal data of employees based on legitimate interest (Article 6(1)(f) of the GDPR). This means that the processing is necessary for a legitimate purpose of Lopital, provided that this interest outweighs the privacy rights of employees.

Examples of legitimate interests:

- IT and business security: access control, network monitoring and fraud prevention.
- Efficient business operations: Personnel administration, internal communication and schedule management.
- Performance management and quality control: performance reviews and handling complaints.

Lopital considers whether each processing operation is necessary and proportionate and takes appropriate measures to minimize privacy risks. Employees may object if they believe that their privacy interests outweigh the interests of Lopital.

6. Retention periods

We do not retain personal data for longer than is necessary for the purpose for which it was collected, unless a longer retention period is required by law. The following retention periods apply:

Type of personal data	Retention period	Legal basis/reason
Identification details	5 years after termination of employment	Tax and social security law
Contact details	Up to 2 years after termination of employment	Only if necessary for reference
Financial details	7 years after termination of employment	Tax legislation
Leave and absence details	2 years after recovery	Gatekeeper Improvement Act
Employment contract and related documents	7 years after end of employment	Tax and employment law obligations
Appraisals and performance reviews	Up to 2 years after termination of employment	Best practice, unless legally relevant
Application details	4 weeks after rejection (or 1 year with permission)	GDPR guidelines
Education and training details	Up to 2 years after termination of employment	Relevance for HR administration

7. Sharing personal data with third parties

Unless stated otherwise in this policy, personal data of employees will not be rented, sold or otherwise shared with third parties. Lopital may share data with third parties if the employee has given their explicit consent or if this is necessary to comply with a legal obligation, such as a request from law enforcement authorities or fraud prevention organizations.

In addition, business service providers may perform certain HR or administrative processes on behalf of Lopital, such as payroll administration or IT services. Contractual agreements are made with these processors to ensure confidential and careful handling of personal data, as laid down in processing agreements.

7.1 Transfer of personal data outside the EU

In principle, Lopital does not transfer personal data of employees to countries outside the EU. If this is necessary for IT services or payroll processing, for example, this will only be done with appropriate safeguards, such as:

- An adequacy decision by the European Commission, if applicable.
- Model contracts approved by the European Commission that guarantee the protection of personal data.
- Explicit consent from the employee in specific cases.

Lopital takes measures to ensure the security and confidentiality of data during international transfers.

8. Security measures

We take appropriate technical and organizational measures to protect personal data, including:

- Secure storage and encryption of data;
- Access control and authorization management;
- Periodic audits and updates
- Incident management and data management;
- Multi-factor authentication for accounts or systems;
- Regular backups;
- Role-based access;
- SSL security;
- Password protection and policy;
- Firewall;
- Logging;
- Network segmentation;
- Virus, malware en phishing detection;
- Automatic updates and patches;
- Necessary organisation documentation;
- Data breach protocol and register;
- Cybersecurity Risk Assessment.

9. Rights of data subjects

Data subjects have the following rights:

1. **Right of access – Article 15 GDPR**
   Data subjects have the right to know what personal data is being processed about them and for what purposes.

2. **Right to be forgotten (right to erasure) – Article 17 GDPR**
   Data subjects may request that their personal data be deleted, provided that there is no legal obligation to retain it.

3. **Right to rectification or supplementation – Article 16 GDPR**
Data subjects may have inaccurate or incomplete data corrected or supplemented.

4. **Right to data portability – Article 20 GDPR**
Data subjects have the right to receive their personal data in a structured, commonly used and machine-readable format and to transfer it to another organization.

5. **Right to withdraw consent – Article 7 lid 3 GDPR**
Where processing is based on consent, the data subject has the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

6. **Right to restriction of processing – Article 18 GDPR**
Data subjects may, under certain circumstances, request that the processing of their personal data be temporarily restricted, for example if the accuracy of the data is disputed.

7. **Right to object– Article 21 GDPR**
Data subjects may object to the processing of their personal data on the basis of legitimate interests or for direct marketing purposes.

9.1 Rules for employees

The rules for employees are described in the cyber hygiene policy.

10. Internal procedures at Lopital

Lopital has the following internal procedures in place to guarantee cybersecurity and information security:

- **Privacy-audit:** AMVM Advise conducts an internal privacy audit.
- **Data breach procedure:** Data breaches are reported to the Data Protection Authority within 72 hours in accordance with Article 33 of the GDPR.
- **Privacy by Design & Default:** All systems and processes are designed to ensure privacy protection (Article 25 of the GDPR).
- **Incident management:** A protocol for identifying and addressing security incidents is available to all employees.
- **Processing register:** Lopital keeps a register of all data processing activities (Article 30 of the GDPR).
- **Risk analysis and management**: Lopital has a risk analysis focused on internal processes, systems, data and other IT & OT resources. Based on this risk analysis, control measures are taken to prioritize and mitigate the risks.

11. Roles and responsibilities

Within Lopital, there are roles and responsibilities relating to the GDPR and overall cybersecurity. An overview is provided below.

- **Director:** Ultimately responsible for GDPR compliance.
- **Finance Manager:** Responsible for internal communication, compliance with policies and procedures.
- **AMVM Advice:** Responsible for advising and supporting with regard to privacy and cybersecurity where necessary.
- **General employee:** Responsible for working with personal data in an appropriate manner and complying with policy.

12. Changes to this policy

This privacy policy is subject to change. The most current version is always available. Important changes will be actively communicated by the Finance Manager.

.