



Privacy Policy: Processing of personal data in the Nordic Road Association NVF

This privacy policy concerns the processing of personal data in the activities of the Nordic Road Association. From this privacy policy, you will find out for what purposes your personal data is used and what rights you have as a data subject.

1. Data controller and contact person

Data controller is the Finnish department of the Nordic Road Association (PTL ry/NVF).

Contact information:

Pohjoismaiden tie- ja liikennefoorumi PTL ry / Suomen osasto
c/o Väylävirasto
Yliopistonkatu 38
33100 Tampere

Contact person responsible for the register:

Anne Ranta-aho
+358 40 8488 638
anne.ranta-aho(a)ftia.fi

2. Purpose and Legal Basis for Processing Personal Data

The purpose of processing personal data is to maintain NVF's membership activities and working group activities, as well as to communicate with NVF members and member companies (including communication related to the distribution of materials).

Personal data is not used for automated decision-making or profiling.

The legal basis for processing personal data in accordance with the General Data Protection Regulation (GDPR) is:

- the individual's consent

The legal basis for processing personal data is based on the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 of the European Parliament and of the Council).

3. Types of Personal Data Collected and Retention of the Data

Following personal data of data subjects are processed:

- name
- title
- contact information (work email address and work phone number)
- company name
- name of the NVF working group

Personal data is collected through the membership register.

The personal data will be kept in the register for as long as the data subject is a member of the NVF.



4. Regular Sources of Data

The personal data is collected directly from the data subjects themselves.

5. Regular Disclosures of Data

Data is disclosed to NVF's Nordic departments, which include the departments of the Faroe Islands, Iceland, Norway, Sweden, and Denmark.

The disclosure of data occurs through the information entered in the NVF's Nordic membership register. The Nordic membership register is a prerequisite for NVF's working group activities. (Members of the working groups are expected to be in contact with each other to collaborate.)

We publish a summary of each working group's members on the respective working group page on NVF's website. The summary includes the names, countries, and companies of the working group members. Contact details are not provided in the summary.

6. Data Transfer Outside the EU or EEA

Data is transferred outside the European Union or European Economic Area to the Faroe Islands. Data is disclosed to the NVF department of the Faroe Islands. The Faroe Islands are not a member of the EEA. Norway and Iceland are members of the EEA but not EU member states.

The European Commission has issued a decision on the adequacy of data protection in certain countries, including the Faroe Islands. Therefore, transferring data to the Faroe Islands does not require separate approval. Data subjects must still have a legal basis (such as consent) for the transfer.

7. Principles of Register Protection

The register is handled with care, and information processed through data systems is protected appropriately. Measures are taken to ensure the security of register information.

The data controller ensures that stored information, server access rights, and other critical data relevant to the security of personal data are handled confidentially and only by personnel who require such access.

8. Obligation to Provide Information

As a practical requirement for membership in NVF, participants must provide their contact information (work email address and work phone number) so that members can communicate with each other and so that the secretariat can communicate with members.

If contact information is not provided, membership in NVF will be terminated.

9. Data Subject Rights

According to the General Data Protection Regulation (GDPR), you have the following rights regarding the processing of your personal data. If you wish to exercise your rights, please contact us using the contact details provided in section 1.

Your rights:

- You have the right to receive clear and understandable information about the processing of your personal data.

- You have the right to obtain confirmation as to whether your personal data is being processed or not, and if so, the right to obtain a copy of this data.
- You have the right to request the correction of inaccurate or incomplete personal data.
- In certain situations, you have the right to request the erasure of your personal data before the general data retention period.
- In certain situations, you have the right to request the restriction of the processing of your personal data. If you have the right to restrict processing, we may in the future only process your data – except for storage – with your consent or for the establishment, exercise, or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.
- In certain situations, you have the right to object to the processing of your personal data. You may also object to the use of your data for direct marketing purposes.
- You have the right to receive your personal data concerning you in a structured, commonly used, and machine-readable format and have the right to transmit those data to another controller without hindrance.

You also have the right to withdraw your consent at any time. If you wish to withdraw your consent, please contact us using the contact details provided in section 1. If you withdraw your consent, this will not affect the lawfulness of the processing based on your consent before its withdrawal. Your withdrawal will only take effect from the time of withdrawal.

Additionally, you have the right to lodge a complaint with a supervisory authority if you believe that the processing of your personal data violates applicable data protection regulations. In Finland, the supervisory authority is the Office of the Data Protection Ombudsman (www.tietosuoja.fi); Office of the Data Protection Ombudsman, P.O. Box 800, 000521 Helsinki).