PRIVACY NOTICE FOR THE WHISTLEBLOWING REPORTING CHANNEL REGISTER OF EPV ENERGIA OY

1. Data Controller

   EPV Energia Oy ("Data Controller")
   Business ID: 0216734-9
   Visiting and postal address: Kirkkopuistikko 0, FI-65100 Vaasa, Finland
   Telephone: +358 10 505 5000
   Website: www.epv.fi

2. Name of the Register:

   EPV Energia Oy Whistleblowing Reporting Channel Register

3. Person Responsible for the Register

   Person responsible for the whistleblowing register: Maija Suutarinen

   If you have any questions concerning the processing of your personal data under this privacy notice or wish to exercise your data subject rights, you may submit your request in writing to the contact person named above.

4. Data Protection Officer

   EPV Energia Oy has appointed a joint Data Protection Officer:
   Data Protection Officer, EPV Energia Oy
   Email: tietosuoja@epv.fi
   The Data Protection Officer monitors compliance with data protection legislation at EPV Energia Oy and provides information and guidance on data protection obligations.

5. Purpose and Legal Basis for Processing Personal Data

   The Data Controller collects and processes personal data for the purpose of

investigating reported misconduct or suspected misconduct concerning the personnel of the Data Controller or the personnel of its contractual suppliers and subcontractors.

The legal basis for processing personal data depends on the nature of the report. For reports falling within the scope of the Finnish Whistleblower Protection Act (1171/2022), the processing is based on the Data Controller's legal obligation (GDPR Article 6(1)(c)).

Processing of reports related to other ethical principles or internal organizational guidelines is based on the Data Controller's legitimate interest (GDPR Article 6(1)(f)).

Categories of Personal Data Processed

- Name and contact details of the reporting person. Reports may also be submitted anonymously.
- Information contained in the report, such as the person or persons concerned, their contact details, and a description of the suspected violation or misconduct.
- Names and possible contact details of witnesses or other persons related to the matter.
- Information revealed or collected during the internal investigation concerning the subject matter of the report or the persons involved.
- Information related to the handling of the report and communications used in the investigation.
- Information concerning persons handling the report, such as name, job title, contact details, and system log data.

6. Regular Sources of Data

The primary source of personal data processed in connection with the whistleblowing procedure is the whistleblowing reporting channel and the reports submitted through it.

During the handling of a report, the information may be supplemented with personal data necessary for the purposes of processing, obtained from other sources, such as the Data Controller's internal registers or systems, or from hearings of the parties involved and other persons connected to the events.

7. Retention of Personal Data

   Personal data will generally be erased within five (5) years after the conclusion of measures related to the suspected misconduct. Data related to clearly unfounded reports will be erased without delay after the processing has ended.

8. Disclosure and Transfer of Personal Data

   As a rule, the Data Controller does not disclose personal data in this register to another data controller. Where necessary, personal data may be disclosed to authorities or, if further investigation of an anonymous report requires it and personal data has been provided in the report, to designated parties within the organization responsible for the investigation.

9. Transfer of Data Outside the European Union or the European Economic Area

   Personal data contained in this register will not be transferred outside the European Union (EU) or the European Economic Area (EEA). If such transfers were to occur, they would be agreed upon separately and appropriate contractual safeguards would be applied.

10. Automated Decision-Making

    The data in this register is not used for automated decision-making.

11. Principles of Data Protection

    Access to personal data is restricted to individuals who, based on their job responsibilities, have a legitimate need to process the data.

    Personal data is protected by generally accepted and reasonable technical and organizational measures, such as access control, staff training, firewalls, and user access management.

    The use of personal data in digital form is restricted by access rights and protected during processing by technical measures such as encryption and other information security controls.

12. Rights of the Data Subject

    Your rights and options regarding personal data depend on the specific situation

and the purpose of processing. You have the following rights, subject to statutory limitations:

- The right to access your personal data and to request rectification of inaccurate data, and in certain situations, erasure of data.
- The right to request correction of data and, in certain situations, restriction of processing or to object to processing.
- The right to erasure of data (the right to be forgotten).
- The right to restrict processing.
- The right to object to processing.

Please note that not all data subject rights are absolute.

13. Restrictions on Data Subject Rights in Whistleblowing Matters

The exercise of data subject rights may be restricted in whistleblowing cases if exercising those rights would compromise the protection of the whistleblower's identity, the investigation of the matter, or the examination of the alleged violation.

More information about your rights is available at:
https://www.epv.fi/tietosuojailmoitus/
When implementing data subject rights under data protection legislation, any restrictions imposed by other applicable legislation are also taken into account.

You may exercise your rights by contacting the register contact person referred to above. You may also contact the Data Protection Officer regarding questions related to the processing of your personal data.

Please note that the Data Controller may request additional information necessary to process your request and must verify your identity. If you do not provide the necessary additional information or cannot be identified, the Data Controller has the right to refuse to process your request.

Otherwise, the Data Controller will respond to your request within the timeframe and in the manner required by applicable legislation.

If a data subject considers that their statutory rights have been violated, they may contact the supervisory authority. The contact details of the Finnish data protection authority are available at Privacy notice - EPV

14. Amendments to This Privacy Notice

The Data Controller continuously develops its operations and therefore reserves the right to amend this privacy notice by publishing updates on its website. Amendments may also be based on changes in legislation. Data subjects are encouraged to review the content of this privacy notice regularly.

Updated: 29 April 2026