Privacy policy

Eurides and NS Mobility Services

March 2021

1. Introduction

Eurides and NS Mobility Services are organisations that attach great importance to privacy. The General Data Protection Regulation (hereinafter: GDPR) requires an organisation to think carefully about how it processes and protects personal data. By complying with the accountability obligation, an important contribution is made to the protection of the fundamental right to privacy. Eurides and NS Mobility Services process personal data of various data subjects, such as their own employees, but also customers and users of the Vaigo and NS Go mobility platforms. This policy sets out the rules for the handling of personal data by Eurides and NS Mobility Services.

2. Vision

Eurides and NS Mobiliteitsdiensten are aware that the protection of personal data is important and attach great importance to it that it is processed lawfully, properly and transparently within the organisation. Eurides and NS Mobility Services therefore consider it important that its employees are aware of the importance of privacy and of the rules concerning it. This reduces the chance of incorrect use of data and data breaches. To ensure this, regular awareness training sessions are held. In addition, the rules concerning privacy are discussed when a new employee joins the company.

3. Legislation and definitions

The GDPR provides rules for the reinforcement and extension of the right to personal data protection. Additional rules and national choices of the Netherlands can be found in the GDPR Implementation Act. The GDPR and GDPR Implementation Act form the general legal framework for dealing with personal data.

Below is a brief description of some of the key terms from the GDPR:

Personal data: means any information relating to an identified or identifiable natural person. An identifiable person is a natural person who can be identified, directly or indirectly, in particular 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. This is therefore any information that can be traced back to a specific person.

Data subject: the person to whom the personal data relates. The data subject is the person whose data is processed. This is not only a citizen, but for example also includes, the tenants, visitors and employees of Eurides and NS Mobility Services.

Data Protection Impact Assessment (DPIA): A DPIA assesses the effects and risks of new or existing processing operations on the protection of privacy. This is also called a Data Protection Impact Assessment.

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controller: a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor: a natural or legal person, public authority, agency or other body which processes personal data (on behalf of) the controller.

4. Scope

This privacy policy applies to all processing of personal data by all employees of Eurides and NS Mobility Services. This policy is an elaboration of the legal regulations and a manual for the employees of Eurides and NS Mobility Services. It provides the rules and principles for a fair, careful and lawful processing of personal data.

5. Processing

Processing of personal data is any operation or set of operations with personal data, whether or not performed through automated processes. In the GDPR, processing includes at least the following actions:

- Collect, record and organise
- Save, update and change
- Retrieve, consult, use
- Disclosure by transmission
- Dissemination or otherwise making available
- Bringing together or combinate
- Restrict, erasure or destruction of data

This list shows that basically everything you do with personal data is processing.

As Eurides and NS Mobility Services, we collect various types of personal data in order to carry out our work. This includes processing in connection with applications, the use of the mobility platform and the payment of salaries. Various categories of personal data are collected, including name and address, contact-, travel- and financial data.

Eurides and NS Mobility Services have made an overview of the various processing activities they perform in their record of processing activities. Eurides and NS Mobility Services always keep this record up to date. The processing record contains further information about each processing operation, including the processing purposes, categories of personal data, categories of data subjects and recipients and the data retention period.

6. Purposes

Personal data may only be collected if there is a purpose. This purpose must be well-defined, clearly described and justified. It should also always be checked whether the processing of personal data is necessary for the initial purpose. These processing purposes are the "why" of processing personal data. Purposes are important for different standards. Think for instance about determining who is responsible for processing personal data. Or the question whether the sharing of this data with other organisations is permitted. Purposes are also important for determining retention periods and informing citizens. This way, you know how long it is necessary to retain personal data or what you need to inform the data subjects about.

An important requirement is that the goals must be specifically formulated in advance. The purposes may therefore not be too broadly and vaguely defined, or determined afterwards. Processing for a purpose other than the original purpose is only permitted under strict conditions. Also the type of data has to be taken into account. The general rule is: the more sensitive the data, the less likely it is compatible. The data may then be less likely to be used for a purpose other than that for which it was previously collected. One must also take into account the consequences of the intended processing for the data subject. For example, informing the data subject in advance of the purpose for which the data will be used when the data subject provides her or his personal data to Eurides and NS Mobility Services.

7. Legitimate basis

For any processing of personal data, a legitimate basis in the law must apply. This means that Eurides and NS Mobility Services must always be able to justify on what basis the personal data of the data subjects are processed. An exception to this is the case discussed above where personal data are processed for a purpose other than the purpose for which they were collected. This is only permitted under strict conditions.

For each processing operation, one of the following must apply:

- the data subject has given her/his unambiguous consent to the processing;
- the data processing is necessary for the performance of a contract to which the data subject is party, taking into account also the negotiation phase;
- the data processing is necessary in order to comply with a legal obligation to which Eurides and NS Mobility Services are subject;
- the data processing is necessary in order to protect the vital interests of the data subject (in the context of life or death, e.g. sharing data in the event of emergencies);
- the data processing is necessary for the proper performance of a task carried out in the public interest by the administrative body concerned or by the administrative body to which the data is provided, or
- the data processing is necessary for the protection of the legitimate interest of Eurides/NS Mobility Services or of a third party to whom the data is provided. However, if the interest of protecting the privacy of the data subject outweighs this interest, the processing of data based on a legitimate interest is not applicable.

For all bases, there will always have to be a necessity to process those data. Whether the processing of certain data is necessary must always be justified.
Of the six bases, for Eurides and NS Mobility Services consent, performance of a contract, legal obligation and legitimate interest can apply.

8. Method of processing

Personal data may only be processed in accordance with the law and with due care. Personal data is collected as much as possible from the data subject. The law is based on subsidiarity. This means that processing is only allowed if the goal cannot be achieved in any other way. The
law also speaks of proportionality. This means that personal data may only be

processed if this is in proportion to the purpose. If the same goal can be achieved with no, or less (burdensome) personal data, this must always be chosen.

Personal data must therefore be accurate, relevant, up-to-date and not excessive in relation to the purpose of processing. This means that only the personal data may be used which are strictly necessary for the purpose of processing. For example, if it is sufficient to use someone's contact details, it is not necessary to also ask for a passport photo and Social Security Number. Strict rules apply to the use of a Social Security Number anyway. If anonymous data is sufficient, no traceable personal data may be used. When registering for a visit, for example, we only ask for the visitor's (first and last) name.

Organisational measures

The organisational measures that Eurides/NS Mobility Services has taken are: confidentiality statements, processors also have a duty of confidentiality, employees have been informed about the GDPR by means of training, privacy policy for the handling of personal data by employees with which they must comply.

Security

The ways in which Eurides/NS Mobility Services secures personal data are through: passwords, logging, VPN-access, IT policy.

9. Transfer to third parties

In principle, personal data may not be transferred to an organisation in a country outside the EU. This is because within the EU there is a good protection for the personal data, and outside the EU not in all cases. Transfer is understood to mean, among other things, storage (for example in the Cloud) or making available to an organisation outside the EU. This does not include making personal data visible via the internet to persons outside the EU. Eurides and NS Mobility Services use a few processors that transfer personal data to a country outside the European Economic Area (EEA). These are Pipedrive, Help Scout and Office 365. We have concluded a processing agreement with these parties, which stipulates that these parties are GDPR-compliant.

10. Transparency and communication

Information obligation

Data subjects must be informed about the processing of their personal data by Eurides and NS Mobility Services. The moment of informing and the way in which this is done depends on the question of how the personal data are collected. Namely, whether the data are obtained directly from the data subject or in some other way.

If the personal data are provided by the data subject, then this person must be informed about the processing of his/her data beforehand. If personal data concerning the data subject is not directly obtained from the data subject but somewhere else, such as another organisation, then the data subject only has to be informed at a later stage. The data subject must then be informed only when this personal data is

recorded by Eurides and NS Mobility Services. Or at the moment when the data are given for the first time to another organisation and this is obviously necessary.

Access

Data subjects have the right to access their own personal data. The data subject does not have to give a reason for her or his access request, but she or he may not make too many requests in a short period of time. If a data subject requests access, she or he is entitled to a full overview of the data that are used. Access must also be given to the origin of the data, the recipients of the data and the purposes of the processing of the personal data. Eurides and NS Mobility Services shall ensure that this request is followed up in a timely and complete manner.

Correction and erasure

In addition to the right of access, the data subject also has the right to correct, supplement, erase or restrict her or his personal data. This request must only be complied with if the data is incorrect or incomplete for the purpose for which the data was collected. This request must also be respected if the data is irrelevant or used in breach of the law.

The data subject must clearly indicate in his/her request which data are to be amended for which reason. The right cannot be used to change opinions or research results. If the decision is in favour of the request, the changes must be made as soon as possible.

The changes or erases of personal data must also be communicated to other organisations to which Eurides and NS Mobility Services have provided the data.

Objection

The data subject has the possibility to oppose the use of their personal data. If a data subject objects to the use of her/his personal data, Eurides and NS Mobility Services may no longer use the data. Even if the data processing is in itself justified and permitted. There are a number of situations in which the right to object can be exercised. Firstly, in the event of special personal circumstances and the processing is based on the public law task (not applicable for Eurides and NS Mobility Services). Or in the situation that it concerns an employee and she or he objects to the processing of his or her data based on a legitimate interest due to special personal circumstances.

The data subject may always object to the use of personal data for direct marketing or charitable purposes.

Submission of request

In order to exercise her or his rights, the data subject may submit a request. This request may be made in writing or by e-mail. Eurides and NS Mobility Services will have one month from the receipt of the request to assess whether the request is justified. Within one month, Eurides and NS Mobility Services will indicate what will happen with the request. If the request is not complied with, there is the option of objecting to Eurides/NS Mobility Services or submitting a complaint to the Dutch Data Protection Authority (''Autoriteit

Persoonsgegevens''). On the basis of a request, Eurides and NS Mobility Services may ask for additional information in order to be sure of the identity of the data subject. The manner in which a request is handled and dealt with is laid down in the procedure for *the Rights of the Data Subjects*.

11. Obligations of Eurides and NS Mobility Services

Records of processing activities

Eurides and NS Mobility Services are obliged to document which personal data they process, what the purpose is, from whom or where this data originates and with whom this data is shared. In addition, for each processing operation, we must document and justify the legal basis on which Eurides and NS Mobility Services process personal data.

Retention periods

Eurides and NS Mobility Services do not retain data any longer than is necessary for the purpose of processing. A number of laws include specific storage periods for certain personal data. If no retention period is available, it must be possible to substantiate why personal data is retained for a specific period. When there are still personal data stored that are no longer necessary for achieving the goal, these will be removed as soon as possible. After the storage periods have expired, the personal data must be destroyed or anonymised. This applies not only to the data itself, but also to copies and back-ups. For all personal data, the destruction must be irreversible. So it is not a matter of putting the files in the bin and emptying the bin, but for example overwriting data with zeros, ones and random characters (data wiping).

The manner in which the retention and destruction periods are applied is laid down in the *Retention Period Policy*.

Duty to report data breaches

The duty to report data breaches means that Eurides and NS Mobility Services must report a serious data breach as soon as possible (within 72 hours) to the Dutch Data Protection Authority. A data breach is a breach of security that has significant adverse effects on the party involved or on the protection of personal data. Examples are a lost USB stick with personal data, a stolen laptop or a break-in on the network (hack). If there is a chance that the data breach could have adverse consequences for the data subjects, Eurides and NS Mobility Services must also report it to the data subjects themselves. In addition, the data subject must be informed of the measures that Eurides and NS Mobility Services are taking to limit the risks and damage.

Besides reporting, we must also document all data breaches. With this documentation, the Dutch Data Protection Authority should be able to check whether we as Eurides and NS Mobility Services have complied with the reporting obligation.

The procedure for dealing with data breaches can be found in the *Data Breach Procedure*.

Data processing agreement

Data processing agreements must be concluded each time third parties - also called processors - process personal data on behalf of Eurides and NS Mobility Services. Of course, clear agreements must be made about how these processors are to handle the data they receive from Eurides and NS Mobility Services. Think of what data they need to perform their task. Or the way in which the organisation has secured the data and what it must do if there is a data breach. Eurides and NS Mobility Services have made available a standard data processing agreement that must be used in all these cases.

Data Protection Impact Assessment (DPIA)

A DPIA assesses the impact and risks of new or existing processing activities on the protection of privacy. This applies in particular to processing in which new technologies are used. Eurides and NS Mobility Services only carry these out when:

- there is high-risk (automated) processing,
- there is an (automated) processing for which the Dutch Data Protection Authority has indicated that a DPIA is mandatory;
- large-scale processing takes place,
- or when there is large-scale monitoring of public areas.

Privacy by Design and Privacy by Default

When acquiring or developing products, systems or processes, the protection of personal data must always be taken into account. We call this Privacy by Design (PbD) and Privacy by Default. For all products, systems or processes, the technical and organisational measures must ensure that, as a standard, only the data necessary for the purpose are used. If it becomes apparent that a system involves the processing of sensitive or special personal data and this may entail a high privacy risk, we are obliged to carry out a Data Protection Impact Assessment (DPIA).

Responsibility

The management is responsible for the way in which personal data is handled within Eurides and NS Mobility Services. For substantive questions about this or about the policy and the GDPR, please contact the management. You can reach them via privacy@eurides.eu

For questions, you can also contact our Data Protection Officer, Annemarie Nijhoff. She can be reached via FG@ns.nl