Technical and organizational measures of OneVision Software AG according to Art. 28 GDPR

12 - 2024

No.	Area	Description
0	**Organization**	
	How is the implementation of data protection organized?	Internal data protection officer, work instructions, regular training, technical and organizational measures, emergency plans
	Please provide us with the name and contact details of your data protection officer.	Jens Langer OneVision Software AG Ladehofstraße 50 93049 Regensburg Phone 0941-78004-0 Mail: Datenschutz@onevision.com
	What organizational measures have been taken to ensure that the processing of personal data complies with the law?	Appointment of a data protection officer, instructions, regular training, technical and organizational measures
	How do you ensure that internal processes are carried out in accordance with current data protection regulations and is this checked regularly?	Regular audits by the data protection officer
	In what form are the employees prepared for the implementation of the agreed technical and organizational measures that apply to this processing?	Training by the data protection officer, training by qualified in-house employees
	Are the processing operations documented with regard to data protection lawfulness?	Yes, in the processing directory

No.	Area	Description
1	**Confidentiality (Art. 32 para. 1 lit. b GDPR)**	
1.1	**Access control**	
	How are the buildings in which the processing takes place secured against unauthorized access?	Physical keys
No.	**Area**	**Description**
	How are the rooms/offices where the processing takes place secured against unauthorized access?	Only authorized employees have physical access to those rooms
	How are the processing systems protected against unauthorized access?	Rules for admission of external individuals, guidelines for accompanying external individuals in buildings.
1.2	**Access control**	
	How is user access assigned?	User authentication via standard process (LDAP), access concept
	How is the validity of user access checked?	Standard process (LDAP and local operating systems)
	How are user accesses documented, including applications, approval procedures, etc.?	Standard process (LDAP and local operating systems), database for new and joining, transferred and departed employees
	How is it ensured that the number of administration accesses is reduced to the necessary number only and that only professionally and personally suitable personnel are deployed for this purpose?	Standard process (LDAP and local operating systems), work instructions, access concept
	Is it possible to access the systems / applications from outside the company (home offices, service providers, etc.) and how is access organized?	Access exclusively via VPN or special applications. Control via firewalls and servers

No.	Area	Description
1.3	**Access control**	
	How do you ensure that passwords are only known to the respective user?	Standard process (LDAP and local operating systems), work instructions
	What requirements are placed on the complexity of passwords?	Character mix, at least 8 characters, password history
	How is it ensured that the user can / must change their password regularly?	Standard process (LDAP and local operating systems, group policy)
	What organizational precautions are taken to prevent unauthorized access to personal data in the workplace?	Access authorizations based on the operating system, logging, work instructions, trainings
	How is it ensured that access authorizations are assigned according to requirements and for a limited period of time?	Access authorizations based on the operating system
	How are access authorizations documented?	Standard process (LDAP and local operating systems in conjunction with access authorizations based on the operating system)
	How is it ensured that access authorizations are not misused?	Logging, instructions
	How long are logs kept? Who has access to the logs and how often are they analyzed?	No fixed deadlines, rotation of 6 months, mostly set system parameters. Only authorized employees (IT department and head of development) have access to the logs. The evaluations are carried out on a random basis and on request

No.	Area	Description
1.4	**Separation control**	
	How is it ensured that data collected for different purposes is processed separately?	Separate systems, work instructions, separate directories, client regulations
1.5	**Pseudonymization**	
	What organizational measures have been taken to ensure that the processing of personal data complies with the law?	All persons entrusted with the processing of personal data have been obligated accordingly. A data protection concept is used in the company and is made known to all employees. The training concept includes both data protection instructions at the start of work and constant sensitization through regular training and individual sensitization by the data protection officer. Attention has been drawn to the special features of handling pseudonymized data.
2	**Integrity (Art. 32 para. 1 lit. b GDPR)**	
2.1	**Transfer control**	
	How do you ensure the integrity and confidentiality of the transfer of personal data?	Depending on requirements (encryption, encrypted data line, registered mail if necessary, etc.)
	Are encryption systems used for the transfer of personal data and if so, which ones?	Yes, various (e.g. VPN, SSL, bilateral certificates, password-protected files, encrypted media, etc.)
	How is the transfer of personal data documented?	In compliance with legal requirements
	How is the unauthorized outflow of personal data restricted by technical measures?	Access control, technical and organizational measures
	Is there a control system that can detect an unauthorized outflow of personal data?	Logging, differentiated access authorizations

No.	Area	Description
2.2.	**Input control**	
	What measures are taken to be able to track who has accessed applications, when and for how long?	Logging
	How is it possible to track which activities have been carried out on the corresponding applications?	Logging, differentiated access authorizations
	What measures are taken to ensure that processing by employees can only be carried out in accordance with the client's instructions?	Logging, differentiated access authorizations, work instructions
	What measures are taken to ensure that subcontractors only process the client's personal data to the agreed extent?	Monitoring by the DPO, contract design, agreements on commissioned data processing
	How is the deletion/blocking of personal data ensured at the end of the retention period for subcontractors?	Monitoring by the DPO, contract design, agreements on commissioned data processing
3	**Availability and resilience**	
3.1.	**Availability control**	
	How is it ensured that the data carriers are protected against elementary influences (fire, water, electromagnetic radiation, etc.)?	Protected storage facilities and locations
	What protective measures are used to combat malware and how is it kept up to date?	Firewalls, virus scanners, filters, encryption programs, separate systems; regular and largely automated updates
	How is it ensured that data carriers that are no longer required or defective are disposed of properly?	Data protection and data security-compliant destruction of electronic data carriers

No.	Area	Description
3.2.	**Recoverability**	
	What organizational and technical measures are taken to ensure the availability of data and systems as quickly as possible even in the event of damage? (rapid recoverability in accordance with Art. 32 para. 1 lit. c GDPR)	Backups, replacement systems, emergency plans
4.	**Procedures for regular review, assessment and evaluation (Art. 32 (1) (d) GDPR, Art. 25 (1) GDPR)**	
	What procedures are in place for regular assessment/review to ensure the security of data processing (data protection management)?	The data protection officer regularly checks compliance with the technical and organizational measures, sometimes unannounced.
	How do you respond to requests or problems (incident response management)?	Use of a ticket system (based on OTRS) with two levels (1st and 2nd level); additional telephone hotline and automated monitoring and alerting (Icinga2 / Observium)
	What data protection-friendly default settings are there (Art. 25 (2) GDPR)?	No pre-checked check boxes; no boxes are pre-filled when logging into the system; user must enter the login credentials manually in each case
4.1	**Order control**	
	What processes are there for issuing instructions or dealing with commissioned data processing (data protection management)?	The contract was drawn up in accordance with the new guidelines on commissioned data processing. The data protection officer performs the corresponding advisory and monitoring duties.