Self-disclosure on technical and organisational measures for commissioned processing | Status: 20.10.2021

According to the provisions of the EU General Data Protection Regulation (Art. 28 GDPR), the client must check before the start of data processing whether suitable technical and organisational measures to protect the confidentiality, integrity, availability, resilience and recoverability of the data have been set up at the contractor and are being complied with. The result of this check shall be documented. To simplify this verification, the following self-disclosure is provided. For quick readability and a transparent presentation of the measures, the self-disclosure is designed as a checklist. Individual measures support several data protection objectives of the GDPR. In order to avoid repetition, the measures are therefore structured according to their objectives. Overall, the measures cover the data protection objectives of the GDPR.

The questions relate only to employees and systems, procedures and facilities entrusted with or used for the performance of the commissioned services or processing operations.

In order to be able to provide secure commissioned processing that complies with data protection requirements, the technical and organisational measures described below have been set up.

Request	Fulfilled		Comment / Explanation
	Y	N	
1. general information			
Has a data protection officer been appointed?	☑	☐	Thorsten Schröers SAFE-PORT Consulting GmbH datenschutz@trilux.com | privacy@safe-port.de
Does the data protection officer undergo - regular training?	☑	☐	IHK Arnsberg / Sauerland ITKservice GmbH IQ-Zert GmbH & Co KG
What other position(s) does the data protection officer hold in addition to this task?			No further activity, as external data protection officer
Are employees obliged to maintain confidentiality in accordance with the provisions of the GDPR?	☑	☐	All employees of the TRILUX Group are obliged to maintain confidentiality and to observe data protection in accordance with the GDPR and BDSG.
Is the commitment verifiably documented?	☑	☐	In writing in the personnel file
Are employees continuously instructed in the requirements of data protection, if applicable how?	☑	☐	Type of instruction ☑ Online training ☑ Written instructions ☑ Regular team meetings
Is there a deletion concept with a regulation of the retention or storage periods and for the timely and secure deletion or destruction of the data?	☑	☐	
Is there a systematic data protection and data security management with a regulated procedure for review and evaluation?	☑	☐	

Request	Fulfilled		Comment / Explanation
	Y	N	
Is there a certification for IT security or IT security management or any other certificate on a legally compliant implementation of data protection in the company?	☑	☐	The data processing takes place in a data centre of a cloud provider based in the EU. This is certified according to DIN EN/ISO IEC 2700x and is subject to a regular inspection routine.
Is there a data protection concept or a data protection manual to regulate and implement data protection in the company?	☑	☐	
Is there an IT security manual or are there other regulations for the technical and organisational measures for data protection?	☑	☐	
Are subcontractors used?	☒	☐	
If applicable, are the same obligations imposed on subcontractors as those established between the contracting authority and the contractor?	☑	☐	
Do the necessary data protection agreements or obligations also exist with maintenance and other service providers, and if so, what kind?	☑	☐	All service providers are obliged in writing to comply with the current data protection laws.
Is the data processing carried out on the territory of the Federal Republic of Germany or within the European Union or the states of the European Economic Area?	☑	☐	

Request	Fulfilled		Comment / Explanation
	Y	N	
2. technical and organisational measures			
2.1 Confidentiality (Art. 32 para. 1 lit. b GDPR)			
2.1.1 Access to the company			
Are the premises and buildings secured against unauthorised access outside operating hours?	☑	☐	☑ Security guards ☑ Motion detector/alarm system ☑ Access control system ☑ Central locking system, security locks
Are entrances and exits secured?	☑	☐	Building entrance doors ☑ Yes☐ No Escape doors/emergency exits ☑ Yes☐ No☐ Not applicable Fire escapes and stairs ☑ Yes☐ No☐ Not applicable Delivery and delivery areas ☑ Yes☐ No☐ Not applicable
Is the guidance and supervision of visitors regulated?	☑	☐	☑ Reception ☑ Visitor book ☑ Visitor badge ☑ Personal visitor guidance
Is outside personnel, e.g. maintenance and service personnel, supervised?	☑	☐	Maintenance and service personnel are supervised at all times by a member of staff responsible for the relevant area.

Request	Fulfilled		Comment / Explanation
	Y	N	
Are access controls in place?	☑	☐	☑ Access control system ☑ with ☐ without security zones ☑ Central locking system with key control Access authorisations are only granted to an employee if this has been requested by the respective supervisor and/or the HR department. The principle of necessity is taken into account when issuing authorisations.
Are security areas defined, e.g. server room, PBX, archives, network distributors and separately protected against unauthorised access?	☑	☐	
Are these security areas specially protected against unauthorised access, if so how?	☑	☐	Type of protection ☑ Access control system ☑ Central locking system with Key regulation
Are the access authorisations to these security areas regulated and documented in an access authorisation concept?	☑	☐	Key allocation and key management is carried out according to a defined process that regulates the granting or withdrawal of access authorisations for rooms both at the beginning of an employment relationship and at the end of an employment relationship.
Are there any other protective measures in place for these rooms?	☑	☐	☑ Porter ☑ Alarm system ☑ Company card

Request	Fulfilled		Comment / Explanation
	Y	N	
2.1.2 Access to the data processing systems			
Are measures in place to control access to the desktop and networked systems?	☑	☐	Secure user ID ☑ Secure password Password repeat☑ lock after 3 failed attempts To gain access to IT systems, users must have the appropriate access authorisation. For this purpose, corresponding user authorisations are - issued by administrators. However, this is only done if requested by the respective supervisor. The request can also be made via the HR department.
Are there password rules for all access levels (network, server, applications) to ensure a secure and confidential password?	☑	☐	The user receives a user name and an initial password, which must be changed the first time the user logs in. The password specifications include a minimum password length of 8 characters, whereby the password must pass the complexity requirements.
Is compliance with these rules checked automatically at all levels during entry?	☑	☐	Passwords are changed regularly. An automatic password change is indicated. A password history is stored. This ensures that the past 10 passwords cannot be used again. Passwords are always stored in encrypted form.
Is a time-controlled password-protected - pause circuit (screen saver) set up?	☑	☐	

Request	Fulfilled		Comment / Explanation
	Y	N	
Are the systems protected against unauthorised intrusion and against the internet?	☑	☐	☑ Firewall ☑ Virus scanner ☑ Mains separation All server and client systems are equipped with virus protection software that guarantees a daily supply of signature updates. All servers are protected by firewalls that are always maintained and provided with updates and patches. The access of servers and clients to the Internet and the access to these systems via the Internet is also secured by firewalls. This also ensures that only the ports required for the respective communication can be used. All other ports are blocked accordingly.
Are logging/monitoring measures in place, if applicable which ones?	☑	☐	☑ Setting up users and rights ☑ System changes ☑ Faulty access attempts ☑ System monitoring ☑ Logging on and off to data processing procedures
Is the log data stored in an audit-proof and access-protected manner?	☑	☐	
Is the log data checked promptly and regularly for security-relevant actions and processes?	☑	☐	☑ Manual and occasion-related
Is access to the data processing systems - restricted by a rights system to the required group of users?	☑	☐	☐ Rights profiles and rights management ☐ Functional limitation of terminals Authorisations for IT systems and applications are set up exclusively by administrators.
Is access from external bodies made secure, if so how?	☑	☐	☑ VPN connection ☑ Encryption ☑ Special software for remote maintenance/remote support

Request	Fulfilled		Comment / Explanation
	Y	N	
2.1.3 Protection of data from unauthorised access			
Is there a documented authorisation profile that ensures that each employee only has the access authorisations they need to complete their tasks?	☑	☐	In what form? If necessary, also differentiated according to: ☑ Read authorisation ☑ Write permission Authorisations are always granted according to the need-to-know principle. Accordingly, only those persons are granted access rights to data, databases or applications who maintain and service these data, applications or databases or are involved in their development. There is a role-based authorisation concept with the possibility of differentiated allocation of access authorisations, which ensures that employees receive access rights to applications and data depending on their respective area of responsibility and, if necessary, on a project basis.
Are measures in place to limit storage, in particular pseudonymisation or anonymisation?	☑	☐	
Are the defined authorisations and their changes documented in a comprehensible way?	☑	☐	
Has a rights management system been set up for the documented allocation of rights, which also ensures that rights that are no longer required are cancelled promptly in the event of a change in the area of responsibility?	☑	☐	The prerequisite is a corresponding request for authorisation for an employee by a superior. A corresponding check-out process has been set up.
Are there any other access control measures, if applicable?	☑	☐	☑ Programme review and approval process ☑ Logging and evaluation of safety-critical incidents

Request	Fulfilled		Comment / Explanation
	Y	N	
2.2 Integrity (Art. 32 para. 1 lit. b GDPR)			
2.2.1 Protection of data during transmission and transfer			
Is the data protected from unauthorised access during transmission?	☑	☐	☑ Encryption ☑ Secure connections, VPN
Is secure deletion, destruction and disposal of data carriers guaranteed?	☑	☐	All staff are instructed to place information containing personal data and/or information about projects in the designated destruction bins.
Is the deletion/destruction of data carriers - contracted out to a service company?	☑	☐	The destruction of data carriers and paper is carried out by a service provider who guarantees destruction in accordance with DIN 66399.
Is there a contract/order for this in accordance with the requirements of Art. 28 GDPR?	☑	☐	
Is the secure and confidential decommissioning of devices with data carriers (e.g. servers, multifunctional devices, etc.) regulated?	☑	☐	
In the case of remote maintenance, is access to customer data and customer systems only via secure lines?	☑	☐	Securing the lines: ☑ VPN ☑encryption Remote access to IT systems always takes place via encrypted connections.
Is secure identification/authentication guaranteed for remote maintenance?	☑	☐	
In the case of remote maintenance, are the lines monitored by suitable safety devices, e.g. logging and log evaluation?	☑	☐	

Request	Fulfilled		Comment / Explanation
	Y	N	
2.2.2 Control of data entries			
Are the dial-in processes to customer systems logged and monitored in a traceable manner?	☑	☐	The entry, modification and deletion of personal data processed on behalf of the customer is always logged. Employees are obliged to work with their own accounts at all times. User accounts may not be shared or used jointly with other persons.
Are the use of data processing systems and the input of data logged?	☑	☐	Logging of file usage: ☑ Yes☐ No Logging of entries and changes: ☑ Data field-related ☑ Record-related
Are user authorisations with differentiated rights profiles set up?	☑	☐	Rights: ☑ Read, change, delete ☑ Partial access to data and functions
Has a procedure been set up for the comprehensible allocation of rights and for changing or cancelling rights?	☑	☐	Authorisations are always granted according to the need-to-know principle. Accordingly, only those persons are granted access rights to data, databases or applications who maintain and service these data, applications or databases or are involved in their development. The prerequisite is a corresponding request for authorisation for an employee by a superior. A corresponding check-out process has been set up.
Is the minimum principle observed when assigning rights?	☑	☐	
Are the rights allocation/authorisation and rights establishment bodies separate?	☑	☐	

Request	Fulfilled		Comment / Explanation
	Y	N	
2.2.3 Control of the processing operations			
Is the execution of the customer - order/service action monitored in a - traceable manner to ensure completion in - accordance with the order?	☑	☐	Corresponding regulations can be found in the contract for commissioned processing.
Are suitable logging and evaluation mechanisms in place to monitor unauthorised access to client systems and client data?	☑	☐	Corresponding regulations can be found in the contract for commissioned processing.
Are there regulations on the handling of incidents and on the fulfilment of reporting obligations to the client?	☑	☐	Corresponding regulations can be found in the contract for commissioned processing.
When awarding service contracts (e.g. IT service, maintenance, etc.), are the requirements of Art. 28 GDPR observed?	☑	☐	☑ Selection of the contractor ☑ Review of the technical and organisational measures at the contractor ☑ Conclusion of a contract pursuant to Art. 28 GDPR ☑ Regular review of the contractor
Are maintenance activities on commissioned processing systems reliably monitored and logged?	☑	☐	

Request	Fulfilled		Comment / Explanation
	Y	N	
2.3 Availability and resilience of the systems (Art. 32 (1) (b) GDPR)			
2.3.1 Ensuring the availability of the data			
Are customer data protected against destruction and loss by appropriate backup procedures?	☑	☐	☑ Mirrored data stock ☑ Regular backup copies/back-up solution Is there a backup concept that specifies the manner of a regular backup and the reconstruction of the data? ☑ Yes☐ No
Are measures in place to secure the server room and IT infrastructure?	☑	☐	The customer data is housed in a data centre certified according to DIN EN/ISO IEC 2700x.

Request	Fulfilled		Comment / Explanation
	Y	N	
2.3.2 Separation of different clients			
Are the data of the different clients appropriately separated from each other to ensure separate processing?	☑	☐	Type of separation: ☑ Client separation

Request	Fulfilled		Comment / Explanation
	Y	N	
2.4 Procedures for regular review, assessment and evaluation			
Is an IT security management system in operation?	☑	☐	The customer data is housed in a data centre certified according to DIN EN/ISO IEC 2700x.
Is the effectiveness of the technical and organisational measures in the company also regularly checked in another way?	☑	☐	Data protection management is implemented. There is a guideline on data protection and data security and guidelines to ensure the implementation of the guideline's objectives. A Data Protection and Information Security Team (DST) has been established to plan, implement, evaluate and make adjustments to data protection and data security measures. The guidelines are regularly evaluated and adapted with regard to their effectiveness. In particular, it is ensured that data protection incidents are recognised by all employees and reported immediately to the DST. The DST will investigate the incident immediately. If data processed on behalf of customers is affected, care shall be taken to ensure that they are informed immediately of the nature and scope of the incident. In the case of processing of data for own purposes, if the requirements of Art. 33 GDPR are met, a notification to the supervisory authority will be made within 72 hours of becoming aware of the incident.

Request	Fulfilled		Comment / Explanation
	Y	N	
2.5 Procedures for regular review, assessment and evaluation			
Are the requirements "data protection by technology" and "data protection-friendly - default settings" observed? ("Privacy by Design" and "Privacy by Default")	☑	☐	Already during the development of the software, care is taken to ensure that the principle of necessity is already taken into account in connection with user interfaces. For example, form fields and screen masks can be designed flexibly. Mandatory fields can be provided or fields can be deactivated. The software supports both input control through a flexible and customisable audit trail that - provides immutable storage of changes to data and user permissions. Authorisations on data or applications can be set flexibly and granularly.

Arnsberg | 20.10.2021

Place | Date

Signature