Controls	Selection	Reason
Access Control **denial of unauthorised access to processing facilities with which processing is carried out**		
Is there a dedicated server room for processing personal data?	yes	There is a server room at the ONTEC site, as well as a locked rack in a dedicated data center.
Is the server room locked?	yes	Both mechanical and biometric.
Is access to the server room logged?	yes	Access is logged at both locations
Does a list of authorized persons exist?	yes	For both locations.
Is this list checked regularly and in special cases for up-to-dateness?	yes	In the course of the user authorization process
Are mobile devices (laptop, mobile phone, tablet, etc.) safely stored if they are unattended?	yes	
Does a documented guideline exist for this purpose?	yes	Contained in "ONTEC IT Terms of Use"
Are office rooms locked when the last employee leaves the building	yes	Contained in "ONTEC IT Terms of Use"
Medium Control **Prevent unauthorized reading, copying, modifying or removing of data carriers**		
Is there a policy for the safe handling of data carriers?	yes	Contained in "ONTEC IT Terms of Use"
Are personal data stored exclusively on dedicated data carriers (server or client)?	yes	Conatined in Data processing directory
Does a documented guideline exist for this purpose?	yes	Contained in "ONTEC IT Terms of Use"
Are data carriers safely disposed of after they are discarded?	yes	Encrypted or securely disposed
User Control **Prevention of unauthorized use of automated processing systems by means of data transmission devices**		

Can only authorized persons access personal data	yes	Contained in "ONTEC IT Terms of Use"
Does a documented guideline exist for this purpose?	yes	In the course of the user authorization process
Are user rights checked regularly, documented and, if necessary, adjusted?	yes	In the course of the user authorization process
Access Control **ensuring that those entitled to use an automated processing system have access only to personal data subject to their right of access**		
Can users only access data for which there is a need and authorization due to their activity?	yes	Technically regulated
Does a documented guideline exist for this purpose?	yes	In the course of the user authorization process
Does a documented guideline exist for the management of passwords?	yes	Technically regulated
Is there a logged access monitoring	yes	Technically regulated
Transmission Control **ensuring that it can be verified and determined where personal data has been or may be transferred or made available by means of data transmission facilities**		
Is there a documented regulation on how personal data must be transferred to other entitled parties (including third parties)?	yes	Contained in "ONTEC IT Terms of Use"
Is personal data only transmitted in encrypted form?	no	Only where required by contract.
Is personal data also transmitted using transportable data carriers?	no	Contained in "ONTEC IT Terms of Use"

Input Control **Ensuring that it can be subsequently verified and determined what personal data has been entered into automated processing systems at what time and by whom**		
Does a documented guideline exist for event logging?	no	Event logging is performed, but there is no dedicated control.
Is it possible to subsequently determine which user accessed personal data at which time and from which location	yes	
Are event logs for systems and applications kept safe from manipulation and unauthorized access for at least 3 months?	yes	Except firewall log files: less than 3 months
Is there a separate event logging for privileged users (admins, remote maintenance users - third parties, etc.)?	yes	
Transport Control **Prevention of unauthorised reading, copying, altering or deleting of data during the transmission of personal data and the transport of data carriers**		
Does a documented guideline exist for handling mobile data carriers?	yes	Contained in "ONTEC IT Terms of Use"
Are USB sticks, smart phones, tablets, external hard drives, memory cards, etc. used for the transport or storage of personal data?	no	Exception: contact data in encrypted container.
Are these data carriers only allowed to be transported by persons designated for this purpose?	n.a.	
It is ensured that no personal data is stored on the data carriers of devices being repaired	yes	no devices with personal data will be passed on to third parties
Is it ensured that there is a confidentiality agreement regarding personal data between sender and recipient and, if applicable, third parties?	yes	

Remediation **Ensuring that the systems can be restored in the event of a malfunction**		
Does a data backup and recovery concept exist?	yes	Backup
Is there an archiving concept ?	yes	Only where required by contract.
Are regular data backups carried out?	yes	
Can data that has been lost or changed incorrectly or intentionally be restored promptly?	yes	
Are all specified service agreements (SLAs) fulfilled?	yes	
Are there regular functional tests for the recovery of data	yes	
Are all legal and contractual requirements regarding the retention period fulfilled?	yes	
Data Integrity **Ensure that all functions of the system are available, that malfunctions are reported (reliability) and that stored personal data cannot be damaged by malfunctions of the system.**		
Is there a process for Business Continuity Management (BCM)?	yes	Continuity Management Prozess
Is there a process for Change-Management Process	yes	Change Management Prozess
Is there a process that ensures that especially security-relevant updates are implemented promptly?	yes	Security Incident Prozess
Is there adequate, state-of-the-art protection against malware?	yes	Virenscanner, Firewall, etc.
Is there adequate, state-of-the-art protection against external attackers (hackers)?	yes	Firewall

Is there a regulation which ensures that, within the framework of economic possibilities and the state of the art, appropriate protective measures are identified and implemented in a timely manner?	yes	Security Incident Prozess
Personal security **Ensure that only qualified, dedicated and reliable persons are granted access to personal data**		
Is there a documented recruitment process that specifies the exact requirements?	yes	Screening policy und terms and conditions of employment
Is there a regulation that ensures that only suitable and reliable contractors are used?	yes	where relevant for the processing of personal data (e.g. Data Center)
Ensuring that user rights are adjusted in the event of changes during employment, maternity leave or the employment relationship	yes	In the course of the user authorization process
It is ensured that the respective user authorizations are promptly and documented withdrawn upon termination of the employment or order relationship.	yes	In the course of the user authorization process
Ensuring that there is a valid and appropriate confidentiality or non-disclosure agreement with all employees and relevant contractors	yes	In the employment contract or with suppliers where relevant for the processing of personal data (e.g. data processing centre)