

## LANSWEEPER WHISTLEBLOWING PRIVACY POLICY

### I. Introduction

This Privacy Policy applies to Lansweeper NV, a limited liability company existing under Belgian laws with registered office at Fraterstraat 12, 9820 Merelbeke and registered with the Crossroads Bank for Enterprises under company number 0538.668.417 and its affiliates (hereinafter referred to as "**LANSWEEPER**" or "**We**").

With this Privacy Policy, LANSWEEPER would like to inform you why and how LANSWEEPER collects and processes personal data as part of the whistleblowing process, as we attach great importance to the protection of your privacy during the processing of your personal data.

By using the report form, the whistleblower agrees to the processing of his/her Personal Data for the purposes indicated in this Privacy Statement.

LANSWEEPER's whistleblowing process is in accordance with EU Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (hereinafter the "**Directive**"), the regulation on the protection of personal data being EU Regulation No. 2016/679 (hereinafter "**GDPR**"), the Belgian law transposing this Directive of 28 November 2022 on the protection of reporting persons of breaches of Union or national law adopted within a legal entity in the private sector (Belgian *Official Gazette* of 15 December 2022), as well as the Spanish Act 2/2023 on the protection of persons who report regulatory breaches and anti-corruption measures.

More information about the scope, the reporting procedure and the protection mechanisms for whistleblowers can be found online in our General Policy on Whistleblowing, published on our website [www.lansweeper.com/whistleblowing](http://www.lansweeper.com/whistleblowing).

As a data controller pursuant to Article 4 of the GDPR, We are responsible for the processing of the personal data that LANSWEEPER collects and processes in order to comply with the Whistleblowing legislation.

### II. How do we process your personal data?

The processing of personal data is carried out on paper and/or with the help of digital media.

LANSWEEPER will treat the information provided confidentially and only certain persons who are authorized to perform these tasks and who have been made aware of the restrictions imposed by the legislation on the protection of personal data will process your personal data.

LANSWEEPER will never disclose the information provided without any legal basis.

LANSWEEPER has taken appropriate and organizational measures to protect your personal data against any form of loss or unlawful processing, such as secure network protocol, end-to-end encryption and strong authentication mechanisms.

### III. Which types of personal data do we process?

LANSWEEPER may collect the following personal data from you (in case you are the reporting person) or process it from a third person (in case you are the accused person and/or a witness):

#### 1. Basic Identification Data

The submittal of reports is done anonymously, however the Whistleblower may choose to voluntarily provide his/her basic identification data. By "basic identification data" we mean any information that refers to a particular natural living person.

This personal data may contain basic identification data such as your first and last name, address, profession, contact details and any other information you have given us about the yourself and/or person(s) involved in the report.

2. Sensitive categories of personal data

Special categories of personal data may be collected as a result of a report. This includes, for example, personal data relating to race or ethnicity, health, sex life, religion or personal beliefs or trade union membership.

In this case, such personal data will only be processed to the extent permitted by applicable law or the need to establish a breach, or to exercise whistleblower rights.

If, on the other hand, this sensitive personal data is not relevant and falls outside the scope of the applicable law or is not necessary to exercise a rights, it will be deleted immediately.

3. A description of the alleged infringement and a description of the circumstances of the case.

When LANSWEEPER receives a report, a file is created containing the data of the report.

After all, We process this personal data for internal reporting purposes to disclose information internally such as the number of reports We receive and about all the actions We have taken as a result of such reports by whistleblowers. However, this never includes information that identifies individual whistleblowers or their employers (including ex-employers).

Within the description of the alleged breach that you provide, personal data may be processed around:

1. unlawful conduct or violations of the company of which you have become aware in relation to your relationship with LANSWEEPER;
2. unethical behavior, contrary to LANSWEEPER's ethical principles.

#### **IV. For which purposes do We process your personal data?**

We need the information you provide with your report to investigate your report, including any evidence you have provided to us. We need to know the details of your complaint so that We can make a decision about LANSWEEPER's compliance with the relevant legislation and fulfil our obligations.

Your personal data will be processed for the following purposes:

1. Enable you to submit reports;
2. enable LANSWEEPER to process, review and further investigate your reports by involving any relevant LANSWEEPER departments;
3. Comply with legal obligations of competent authorities;
4. enable LANSWEEPER to establish, exercise or defend our rights;
5. Carrying out our controls and activities to monitor business risks and improve our internal processes.

#### **V. On which legal ground do we process your personal data?**

Personal data mentioned in reports of alleged breaches will only be processed on one of the legal basis provided in article 6 GDPR, namely on the basis of a legal obligation, as this information is necessary to comply with the EU Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, the Belgian law transposing this Directive of 28 November 2022 on the protection of those reporting breaches of Union or national law adopted within a legal entity in the private sector

(Belgian Official Gazette of 15 December 2022) as well as the Spanish Act 2/2023 on the protection of persons who report regulatory breaches and anti-corruption measures.

## **VI. Are your personal data being transferred to a third party?**

LANSWEEPER may, directly or indirectly, transfer personal data to:

### **1. Supervisory public institutions:**

As a result of the investigation of the report, LANSWEEPER will in some circumstances be required to pass on personal data information to the relevant supervisory authority, tax authority or public prosecutor's office competent to investigate the related infringement.

These entities will act as independent controllers of the respective processing operations.

### **2. LANSWEEPER and its affiliated Companies:**

Only authorized employees have access to the personal data. These are persons who have been specifically designated and can thereby guarantee the complete confidentiality of the personal data provided in accordance with the most appropriate security measures implemented by LANSWEEPER.

Your personal data may be used by LANSWEEPER personnel who have been assigned to a specific role, are bound by a confidentiality obligation and have received appropriate instructions.

Your personal data will only be made accessible to those persons who need it within the Group for the purposes of their job or hierarchical position. These individuals will be duly instructed to prevent the loss, destruction, unauthorized access, or unauthorized processing of data.

These companies act as part of the designated data controller, LANSWEEPER NV, unless they act as third-party data processors on behalf of LANSWEEPER.

### **3. LANSWEEPER Service Providers:**

In addition, the data may be used by third-party companies that carry out instrumental activities on behalf of LANSWEEPER, such as service providers (including IT companies) entrusted with specific management of contractual obligations, external consultants for the management of the investigation process and legal assistance, companies and companies in the context of assistance and advisory relationships.

These companies act as third-party data processors and are under the direction and control of LANSWEEPER, unless they act as third-party data processors on behalf of LANSWEEPER and have therefore signed a specific contract governing the processing entrusted to them, in accordance with Article 28 of the GDPR.

## **VII. How long do we process your personal data?**

Personal data obtained in the context of whistleblowing services is kept for a period of 5 to 10 years, depending on the severity of the breach in case the report is deemed acceptable for further investigation. Reports that may give rise to criminal investigations can be kept for a period of up to 10 years.

In case your report is refused for further investigation, the personal data will be removed after two months after written feedback of the negative decision to investigate the report.

Your personal data will be processed and stored, in accordance with LANSWEEPER's data retention policy, for the time necessary to manage the reports and for the period strictly necessary to achieve the purposes for which they were collected and for the fulfilment of applicable legal obligations.

In addition, the data will be deleted or permanently anonymized when the above purposes are achieved, unless the data controller is obliged to keep the data for a further period of time in order to comply with legal obligations.

In any case, your data will not be stored for more than 10 years after the report has been submitted.

### **VIII. Do we transfer your personal data outside the EEA?**

LANSWEEPER may transfer your personal data to parties located in third countries, i.e. countries outside the European Economic Area (i.e. the European Union, Norway, Iceland and Liechtenstein).

However, such a transfer is only possible if the country in which the receiving party is established offers sufficient legal safeguards to protect your personal data and which the European Commission has assessed as adequate. In other cases, LANSWEEPER has concluded a standard contractual clause with the recipient in order to provide the same level of protection as in Europe.

If more information or a copy of the safeguards for these international transfers of personal data is desired, the procedure described in Article 10 can always be followed.

### **IX. What are your privacy rights?**

Data protection law provides for various rights for data subjects in relation to the processing of personal data so that the data subject can continue to exercise sufficient control over the processing of their personal data.

LANSWEEPER already tries to provide as much information as possible to data subjects through current policy in order to be as transparent as possible with regard to the processing of personal data.

LANSWEEPER understands that the data subject may still have questions or require additional clarifications regarding the processing of his or her personal data. LANSWEEPER therefore understands the importance of the rights and will therefore comply with these rights taking into account the legal restrictions in the exercise of these rights. The different rights are described in more detail below.

- ***Right of access/inspection***

You have the right to obtain confirmation from LANSWEEPER as to whether or not your personal data is being processed. In the positive case, the data subject may request access to his or her personal data.

LANSWEEPER will inform the data subject of the following:

1. the purposes of processing;
2. the categories of personal data concerned;
3. the recipients or categories of recipients to whom the personal data have been disclosed;
4. the transfer to recipients in third countries or international organizations;
5. if possible, the period for which the personal data is expected to be stored, or if that is not possible, the criteria for determining that period;
6. that the data subject has the right to request from the organization that personal data be corrected or erased, or that the processing of personal data concerning him or her be restricted, as well as the right to object to such processing;
7. that the data subject has the right to lodge a complaint with a supervisory authority;
8. where the personal data are not collected from the data subject, all available information on the source of those data;
9. the existence of automated decision-making, including profiling, and useful information about the logic underlying this decision-making and the significance and expected consequences of that processing for the data subject.

LANSWEEPER also provides a copy of the personal data being processed. If the data subject requests additional copies, LANSWEEPER may charge a reasonable fee.

- **Right to rectification**

If the data subject becomes aware that LANSWEEPER has incorrect or incomplete personal data concerning him/her, the data subject has the right to report this to the organization at any time so that the necessary steps can be taken to correct or supplement this data. It is the responsibility of the data subject to provide accurate personal data to the organization.

- **Right to be forgotten**

You can request the erasure of your personal data if the processing does not comply with data protection legislation and within the limits of the law (Art. 17 GDPR).

- **Right to restriction of processing**

You can request that the processing be restricted if:

1. the accuracy of the personal data has been questioned and for the period to verify the accuracy;
2. the processing is unlawful and the data subject does not wish the data to be erased;
3. the organization no longer needs the data, but asks the data subject not to delete it as he or she needs it in the exercise or defense of a legal claim;
4. Objection to the processing is made pending the clarification of the legitimate interests that outweigh the interests of the data subject.

- **Right to data portability**

You have the right to obtain his personal data that he has provided to the organization in a structured, commonly used and machine-readable format. The data subject has the right to transfer this personal data (directly by the organization) to another controller. This is possible if the processing is based on your consent and on the basis of processing via an automated process.

- **Right to object**

When personal data is processed for direct marketing purposes (including profiling), you can always object to the processing.

You can also object to the processing due to a specific situation relating to the data subject. The organization will cease the processing unless the organization can demonstrate compelling legitimate grounds for the processing that override the interests of the data subject or that are related to the exercise or defense of a legal claim.

- **Automated individual decision-making**

You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him in any other way, such as the evaluation of personal aspects relating to the performance of work, reliability, creditworthiness, etc.

This right not to be subject to such automated decision-making does not exist when the decision is permitted by a mandatory statutory provision.

You may also invoke this right if the decision is necessary for the conclusion or performance of the contract between you and LANSWEEPER or is based on your express consent. In these last two cases, you do have the right to the human intervention of someone from LANSWEEPER and he/she has the right to express his/her point of view and to contest the automated decision.

- **Right to withdraw consent**

If you have given your consent to LANSWEEPER to process your data for a specific processing purpose, you can revoke this consent at any time by sending an e-mail in accordance with the procedure explained in the following article.

**X. How can you exercise your rights?**

To exercise the rights mentioned above, you can send us a written request, dated and signed, with a copy of the front of your identity document.

The request can be sent:

- per e-mail: [whistleblowing@lansweeper.com](mailto:whistleblowing@lansweeper.com);
- in writing to the following postal address: Fraterstraat 12, 9820 Merelbeke, Belgium.

When exercising your right, we ask you to clearly indicate which right you wish to invoke.

The request to obtain a copy of the data will be processed within one month. This period may be extended by two months, taking into account factors such as complexity and the number of requests. In the event of an extension of the deadline, you will be informed of this and of the reasons for the extension.

We will notify third parties to whom the data has been communicated of any rectification, erasure or restriction that has been carried out, unless this is not possible or requires a disproportionate effort.

We are committed to working with you to find a fair resolution to any complaint or concern about your privacy. However, if you believe that we have not been able to assist you with your complaint or concern, you have the right to lodge a complaint with the data protection authority of the country in which you reside using their website.

If you live in Belgium, you can file a complaint with the Belgian Data Protection Authority (GBA/APD). All information about this can be found on <https://www.dataprotectionauthority.be/>.

If you live in Spain, you can file a complaint with the Spanish Data Protection Authority (AEPD). All information about this can be found on [Agencia Española de Protección de Datos | AEPD](#)

**XI. Changes**

We may amend or supplement this Policy as necessary. If significant changes are made to this Privacy Policy, the date on which it is amended will be updated and we will also notify you.

We also encourage you to periodically review this Policy to read the latest version on how we process and protect your personal data.