Privacy Policy for Whistleblowing Channel

1. Controller

Uponor Corporation (“Uponor”)
Äyritie 20
01511 Vantaa
Finland
Telephone: +358 20 129 211

2. Contact Person

Annamari Ahlmark
Äyritie 20
01511 Vantaa
Finland
Telephone: +358201292072
E-mail: annamari.ahlmark@uponor.com

3. Group of Data Subjects

Data subjects (e.g. customers, sub-contractors, employees of Uponor Group companies and any other persons related to Uponor in any way) whose personal data is submitted to the whistleblowing channel by the employees of Uponor Group companies, persons providing services to Uponor Group companies, and any other stakeholders who have reported via the channel (“Person(s)”).

4. Purpose and Legal Basis of Processing Personal Data

The purpose of this personal data register is to enable employees of Uponor Group companies and any other persons related to Uponor in any way (“Whistleblower”) to report on a suspicion of misconduct within Uponor Group companies and to investigate such reports.

Processing of personal data is necessary for compliance with a legal obligation under securities legislation to which Uponor is subject. Uponor may also process personal data based on its legitimate interests to prevent irregularities, fraud, non-compliance and misconduct within the Uponor Group companies.

Uponor retains personal data as long as the data is required for the aforementioned purpose, or as required by applicable laws. If the report turns out to be unsubstantiated, the personal data will be deleted without delay.

5. Content of the Personal Data Register

This personal data register contains personal data submitted by Whistleblowers or otherwise collected in the course of investigating the report.

6. Regular Sources of Information

The data is collected from the Whistleblowers and Persons. In addition, personal data may be, as allowed by applicable legislation, collected from other sources than directly from the data subject, e.g. from Uponor's customers, subcontractors or service providers.

7. Disclosure and Transfer of Personal Data Outside the EU/EEA Area

Personal data may be disclosed to employees of Uponor Group companies and/or third parties for investigation purposes on a strict need to know basis.

Uponor may disclose and transfer personal data outside EU/EEA in accordance with and subject to the limitations imposed by applicable legislation as follows:

- to companies belonging to the Uponor Group in accordance with a contract entered into between the relevant Uponor entities, incorporating the European Commission's Standard Contractual Clauses, which ensure that adequate data protection arrangements are in place as well as to authorized third parties to the extent they participate in the processing of personal data for the purposes stated in this personal data register. The personal data may be processed by such authorized third parties also outside EU or EEA in accordance with a contract entered into between Uponor and such authorized third party, incorporating the European Commission's Standard Contractual Clauses or other appropriate transfer mechanisms that provide an adequate level of data protection, as approved in the Data Protection Regulation. Uponor shall oblige such third parties to keep confidential and adequately secure any such transferred personal data; or
- based on consent; or
- as otherwise permitted by applicable legislation.

For technical reasons and for reasons related to the use of data, the personal data may be stored on servers of external service providers who may process the data on behalf of Uponor.

Any transfers of personal data shall be made in accordance with the General Data Protection Regulation (2016/679) and any applicable mandatory legislation, as may be amended from time to time.

8. Rights of Data Subjects

Unless any limitations apply, each data subject has the right to access all personal data Uponor has on him/her. Each data subject also has the right to request that Uponor corrects, erases or stops using any erroneous, unnecessary, incomplete or obsolete personal data. Each data subject may also withdraw any consent previously provided by him/her.

However, during the investigation Uponor may, at its sole discretion, 1) limit Persons' access to personal data for the purpose of securing the ongoing investigation; and/or 2) choose not to notify the Persons of the personal data processing for the purpose of securing the ongoing investigation.

Any requests should be sent to the contact person mentioned in Section 2 above. Uponor processes all requests as soon as possible. If dissatisfied with the decision or actions of Uponor, each data subject has the right to lodge a complaint with his/her country's data protection authority.

9. Principles of Securing Personal Data – Technical and Organisational Controls

Uponor shall ensure that sufficient technical and organisational personal data protection measures are implemented and maintained throughout its own organisation. Further, Uponor shall ensure that any transfer or disclosure of personal data described in this personal data register to any third party is subject to Uponor having ensured an adequate level of data protection by agreements or by other means required by law.

Technical controls:

Physical material is stored in locked spaces with restricted access. Any IT systems are secured by means of the operating system's protection software. Access to the systems requires entering a username and a password and data transfers happen via high encryption channels. Further information on the technical measures of the whistleblowing channel, please see: https://whistleb.com/trustcentre.

Organisational Controls:

Within the organisation of the controller, the use of the personal data is instructed, and access to IT systems including personal data is limited to such persons who are entitled to access them on the basis of their work assignments or role and who are subject to confidentiality obligations regarding the personal data. Reports are processed by Uponor's Compliance Committee consisting of Group CFO, General Counsel and Compliance Officer.