# TRILUX DIGITAL SERVICES

# ANNEX CONCERNING DATA PROCESSING

This annex specifies the data protection obligations of the parties that arise from the General Terms and Conditions of TRILUX Digital Services and the associated performance specification, see www.trilux.com/AGB. They apply to all activities connected therewith and with regard to which staff of TRILUX (hereinafter referred to as "TRILUX" or "Contractor") or representatives authorized by TRILUX process personal data or may come into contact with the personal data of the principal (hereinafter “Customer”).

## 1. Subject matter and duration of the Agreement

1.1. TRILUX processes personal data on behalf of the Customer. This includes all activities provided by TRILUX pursuant to the performance specification and the TRILUX Digital Services GTC vis-à-vis the Customer and which represent data processing

1.2. The services are provided exclusively in a member state of the European Union or in a contracting state of the Treaty on the European Economic Area. Each relocation of the service or parts thereof to a third country require the Customer’s prior consent and may occur only if the special prerequisites of Art. 44 et seqq. GDPR have been met.

1.3. Processing is carried out for an unlimited period of time, unless contractually specified otherwise.

1.4. The Customer is authorized to terminate the agreement at any time without notice if a serious infringement of data protection provisions or the provisions of this agreement exists on the side of TRILUX, TRILUX cannot or will not execute an instruction issued by the Customer, or TRILUX refuse the Customer’s monitoring rights in violation of the agreement. Nonfulfillment of the obligations specified in this agreement and derived from Art. 28 GDPR represent a serious infringement.

## 2. Nature and purpose of processing, type of personal data, and categories of data subjects

2.1. The nature of processing includes all types of processing in terms of Art. 4 No. 2 GDPR.

2.2. The purposes of processing are all contractual purposes necessary for the provision of the contractually negotiated services and all other contractual purposes negotiated in Sections 12 and 13 of this Data Processing Agreement and the performance specification.

2.3. TRILUX processes the following data from the luminaires in case of energy monitoring: energy consumption, operating time and service life, switching status on/off, variable DALI indicators, and serial numbers of the TRILUX luminaires used by the Customer, information concerning the rooms in which the luminaires are installed. TRILUX also processes the following data in case of light monitoring: dimming level, errors from the DALI ballast units, and LiveLink light management system, temperature in the ballast unit in the luminaire.

2.4. Data subjects might be staff and periodically active staff of third-party providers insofar as floor plan and space utilization in conjunction with the TRILUX digital services allow conclusions concerning identifiable persons and/or their usage behavior with regard to TRILUX luminaires.

## 3. Notes on remote maintenance:

3.1. If the Contractor carries out the maintenance and/or servicing of the IT systems by means of remote maintenance, the Contractor is obliged to enable the Customer to effectively control the remote maintenance work. This can be done, for example, by using technology which enables the Customer to follow the work carried out by the Contractor on a monitor or similar device.

3.2. In the event that the Customer is subject to a duty of professional secrecy within the meaning of Section 203 of the German Penal Code (StGB), the Customer shall ensure that no unauthorised disclosure within the meaning of Section 203 of the German Penal Code occurs as a result of the remote maintenance. In this respect, the Contractor is obliged to use technologies that not only enable the activity to be followed on the screen, but also provide the Customer with a possibility to stop the remote maintenance work at any time.

3.3. If the Customer does not wish to observe the activities on a monitor or similar device during remote maintenance work, the Customer will not use this technology. If the Contractor does not wish to observe the activities on a monitor or similar device during remote maintenance work, the Contractor shall document the work carried out by him in a suitable manner.

3.4. If data was stored at the Contractor's premises in the course of the maintenance, it shall be carefully deleted again after completion of the work.

## 4. Customer’s rights and duties, instructional authority

4.1. Only the Customer is responsible for assessing the permissibility of processing pursuant to Art. 6 (1) GDPR as well as for safeguarding the rights of the data subjects pursuant to Art. 12 through 22 GDPR ("Controller" in terms of Art.4 No.7 GDPR). Nevertheless, TRILUX is obligated to immediately forward all inquiries to the Customer insofar as such are discernibly addressed exclusively to the Customer.

4.2. If necessary, the Customer will disclose to TRILUX the contact person for data protection matters arising within the scope of this Data Processing Agreement.

4.3. Modifications of the subject matter of processing and process modifications must be coordinated jointly between the parties and must be specified in writing or in a documented electronic format. The Customer shall generally place all orders, partial orders, and issue instructions in writing or in a documented electronic format. Oral instructions must be confirmed immediately in writing or in a documented electronic format.

4.4. The Customer prior to start of processing and periodically thereafter is authorized, in a reasonable manner, to ensure compliance with the technical and organizational measures taken by TRILUX as well as the duties specified in this agreement. The Customer shall immediately inform TRILUX if it discovers errors or irregularities in an audit of the processing results.

## 5. Customer's representatives with authorization to instruct, TRILUX's instruction recipients

The Customer's representatives with authorization to instruct, TRILUX's instruction recipients and the communication channels to be utilized for instructions are negotiated separately between the parties. In case of a change or long-term non-availability of the contact persons, the contractual partner must immediately be informed of the successors or representatives in writing or electronically. Instructions must be retained for their validity period and subsequently for another 3 full calendar years.

## 6. TRILUX's duties

6.1. TRILUX processes personal data exclusively as agreed with and as instructed by the Customer, unless TRILUX is obligated to other processing based on applicable legal provisions (e.g. investigations by prosecution or state security authorities); in such a case, TRILUX shall inform the Customer of these legal requirements prior to processing, insofar as such a notification is not prohibited based on substantial public interest.

6.2. TRILUX shall not use the personal data submitted for processing for any other purposes, in particular not for its own purposes. No copies or duplicates of the personal data is generated without the Customer's knowledge.

6.3. Within the scope of contractual processing of personal data, TRILUX assures contractual handling of all agreed measures.

6.4. TRILUX is obligated to participate to the necessary extend in the Customer's fulfillment of the data subject's rights pursuant to Art. 12 through 22 GDPR and in the creation of directories of processing activities, and reasonably support the Customer insofar as possible.

6.5. TRILUX shall immediately notify the Customer if TRILUX is of the opinion that issued instructions violate statutory provisions. TRILUX is authorized to suspend execution of the relevant instruction until, after review, such are confirmed or modified by the Customer's Controller.

6.6. TRILUX is obligated to rectify, erase, or restrict processing of personal data under the contractual relationship if the Customer requests this in an instruction and such is not opposed by TRILUX's legitimate interests. TRILUX is authorized to provide information concerning personal data under

6.7. the contractual relationship to third parties or the data subject only after the Customer's prior instruction or consent.

6.8. TRILUX declares its consent that the Customer to reasonable and necessary extend and generally after scheduling an appointment is itself, or through third parties commissioned by the Customer, authorized to monitor compliance with the data protection and security regulations as well as the contractual provisions. This may in particular take place by obtaining information and viewing the stored data and data processing programs as well as auditing and inspections on site, insofar as TRILUX's work and organizational processes are not affected thereby. TRILUX will support such monitoring.

6.9. TRILUX assures that it has familiarized the staff employed for the performance of work with the relevant data protection provisions prior to such staff commencing work and that they have also been suitably obligated to maintain confidentiality for the duration of their activity as well as after the end of the employment. TRILUX monitors compliance with the data protection regulations in its operation.

6.10. The data protection officer at TRILUX is SAFE-PORT Consulting GmbH, Hülshoff-Straße 7, D-59469 Ense | Data protection | privacy@trilux.com. The Customer must immediately be informed of a change of the data protection officer.

## 7. TRILUX's reporting obligations in case of processing errors and breaches of the protection of personal data

TRILUX shall immediately inform the Customer of any errors, violations of data protection regulations or the specifications outlined in the order, as well as of the suspicion of data protection violations or irregularities in the processing of personal data. This applies in particular also in light of the Customer's possible reporting and notification obligations. TRILUX assures that it will reasonably support the Customer, if necessary, in its duties pursuant to Art. 33 and 34 GDPR. TRILUX may file reports pursuant to Art. 33 or 34 GDPR for the Customer only after prior instruction.

## 8. Sub-contractual relations with subcontractors/additional processors

8.1. The Customer grants to TRILUX the general permission to utilize additional processors in accordance with Art. 28 GDPR.

8.2. TRILUX shall inform the Customer of an intended change with regards to using or replacing additional processors. An objection against the intended change must be raised vis-à-vis TRILUX within 4 weeks after receipt of the information concerning the change. In the event of an objection, TRILUX at its own choice is authorized to provide the service without the intended change or insofar as provision of the service is unreasonable for TRILUX without the intended change terminate the service affected by the change vis-à-vis the Customer within 4 weeks after receipt of the objection.

8.3. In the event that TRILUX awards orders to additional processors, it is incumbent upon TRILUX to also transfer its data protection obligations under this agreement to the additional processor. The agreement with the subcontractor must be in writing or in an electronic format.

8.4. An up-to-date list of the subcontractors/additional processors awarded can be viewed at www.trilux.com/AGB.

## 9. Technical and organizational measures pursuant to Art. 32 GDPR (Art. 28 (3) Clause 2 c) GDPR)

9.1. The respective current applicable technical and organizational measures are available to the Customer under www.trilux.com/AGB.

9.2. A level of protection appropriate to the risk to the rights and freedoms of the natural persons affected by processing is assured for the specific data processing. In this regard, the privacy objectives of Art. 32 (1) GDPR, e.g. confidentiality, integrity, and availability of the systems and services as well as their resilience in terms of nature, scope, circumstances, and purpose of processing is taken into consideration in a manner that suitable technical and organizational measures permanently limit potential risks.

9.3. The Customer, prior to concluding the Data Processing Agreement and thereafter periodically, shall obtain information concerning these technical and organizational measures. The Customer shall be responsible for the fact that the respective currently applicable and contractually negotiated technical and organizational measures offer an appropriate level of protection with regard to the risks of the data to be processed. TRILUX reserves the right to change the adopted technical and organizational measures insofar as such do not fall below the level of protection pursuant to GDPR and the agreed standards.

## 10. TRILUX's obligations after the end of the order

10.1. After completion of the contractual services, TRILUX shall erase or destroy all personal data, records, and processing or utilization results that were created in connection with the contractual relationship, which are in its possession or in the possession of subcontractors.

10.2. The erasure or destruction shall be confirmed by TRILUX, including the date, in writing or in a documented electronic format.

## 11. Mutual support

In case of Art. 82 GDPR, the parties are obligated to support each other and to participate in clarifying the underlying facts.

## 12. Agreement of additional contractual purposes

12.1. TRILUX is authorized to process the personal data covered by this agreement

a) for rectification in the provided service in which the data is stored,

b) for the purpose of quality assurance for the provided service or for a newer version of the service,

c) for the purpose of developing new or for the purpose of further developing existing TRILUX services in a reasonably secure environment.

12.2. TRILUX is authorized to process the personal data covered by this Agreement

a) insofar as this is absolutely necessary and appropriate to assure network and information security,

b) insofar as this assures the ability of a network or information system to fend off, with a reasonable level of reliability, errors or unlawful or deliberate interferences that affect the availability, authenticity, accuracy, and confidentiality of stored or transmitted personal data as well as the security of services connected therewith that are offered or accessible through these network or information systems.

12.3. This includes in particular also preventing the access of unauthorized parties to electronic communication networks and the distribution of harmful program codes and to fend off attacks in the

12.4. form of the targeted overloading of servers (“denial of service attacks”) and harming of computer and electronic communication systems.