Whistleblowing Privacy Policy

Updated 29 August 2024

This Whistleblowing Privacy Policy applies to the joint internal whistleblowing channel between Meriaura Group Oyj, Meriaura Oy, Meriaura Energy Oy and Rasol Oy (hereafter "Meriaura") and the collection and processing of personal data.

Data Controller	Meriaura Group Oyj Business ID 2309682-6 Linnankatu 88, 20100 Turku, Finland Tel.: +358 10 271 0810 Meriaura Ltd Business ID 0669579–8 Linnankatu 88, 20100 Turku, Finland Tel.: +358 2 211 1600 Meriaura Energy Oy Business ID 3355280-5 Insinöörinkatu 7, 50150 Mikkeli, Finland Tel.: +358 10 271 0810 Rasol Oy Business ID 3016363-6 Hiekkamäentie 25 B, 01150 Sipoo, Finland Puh. + 358 50 523 8358
Data protection contact	Meriaura Group Oyj [●] Meriaura Ltd Jessica Troberg , jessica.troberg@meriaura.fi Tel. +358 40 584 0381 Eerikinkatu 26, 20100 Turku Meriaura Energy Oy [●] Rasol Oy [●]
Data Protection Officer contact	Meriaura Ltd Jessica Troberg, Jessica.troberg@meriaura.fi Tel.: +358 40 584 0381 Eerikinkatu 26, 20100 Turku, Finland [●]

Purpose and legal basis for processing personal data

Maintaining an internal whistleblowing channel is predicated on the Whistleblowing Directive (EU 2019/1937) of the European Parliament and Council to protect people who report about breaches of Union law and on national whistleblower protection legislation (Whistleblower Protection Act 1171/2022).

The purpose of the whistleblowing channel is to ensure compliance with the European Union and national legislation referred to in Section 2 of the Whistleblower Protection Act.

Processing third-party personal data, such as that of the object of the whistleblowing, is based on the Data Controller's statutory obligation to process such data. Processing the whistleblower's personal data is based on consent.

Personal data categories and data content

Whistleblowing notifications may be made via the whistleblowing channel only. Contacts concerning notifications will also be made via the whistleblowing channel only.

Meriaura employees who have, in their work or in connection with it, witnessed or received information about a breach of law in the branches, which are specified in the Whistleblowing Protection Act and are punishable by law, and which may result in a punitive administrative ramification, or may seriously jeopardize the public interest objectives in the legislation.

When making notifications in the whistleblowing channel, whistleblowers indicate whether their notification concerns Meriaura Group Oyj, Meriaura Oy or Meriaura Energy Oy.

The instructions for making notifications state that whistleblowers do not need to provide their personal data. They can make a notification anonymously in which case their personal data will not be processed. If a whisltblower wishes to provide their personal data, the whistleblowing channel has fields for entering name and telephone number.

The notification may contain the personal data of other people, such as the person who is the object of the whistleblowing and other people involved in the situation (e.g., witnesses).

The notification may also contain sensitive personal data (e.g., a person's health condition), criminal offences or misdemeanours, if the whistleblower has included this data in the explanation of an unlawful act. The Data Controller will process this data only if necessary for the purposes of the Whistleblowing Protection Act.

The personal data contained in notifications may be used in resolving the issue.

Normal sources of data

Data are collected from the notifications made in the whistleblowing channel.

Retaining period for personal data

Personal data are deleted after one year of receiving a notification, unless there is a compelling reason for retaining them for a longer time.

Personal data, which are unnecessary for processing a notification, are deleted without undue delay.

The Data Controller deletes or destroys the personal data after their processing is no longer necessary.

Personal data processors

Only those people, who have been designated by the Data Controller, are permitted to process the personal data of the whistleblower, the object of the whistleblowing and any other people mentioned in the notification. The designated person's rights are limited to notifications concerning the company in question.

The identity of the whistleblower, if provided in the notification is not disclosed to the person against whom allegations are made. The whistleblower's identity may be disclosed only with their permission or if it is needed for criminal proceedings.

Personal data are disclosed to third parties, e.g., authorities or third-party investigators, within the limits permitted and required by the applicable legislation. This may include requests for the data by authorities or when required by the Data Controller's legal obligation or legitimate interest, e.g., to file an offence report, conduct a preliminary investigation or in court proceedings.

We use a service offered and maintained by the Chamber of Commerce as the internal whistleblowing channel. The Chamber of Commerce employees do not have access to the notifications in the channel.

Transferring data outside the EU and EEA

Personal data are not relinquished or transferred
outside the European Union or the European Economic Area.

Registry protection

Notifications are stored in a protected format.

Only the notification processors designated by the Data Controller receive information about notifications and have access to process them. Each processor uses their unique personal ID to sign in to the system and process notifications.

The notifications and the related data are archived in a protected format. The designated notification processors have access to the archived data.

Data subjects' rights and limitations thereof

Right of access

The data subject's right of access to their personal data, as per Article 15 of the General Data Protection Regulation (GDPR), may be limited in respect of personal data reported under the Whistleblowing Protection Act if limiting access is necessary and appropriate to safeguard investigation of the validity of the notification or to protect the identity of the whistleblower.

If only some data is restricted from a data subject, they have the right to access their non-restricted personal data. The data subject has the right to know the reasons for the restrictions and request they be given to the Data Protection Ombudsman as per Section 34, Paragraphs 3 and 4 of the Data Protection Act (1050/2018).

The request for access to the data are to be made to the contact person mentioned in this document. When a data subject exercises their right to access their data, the Data Controller sends them a copy of the personal data which has been processed. If a data subject wishes to have multiple copies, the Data Controller may charge a reasonable fee to cover administrative costs.

Right of rectification and erasure

The right to rectify or erase inaccurate, incomplete, unnecessary or outdated data, which are intended for processing in the register, applies to non-restricted access data. The request for rectification or erasure of data is to be made to the contact person mentioned in this document.

Right to object to data processing

The data subject does not have the right to object to the processing of their personal data.

Right to restrict processing

The data subject does not have the right to restrict the processing of their personal data.

Right to withdraw consent

The data subject has the right to withdraw their consent if the data processing is based on consent.

Right to receive notification of a data protection breach

The data subject has the right to know about any data protection breaches regarding their personal data.

Right to appeal

The data subject has the right to make an appeal to the Office of the Data Protection Ombudsman, if they feel their personal data have been processed contrary to the EU's General Data Protection Regulation.

Data Protection Ombudsman:
Office of the Data Protection Ombudsman
Street address: Lintulahdenkuja 4, 00530 Helsinki
Postal address: PL 800, 00531 Helsinki
Exchange: +358 29 566 6700
tietosuoja@om.fi

Amendments to this document

This document may be updated occasionally if changes occur in Meriaura's data protection practices or in the applicable legislation.