Privacy Policy – Uponor Whistleblowing Channel
Updated 12.6.2023

1. Controller

Uponor Corporation ("Uponor")
Ilmalantori 4, 00240 Helsinki, Finland
Telephone: +358 20 129 211

2. Contact Person

Erika Nylund
Legal Counsel & Group Compliance Officer
Ilmalantori 4, 00240 Helsinki, Finland
E-mail: erika.nylund@uponor.com
Telephone: +358 20 129 2326

3. Purpose and Legal Basis for Processing Personal Data

The Whistleblowing Channel of Uponor Group provides an opportunity to report suspicions of misconduct in Uponor operations – for example a violation of Uponor Code of Conduct, breach of law or anything not in line with Uponor values. The Whistleblowing Channel is also used for reporting any violations of European Union law or European Union member state national laws under the scope of the Whistleblowing Directive (*Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law*) and national legislation implementing the Whistleblowing Directive.

Personal data will be processed in connection with the Whistleblowing Channel when the messages/notifications/reports ("Reports") are being submitted via the Whistleblowing Channel. Reports submitted via the Whistleblowing Channel provide Uponor the opportunity to address, handle and investigate the concerns raised in the Reports. The personal data will only be processed for handling the Reports and reacting on the possible wrongdoings.

The legal basis for collecting and processing personal data is either the mandatory legal obligation of Uponor Group under the Whistleblowing Directive and national legislation implementing the Whistleblowing Directive **or** the legitimate interest of Uponor Group, depending on the content of the Reports. The legitimate interest of Uponor is based on Uponor's 1) obligation to ensure compliance with applicable legislation, 2) efforts to prevent irregularities, fraud, non-compliance and misconduct within Uponor and 3) maintaining of stakeholder relationship between Uponor and Data Subjects.

4. Data Subjects and Personal Data Processed

Uponor may receive personal data when handling Reports submitted via the Whistleblowing Channel, or otherwise collected in the course of handling such Reports. Data Subjects may include persons submitting the Reports and persons whose suspected misconduct is described in the Reports,

e.g. employees of Uponor Group companies, representatives of Uponor suppliers, customers, sub-contractors or other persons related to Uponor in any way. The Report may be submitted anonymously but it is possible for the person submitting the Report to include their contact details.

The personal data processed for the purposes defined in this privacy policy may include for example first and last name, language, contact details (e.g. email, phone number), role and job title, gender and details on the reported misconduct.

Uponor does not intend to process any special categories of personal data, and if such personal data is included in the Reports or is disclosed to Uponor during the further handling of the Reports and related investigations, such personal data will be only processed in accordance with applicable legislation or if necessary, under the scope of Whistleblowing Directive or national legislation implementing the Whistleblowing Directive.

5. Regular Sources of Information

The personal data is collected via the Whistleblowing Channel when a person submits a Report and further in connection with handling of the Report, for example in an internal investigation. Further individuals may be contacted for additional details and the accuracy of personal data may be checked, if persons are identifiable from the Report. If necessary in handling the Report, the personal data may be collected from other sources than directly from the data subject as allowed by applicable legislation, e.g. from Uponor's customers, subcontractors or service providers.

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

Uponor does not disclose personal data to unauthorised third parties. Uponor may disclose personal data to employees of Uponor Group companies, authorities or other third parties on a strict need to know basis if required by the handling of the Report or applicable legislation.

Uponor uses an external service provider in providing the Whistleblowing Channel. The service provider and its subcontractors act as data processors of Uponor and the personal data will be processed by such service providers only for the provision of services to Uponor and on behalf of Uponor.

Uponor may process personal data in jurisdictions where it has presence and therefore the personal data may be processed within EU/EEA and outside EU/EEA. Uponor will only transfer personal data outside the EU/EEA in accordance with and subject to the limitations imposed by applicable legislation. 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, 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 adequate data protection arrangements are in place
- Authorised third parties: Data transfers to authorised third parties are allowed to the extent such third parties participate in the processing of personal data for the purposes stated in this privacy policy. Any transfers are allowed only by incorporating the European Commission's

Standard Contractual Clauses or other appropriate safeguards for data transfers as listed in the EU General Data Protection Regulation, which ensure that adequate data protection arrangements are in place

- The recipient country is regarded by the European Commission to provide adequate protection for personal data;
- based on consent given by the data subject; 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.

7. The Storing and Retention of Personal Data

Uponor retains personal data submitted via the Whistleblowing Channel and processed in connection with purposes defined in this Privacy Policy only as long as necessary and justified based on applicable legislation. The personal data clearly unnecessary for handling the Report will be deleted without delay. For Reports under the scope of Whistleblowing Directive or national law implementing the Whistleblowing Directive, Reports are stored for a maximum of five years from receiving the Report, if not otherwise required by applicable laws to protect Uponor's rights or obligations, or to prepare, present or defend legal claims.

8. Rights of the Data Subjects

Unless any limitations apply, the data subject has the right to access all personal data Uponor has concerning the data subject. Each data subject also has the right to request that Uponor corrects, deletes or discontinues the use of any erroneous, unnecessary, incomplete or obsolete personal data.

The rights above may be exercised via a form on Uponor website or by contacting the 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 their country's data protection authority.

Please note that the data subject's rights may be restricted if the processing of personal data is necessary for an ongoing investigation on misconduct or for Uponor's legal obligations under the Whistleblowing Directive, national law implementing the Whistleblowing Directive, or other applicable legislation.

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

The reports received via the Whistleblowing Channel are strictly confidential and handled with care. The access rights to personal data are restricted to personnel whose duties include handling reports submitted via the Whistleblowing Channel, mainly meaning Uponor Compliance Committee and/or local specifically assigned persons.

Uponor shall ensure that sufficient technical and organisational personal data protection measures are implemented and maintained throughout its own organisation. In addition, Uponor shall ensure

that any transfer or disclosure of personal data described in this privacy policy 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/trust-centre/.

Organisational Controls:

Uponor Corporation and the technical implementation provider Navex Global, Inc have instructed their organisations on the processing of personal data. Within Uponor, the access to IT systems containing personal data is limited to persons entitled to access based on their work assignments or role and who are subject to confidentiality obligations regarding the personal data. Reports are mainly handled by Uponor's Compliance Committee consisting of Group Chief Financial Officer, Chief Legal Officer and Group Compliance Officer or by specifically assigned Uponor personnel in Uponor local group companies.