Uponor Job Applicant Privacy Statement – UK & Ireland

1. Controller of Personal Data

Uponor (with regard to job applicants applying a position in Uponor Limited)
The Pavilion
Blackmoor Lane
Watford WD18 8GA
UK
+44 (0)1923 381212

In parallel with

Uponor Corporation
Ilmalantori 4
00240 Helsinki
Finland

Uponor Corporation and Uponor Limited hereinafter together “Uponor”.

2. Contact Information

Kavita Lad
The Pavilion
Blackmoor Lane
Watford WD18 8GA
UK
TEL: 01923 381212
E-mail: Kavita.lad@uponor.com

In case you wish to make a request relating to your personal data, please use the forms available at https://www.uponorgroup.com/en-en/legal-information/data-protection and on the local Uponor websites.

3. Group of Data Subjects

Persons participating in recruitment processes at Uponor in UK & Ireland.

4. Purpose and Legal Basis of Processing Personal Data

The purpose of job applicant personal data processing is the management of Uponor’s employee recruitment processes including the processing of job applicant personal data. In case the job applicant has applied through a web portal service provided by a third party, the privacy policies of such third party service providers shall apply. The processing described above may include processing and evaluating the personal data in order

to fill vacant positions and to inform the job applicants of the outcome of the recruitment process. The processing may also include sifting of job applicants by automated tools (based on search words).

Uponor has legitimate interest to process the personal data for the abovementioned purposes.

The job applicant personal data may be stored after the end of the recruitment process as long as Uponor need it for the performance of their obligations related to the recruitment process or in future recruitments, however not longer than 6 months.

5. Content of the Personal Data processing

Uponor may process especially the following job applicant information:

- Basic information, such as: name, date of birth, e-mail address, telephone number, home address, position;
- Qualification data, such as: education, work experience, permissions and permits, diplomas, certificates, CV's, application letters, language skills;
- Compensation data: salary request;
- Photo (if uploaded by the job applicant);
- References and basic information on the referee (such as name, title, e-mail address, telephone number);
- Links to personal profiles, e.g. in social media applications such as LinkedIn (if uploaded by the job applicant);
- Videos recorded during possible video interviews; and
- Assessment data: evaluation and comments made by Uponor Group's recruiting personnel.

6. Regular Sources of Data

The data is primarily collected from each data subject him/herself. As allowed by applicable legislation, personal data may, in some situations, be collected from other sources than directly from the data subject, e.g. from Uponor's subcontractors or service providers.

Uponor informs each data subject of the data processing, including of any third party data sources and data collected from such sources, in accordance with applicable legislation.

The data is entered into the personal data database by the data subject, Uponor Group's Human Resources personnel and the recruiting manager during the recruitment process.

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

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 privacy statement. 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 safeguards for data transfers as listed in the EU General Data Protection Regulation (GDPR), which ensure that adequate data protection arrangements are in place. 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 amended.

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, and object to all direct marketing.

Any requests should be sent via the request forms available at https://www.uponor.com/en-gb/legal-information/data-protection. 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 Organizational Controls

Uponor shall ensure that sufficient technical and organizational personal data protection measures are implemented and maintained throughout its own organization. Further, Uponor shall ensure that any transfer

or disclosure of personal data described in this privacy statement 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.

Organizational controls:

Within the organization 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.