Employees and Applicants

Last change on Apr. 20, 2026

We would like to inform you which personal data we as a corporate group will process as part of the application procedure and during an employment relationship, i.e. if you are hired. In each case, the company for whose position you have applied is responsible.

1. Name and Contact Details of the Controller

SupplyOn GmbH
Ludwigstrasse 49
85399 Hallbergmoos
Telephone: +49 811 99997 0
E-Mail: datenschutz@supplyon.com

Please note: The former Newtron GmbH merged with SupplyOn GmbH in 2026. SupplyOn GmbH will therefore be responsible for processing within the Newtron brand from now on.

EURO-LOG AG
Am Söldnermoos 17
85399 Hallbergmoos
Telephone: +49 811 9595-0
E-Mail: info@eurolog.com

2. Contact Details for the Controller's Data Protection Officer

Data Protection Officer for SupplyOn is
datenschutz süd GmbH
Wörthstraße 15
97082 Würzburg
Telephone: +49 931 304976 0
E-Mail: datenschutz@supplyon.com

Data Protection Officer for EURO-LOG is
Johannes Gabler
Am Söldnermoos 17
85399 Hallbergmoos

Telephone: +49 811 9595-0
E-Mail: datenschutz@eurolog.com

3. Purposes of Processing & Legal Basis

A) During the Application Process

When we receive your application, we process personal data required for Staffing. This may include contact data, any data related to the application (CV, certificates, qualifications, answers to questions, etc.) and, if applicable, bank details (to reimburse travel expenses). The legal basis for this processing is Art. 6 para. lit. b GDPR.

We process the data that you provide us with in your online application exclusively for the purpose of selecting applicants. Data processing for other purposes does not take place. You yourself determine the scope of the data you wish to transfer to us in the context of your online application. If certain information is required due to a specific job description, we will point this out. Online applications are transferred electronically to our personnel department (to the responsible recruiter) and processed there as quickly as possible. The transmission is encrypted. As a rule, applications are forwarded to the heads of the responsible departments in our company.

Due to our affiliation as a group of companies, it is possible that the responsible recruiter will inform the personnel department of an affiliated company about your application, especially if the position for which you originally applied is already filled but another position within our group of companies might be of interest to you. The possibility of forwarding your application to the affiliated company is indicated in the respective job advertisement. The legal basis for forwarding your application documents is Art. 6 para. 1 lit. f GDPR. Our legitimate interest here lies in the fact that we can offer you other positions than those for which you have applied. You have the opportunity to object to this data processing at any time within the limits of Art. 21 GDPR. Your data will not be passed on beyond this.

Your data will be treated confidentially. If your application is unsuccessful, your documents will be deleted after six months. In the event that we may also consider your application for other or future job advertisements, please make a corresponding note on your application. We will then process your data on the basis of Art. 6 para. 1 lit. a GDPR.

B) During Employment

We may collect master data from you which is necessary for the employment relationship: Name, address, date of birth, gender, bank details, nationality.

We may also collect and store information about your employment with us, your qualifications and your career to date. This includes, for example, information regarding your highest level of education or vocational training and the information you provided as part of the application process. Data concerning current second jobs is relevant for us in order to enable us to check

compatibility with your employment.

We may also collect tax and social security relevant data. This includes, among other things, your tax identification number, tax class, child allowances, marital status and information concerning your religious denomination (only if relevant under tax law). We collect this and other data, as regulated by § 39e of the German Income Tax Act, directly from the responsible tax authorities.

We may also collect information on taxable pre-employment periods in the current calendar year so that the tax calculation may be adjusted accordingly. We may also collect information about your health insurance and, if applicable, other employment-related supplementary insurances in order to be able to meet any payment and reporting obligations.

When calculating social security contributions, we ask about your parental status. We need this information in order to determine whether a contribution surcharge for long-term care insurance must be paid in accordance with § 55 para. 3 Social XI. If applicable, we may ask you to prove your existing parental status by submitting appropriate documents. In this case, we will only include a note on the examination of the parental status in your personal file and return or destroy the documents.

If your activity is characterized by a special position of trust, we may ask you to provide us with management credentials.

If you are not yet of legal age at the time of recruitment, we may ask you to submit a medical certificate of initial examination. We are legally obliged to do this in accordance with §32 of the Youth Employment Protection Act.

In certain cases, we ask you to present a work permit or a residence permit. This occurs only if it is necessary to verify the legality of your employment.

We will also ask if you have a severe disability. This question enables us to safeguard your rights under Social Code Book IX and to calculate any compensatory contribution in accordance with § 77 Social Code Book IX. This question must only be answered once you have been with the company for six months. During your first six months of employment answering this question is voluntary.

During the employment relationship, we collect and process further personal data, including information on sick leave, absences (vacation, special leave, etc.) and working hours. Here, too, the principle applies that such data is only collected and processed if it is necessary for the employment relationship in accordance with Art. 6 para. 1 b GDPR or if it is legitimized by other legal provisions.

We maintain a personnel file in which we store all central information required for the employment relationship. If you would like to view the contents of your personnel file, please contact the human resources department.

As an employee of SupplyOn, we process your personal data in connection with the use of

SupplyOn-Services for the purpose of the employment relationship on the legal basis of Art. 6 para. 1 lit. b GDPR. Further relevant information on the use of SupplyOn-Services can be found under “Information regarding data protection for users of SupplyOn-Services”.

We process your personal data in connection with the use of electronic signatures for internal approval and documentation processes on the legal basis of Art. 6 para. 1 lit. f GDPR. Your personal data processed in connection with a signature (name and signature) is processed when you, as a manager, initiate the relevant approval process.

4. Recipients of Data and Involvement of Service Providers Located Outside the EU/EEA

A) During the Application Process

Your data will be treated confidentially and will not be passed on to third parties. If necessary, we use service providers who are strictly bound by our instructions, who support us in the areas such as IT or the archiving and destruction of documents, and with whom separate contracts for commissioned data processing have been concluded.

B) During Employment

Your data will be treated confidentially. We only transmit data to third parties if this is absolutely necessary and there is a legal basis to do so, for instance to:

Banks and tax specialists for the calculation and payment of wages and salaries, Social insurance agencies and fiscal authorities to comply with our legal obligations. We may also pass your data on to service providers who support us in areas such as IT or archiving and destruction of data and with whom separate contracts for commissioned data processing have been concluded.

Furthermore, in individual cases there may be additional legal obligations for the transmission of data, which only arise in individual cases.

Additionally, we refer you to an excerpt from the data protection inter-company agreement of the SupplyOn GmbH.

C) Microsoft Teams

We use Microsoft Teams as part of our work.

Microsoft Teams is used for work-related communication via online meetings. When you participate in an online meeting, audio and video signals are transmitted to the other conference participants in encrypted form. You are free to use the chat, question, or survey functions during the online meeting. Before entering the conference room, you can enter your name and choose whether to enter with your camera or microphone on or off.

If we wish to record online meetings, we will inform you of this in advance and ask for your consent (Art. 6 para. 1 lit. a GDPR). When a video recording starts, all meeting participants will receive a system notification in which they can consent to the recording. Consent is only valid for the respective meeting, is always voluntary, and refusal or withdrawal of consent does not have any negative consequences. The recordings are used for information, training, or documentation purposes, e.g., for employees or external parties.

In addition to video recording, there is a function that automatically transcribes a meeting in order to document meetings, to make work easier, or for colleagues who were unable to attend. If the transcription function is activated in meetings, we will inform you of this in advance and ask for your consent (Art. 6 para. 1 lit. a GDPR). Consent applies only to the respective meeting, is always voluntary, and refusal or withdrawal of consent does not entail any negative consequences. **The transcription is created with the help of artificial intelligence.**

The transcription uses speech recognition to record all contributions to the meeting and summarizes them in a transcript. For this purpose, your voice will be temporarily recorded and deleted shortly after the end of the meeting. Microsoft does not have access to the audio recordings. After the meeting has ended, the meeting host will have access to the minutes and can control access to them by the other meeting participants.

Of course, we have ensured that an appropriate level of data protection is in place. Microsoft is certified under the EU-U.S. Data Privacy Framework and standard contractual clauses are in place where necessary.

5. Criteria for the Erasure of Data

A) During the Application Process

If no legal retention period exists, data will be deleted as soon as storage is no longer necessary or the legitimate interest for storage has expired. If you are not hired, your application will normally be deleted no later than three months after the end of the application proceedings.

In individual cases, individual data may be stored for a longer period of time (e.g. travel expense accounting). The duration of the storage then depends on legal retention obligations, for example from the Tax Code (6 years) or the Commercial Code (10 years).

If you are not hired, but your application is still of interest to us, we will ask you if we may retain your application for future vacancies.

B) During Employment

All data collected by us will be destroyed or deleted as soon as they are no longer required for the employment relationship or the employment relationship has been terminated and legal retention periods have expired.

6. Existing Rights: Information, Rectification, Erasure, Restriction, Objection, Data Portability, Complaint to a Supervisory Authority

Data subjects have the right to be informed by the controller about the personal data concerning them and to have incorrect data corrected or deleted, if one of the reasons stated in Art. 17 GDPR applies, e.g. if the data is no longer required for the purposes pursued. You have also the right to limit the processing if one of the conditions mentioned in Art. 18 GDPR is present and in the cases of Art. 20 GDPR the right to transfer data. If data is collected on the basis of Art. 6 para. 1 lit. e (data processing for the fulfillment of official tasks or the protection of the public interest) or lit. f (data processing to pursue legitimate interests), the data subject has the right to object to the processing at any time for reasons arising from his/her particular situation. We will then no longer process the personal data unless there are verifiable compelling grounds for processing worthy of protection which outweigh the interests, rights and freedoms of the data subject, or the processing serves to assert, exercise or defend a legal claim.

Furthermore, any data subject shall have the right to complain to a supervisory authority if he or she considers that the processing of data concerning him or her is in breach of data protection provisions. In particular, the right of appeal may be exercised before a supervisory authority in the Member State in which the data subject is residing or in which the alleged infringement took place. The competent supervisory authority for SupplyOn is the Bayerisches Landesamt für Datenschutzaufsicht, Promenade 27 (Schloss), 91522 Ansbach, Germany.

7. Consequences of Not Providing Personal Data

The disclosure of your personal data is not required by law and you are not contracted to provide it, but it is necessary for the conclusion of an employment contract.

As an applicant or employee of SupplyOn, you are not obliged to provide your personal data. The consequence of not providing your personal data would be that it could impede the conclusion of an employment contract with you.