- Annex 1 -

Technical and organisational measures for the protection of personal data according as defined in Articel 32 GDPR for the SaaS Application „contentDock®“

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, we have implement the following appropriate technical and organisational measures to ensure a level of security appropriate to the risk:

Access control § 64 Abs. 3 Nr. 1 BDSG (new) Measures to prevent unauthorized access to data processing equipment that processes or uses personal data.	
technical/constructional measures business address	**organisational measures**
• alarm system	• key control
• manual locking system with security locks	• logging of visitors
technical measures server-systems	
• Authentification with username and password	• Management of access / user permissions for the server access and the backend access of the application
• Differentiated access control through „Identity and Access Management“ for hosting	• Application of an internal password policy (incl. length)
• Use of Web Application Firewalls for hosting	• Passwords are created by the users themselves
• Use of VPN- and SSH-tunnels with key login for hosting administration	• Regular control of assigned authorisations
• Use of two-factor-authentification for hosting administration	• No access from visitors to internal networks
• Access to server systems via SSH with key login	
• Use of SSL certificates fort the encrypted connection to the application	
• Key Management Service for managing access and encrytion keys	
• Where technical possible: set timeouts	

Data media control § 64 Abs. 3 Nr. 2 BDSG (new) Measures to prevent unauthorized reading, copying, modification or deletion of data carriers	
technical measures	**organisational measures**
• Encryption of mobile data media	• Logging of the transfer of personal data to data media
• Pseudonymization of personal data	• Check of external media for malicious software
• Where technically possible: Authentication with username and password	• Unrecoverable deletion of data on data media prior to their reuse
	• Data protection compliant disposal of data media that are no longer needed

Storage control § 64 Abs. 3 Nr. 3 BDSG (new) Measures to prevent the unauthorized entry of personal data and the unauthorized viewing, modification and deletion of personal data	
technical measures	**organisational measures**
• Authentification with username and password	• Management of access / user permissions for the server access and the backend access of the application
• Use of VPN- and SSH-tunnels with key login for hosting administration	• Regular control of assigned authorisations
	• Rights assignment within the application / user account by the account administrator

Technical and organisational measures for the protection of personal data according as defined in Articel 32 GDPR for the SaaS Application „contentDock®“

User control § 64 Abs. 3 Nr. 4 BDSG (new) Measures to prevent the use of automated processing systems by means of unauthorized data transmission facilities	
technical measures	**organisational measures**
• Authentification with username and password	• Management of access / user permissions for the server access and the backend access of the application
• Differentiated access control through „Identity and Access Management“ for hosting	• Regular control of assigned authorisations
• Use of VPN- and SSH-tunnels with key login for hosting administration	• Application of an internal password policy (incl. length)
• Use of two-factor-authentification for hosting administration	
• Access to server systems via SSH with key login	
• Key Management Service for managing access and encrytion keys	

Access control § 64 Abs. 3 Nr. 5 BDSG (new) Measures to ensure that the persons entitled to use an automated processing system have access only to the personal data covered by their access authorization	
technical measures	**organisational measures**
• Authentification with username and password	• Management of access / user permissions for the server access and the backend access of the application
• Logging of access to the server as well as the application itself	• Regular control of assigned authorisations
	• Rights assignment within the application / user account by the account administrator
	• Routine testing and also event-related examination of the use of the IT systems

Communication control § 64 Abs. 3 Nr. 6 BDSG (new) Measures to ensure that it is possible to verify and establish to wich bodies personal data may be o have been transmitted using data communication equipment	
technical measures	**organisational measures**
• Authentification with username and password	• Documentation of the recipients of data and the period of the planned release or agreed deletion periods
• Logging of accesses and deliveries of data	• Documentation of the interfaces and the request / transmission programs
	• Event-related plausibility, completeness and correctness checks

Input control § 64 Abs. 3 Nr. 7 BDSG (new) Measures to ensure that it is possible to verify and establish wich personal data has been input or change into automated processing systems by whom and when	
technical measures	**organisational measures**
• Authentification with username and password	• Documentation with which applications which data can be entered, changed and deleted
• Loggin of input, change and delete of data	• Traceability of input, modification and deletion of data by individual user names (Login)
	• Assignment of rights to enter, change and delete data within the application/user account by the account administrator

Technical and organisational measures for the protection of personal data according as defined in Articel 32 GDPR **for the SaaS Application „contentDock®“**

Transport control § 64 Abs. 3 Nr. 8 BDSG (neu) Measures to ensure that the confidentiality and integrity of the data is protected (can not be read, copied, changed or deleted without authorization) when transmitting personal data or transporting data media	
technical measures	**organisational measures**
• Data encryption by HTTPS	
• additional: Encryption of request / response data via AES encryption between server system and the mobile apps	
• Encrypted connection via SSH for hosting administration	
The measures under data media control and communication control also apply!	

Recoverability § 64 Abs. 3 Nr. 9 BDSG (new) Measures to ensure that systems in use can be restored in case of failure	
technical measures	**organisational measures**
• Regular Backups	• Backup & Recovery Concept
• automated scripts for creating server instances	• Regular data recovery testing according to backup / recovery concept
• Planned: multi data center operation	

Reliabillity § 64 Abs. 3 Nr. 10 BDSG (new) Measures to ensure that all functions of the system are available and any malfunctions that occur are reported werden	
technical measures	**organisational measures**
• Logging & evaluation of log files	• Constant monitoring of the hosting systems
• Monitoring of all hosting systems	
• Alarm management in case of errors	
• regular system and security updates	
• Evaluation of all security rules in the web application firewall	

Data integrity § 64 Abs. 3 Nr. 11 BDSG (new) Measures to ensure that stored personal data are not damaged by malfunction of the system	
technical measures	**organisational measures**
• Strict separation of development, testing and production system	

Order control § 64 Abs. 3 Nr. 12 BDSG (new) Measures to ensure that personal data processed on behalf of the customer can only be processed in accordance with the instructions of the client	
technical measures	**organisational measures**
	• Careful selection of processors
	• Written contracts with the processor in accordance with Art. § 28 GDPR
	• Carrying out of controls and obtain evidence (eg certificates)

Technical and organisational measures for the protection of personal data according as defined in Articel 32 GDPR **for the SaaS Application „contentDock®“**

Availability control § 64 Abs. 3 Nr. 13 BDSG (new) Measures to ensure that personal data are protected against destruction or loss	
technical measures	**organisational measures**
• Monitoring of all hosting systems	• Backup & Recovery Concept
• Backups of databases and files	• Regular data recovery testing according to backup / recovery concept
• Scalability of all server instances	
• Replicability of virtual server instances	
• regular system and security updates	
• Planned: multi data center operation	

Separability § 64 Abs. 3 Nr. 14 BDSG (new) Maßnahmen die gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden	
technical measures	**organisational measures**
• Client capability	• Database and file management concept
• Logical client separation	• Definition of database rights
• Strict separation of development, testing and production system	• Micro-services concept
• Database systems and file management systems are stored separately	• Routine testing and also event-related examination of the use of the IT systems
• Splitting system functions into micro-services	

Loading capacity control Measures to ensure that the data-processing equipment is sufficiently robust to remain functional even in the event of high-load and faults	
technical measures	**organisational measures**
• Load-Balancing	• Regular load tests of the systems
• Automated 24/7 monitoring of all hosting systems	• Penetration tests
• Alarm management when an adjustable load limit is reached	• Scaliing conzept
• regular system and security updates	• Limit of load of the data processing systems in advance above the necessary minimum

Procedures for periodic review and evaluation of the effectiveness of the measures taken	
technical measures	**organisational measures**
	• Internal Privacy Policy
	• Commitment of employees to data secrecy
	• Documentation / overview of processing activities
	• Regular load test of the systems
	• exercise of agreed control rights arising from written contracts with the processor