


Document Name Information Security Guidelines for contractors			
Document types system 03 Guidelines / Directives			
Version Version 1, 01.03.2020	Valid from 01.03.2020	Classification Public	Page 1/17

Information Security Guidelines for contractors



Document Name Information Security Guidelines for contractors			
Document types system 03 Guidelines / Directives			
Version Version 1, 01.03.2020	Valid from 01.03.2020	Classification Public	Page 2/17

Table of content

Table of content	2
1 Introduction and scope	3
1.1 Introduction.....	3
1.2 Scope	3
2 Maintaining confidentiality of information/business/company secrets	3
3 Types of cooperation	3
4 Requirements for contractors to maintain information security	5
4.1 Basic principles	5
4.2 Organising the security of information.....	5
4.3 Privacy by design (only relevant for personal related data).....	6
4.4 Privacy by default	6
4.5 Controlling access.....	6
4.6 Cryptography and / or pseudonymisation.....	7
4.7 protection of buildings	7
4.8 Protecting operating equipment / information data	7
4.9 Operating procedures and responsibilities	7
4.10 Data backup.....	8
4.11 Protection against malware by managing weaknesses and patches.....	8
4.12 Protocolling and monitoring.....	8
4.13 Network security management.....	8
4.14 Information transfer	9
4.15 Network separation.....	9
4.16 Obtaining, developing and maintaining systems.....	9
4.17 Relationships with suppliers.....	9
4.18 Managing information security incidents.....	10
4.19 Information security aspects of business continuity management/emergency management.....	10
4.20 Compliance with legal and contractual requirements	10
4.21 Data protection requirements and data protection management	10
4.22 Information security checks	11
5 Contractor’s duty to inform	11
6 Review of the implementation of security measures	11
7 Annex Security measures depending on the form of cooperation	12

Document Name Information Security Guidelines for contractors			
Document types system 03 Guidelines / Directives			
Version Version 1, 01.03.2020	Valid from 01.03.2020	Classification Public	Page 3/17

1 Introduction and scope

1.1 Introduction

This guideline defines the rules for handling information and the use of information technology which suppliers, contractors and service providers (hereinafter referred to as contractors) to Montaplast of North America –(hereinafter referred to as Montaplast) - must adhere to. The purpose of this guideline is to protect the confidentiality, integrity and availability of information, as well as the rights and interests of the customer, as well as all persons (natural and legal in definition) entering into a business relationship with and / or carrying out activities for Montaplast.

1.2 Scope

This directive is addressed to the management of the contractor, their employees and agents.

Contractors are defined as third parties, who provide services for the Montaplast on the basis of contractual relations.


2 Maintaining confidentiality of information/business/company secrets

- (1) The contractor and his subcontractors are obliged to use the access/access rights (IT systems, services, data and applications) granted by the customer exclusively within the scope of their obligations to fulfil the contract.
- (2) All information acquired during the fulfilment of the order that is not publicly known, including copies, records and work results created as a result of the order are the property of the customer and shall be returned to the customer upon completion of the order.
- (3) The Contractor and its subcontractors are obligated to treat as confidential all information pertaining to the Customer, the business and operational affairs of the Customer and all work results collated during the execution of the contract, and are obligated to protect such information appropriately against unauthorized and non-contractual use, reproduction or disclosure. These obligations shall apply beyond the termination of the contractual relationship.
- (4) The contractor is not permitted to acquire business or operational information of any kind not made public pertaining to the customer and/or his customers, suppliers or employees, for personal use or to make copies or records of any kind, unless necessary for the fulfilment of the order. Such information, copies, recordings or work results may not be passed on to third parties or brought to the attention of third parties.
- (5) Confidential information may only be passed on to subcontractors for whom the client has given his consent and who have been obligated to comply with these security guidelines.
- (6) The Contractor may only employ personnel at the Customer's premises who are bound to data secrecy, information security and, if applicable, to other secrets. These obligations shall continue to exist even after termination of the activity.

3 Forms of cooperation

The use of external partners is primarily characterized by the fact that external persons are contracted to support work or business processes as well as the operation of applications and systems of the company.

There are many reasons to give external partners access to company data or company systems. For example, some companies need access for maintenance, service or testing purposes, other companies need to

Document Name Information Security Guidelines for contractors			
Document types system 03 Guidelines / Directives			
Version Version 1, 01.03.2020	Valid from 01.03.2020	Classification Public	Page 4/17


"operate" systems on behalf of the company. Complete services can also be outsourced to external partners, for example, in the context of outsourcing or cloud computing.

Fundamentally, every external company access to Montaplast company data, or the outsourced processing of data, is a potential risk for misuse. For example, there is the risk that the access rights associated with an external company are used to explore the environment within the company network and access systems other than those explicitly released, or information may be obtained from application systems that are not directly related to the company's mission.

Information, which is processed or accessed, is an essential asset of the Montaplast of North America. The information security management system of the Montaplast of North America provides security measures to guarantee a basic protection for data, information and the underlying infrastructure. To achieve a continuous basic protection, it is necessary to apply the security standards also in the context of the cooperation with external contractors. Depending on the type of cooperation, different requirements can arise for the security measures to be implemented. In principle, the defined security regulations apply to all internal and external employees.

Various forms of cooperation with external partners are possible. For the application of the Montaplast Security Regulations different types of cooperation were defined.

Forms of cooperation	
Type	Description of the cooperation with the external partner
Type 1: External data processing (without network connection and remote access)	The client's data is stored on the contractor's systems. For example, the contractor receives the client's data within the scope of a design, development or construction order or becomes active for the client as a software developer. He processes the data independently on his own systems. The contractor receives the data from the principal via data carriers (USB media, tapes, etc.), e-mail or in another way within the framework of an information exchange (VDA/Odette-DFÜ communication, file transfer, download, etc.).
Type 2: Data processing on contractor's systems (outsourcing, cloud, network interconnection, etc.)	The contractor is to, for example, carry out information processing on its own hardware and system software on behalf of the customer. The contractor provides, for example, the operating systems, application systems and/or communication components. The client is responsible for the data, whereby the processing of the data involves (personal) information / data that requires protection. In the case of processing personal data, this is a contract processing. In addition to the connection of the contractor on the basis of routers/firewalls, modems/communication servers as well as the Internet, the direct integration of the contractor into the IT infrastructure of the client is also possible, e.g. cloud computing, SaaS etc. <ul style="list-style-type: none"> – The contractor accesses the client's systems. – The client's data is stored on the contractor's systems. – The client transfers data to the contractor, who processes the data on his systems.
Type 3: On-site access	The contractor accesses data at the client's location and takes over the function of user service (second level support) for the end users (advice, problem assistance, troubleshooting). As operator, the contractor assumes the operational responsibility for networks, systems and applications. As software developer the contractor has access to the IV infrastructure. In the case of on-site access, the contractor is usually directly integrated into the contractor's IT infrastructure. No personal data or information requiring protection is processed on the contractor's systems.

Document Name Information Security Guidelines for contractors			
Document types system 03 Guidelines / Directives			
Version Version 1, 01.03.2020	Valid from 01.03.2020	Classification Public	Page 5/17

Forms of cooperation	
Type	Description of the cooperation with the external partner
Type 4: Remote access or direct coupling	<p>There are two cases of remote access:</p> <ol style="list-style-type: none"> the contractor has remote access to the client's systems and applications via a network connection <p>Examples of use:</p> <ul style="list-style-type: none"> – The contractor is directly integrated into the work process as a client in a client/server application of the client. – The contractor is a participant in a WEB conference, an online meeting, etc. – The contractor takes part in the various forms of office communication. – The contractor is to carry out remote maintenance on the customer's IT systems or installations or other network-integrated systems. <ol style="list-style-type: none"> there is remote access by subcontractors, teleworkers, etc. to systems and applications at the contractor's premises the connection is based on router/firewall, Internet or VPN connections or ISDN/modem/communication server. No personal data or information requiring protection is processed on the contractor's systems.
Type 5: System provision by the client	<p>The Client shall provide the Contractor with a system for use with which the Contractor can be integrated into the Client's infrastructure. The security configurations and standards are defined by the client. (Example: employees of the contractor work with systems provided by the client on the client's premises or are given equipment for use).</p>
Type 6: Physical objects/information	<p>Physical sensitive information such as files, concepts, contracts, samples, prototypes, components, tools, devices, etc. as well as accompanying information and data are processed, created or stored at the contractor's premises, which have been classified as "confidential" or "secret" by the client.</p>
Note: mixed forms will be the rule	

4 Requirements for contractors to maintain information security

4.1 Basic principles

The contractor is required to implement an information security management system in accordance with the requirements of ISO 27001/27002 and to comply with the legal requirements regarding data protection.


Depending on the form of the cooperation there are points of emphasis regarding the requirements covering the security measures to be implemented. The form of the cooperation may change in the course of the business relationship. In these circumstances the security measures to be implemented will also change. The following text sets out the minimum requirements for the contractor's information security management system.

4.2 Organising the security of information

Guidelines, processes and responsibilities must be defined, with which the security of information can be implemented and monitored.

This includes in particular:

- the establishment of an information security guideline.

Document Name Information Security Guidelines for contractors			
Document types system 03 Guidelines / Directives			
Version Version 1, 01.03.2020	Valid from 01.03.2020	Classification Public	Page 6/17

- user guidelines setting out the rules for handling applications, systems and IT devices, as well as ways of using information technology.
- the description of processes for managing data-carriers, documents and information.
- the specification of roles and responsibilities in the field of information security.
- the duties of employees regarding confidentiality and the protection of trade secrets.
- the regular execution of training and awareness measures.

4.3 Privacy by design (only relevant for personal related data)

Systems and applications should be designed and implemented in such a way as to minimise the amount of personal data processed. Essential elements of data economy are the separation of personal identifiers and content data, the use of pseudonyms and anonymisation. Furthermore, the deletion of personal data must be implemented in accordance with a configurable retention period.

This includes in particular:

- No more personal data is collected than is necessary for the purpose.
- GDPR compliant deletion of processed personal data is guaranteed.
- Privacy by Design is taken into account when changing and introducing systems and applications.

4.4 Privacy by default

Systems and applications must be set up in such a way that privacy-friendly pre-setting's/defaults are available and as little personal data as possible is collected.

This includes in particular:


- Simple exercise of the right of withdrawal by the person concerned through technical measures.
- Tracking functions that monitor the affected person are deactivated by default.
- All pre-settings of selection options meet the requirements of the GDPR with regard to data protection-friendly pre-settings (e.g. no pre-settings of opt-ins).

4.5 Controlling access

Actions must be implemented to ensure that personnel authorized to use the information processing procedures can access only the personnel-related data and information/data requiring protection which are covered by their access authorization.

This includes in particular:

- the creation of authorization concepts for access to information, systems and applications requiring protection.
- the implementation of restrictions on access.
- preventing a concentration of functions and establishing a separation of functions.
- the implementation of a process for issuing authorizations.
- the regular checking of authorizations.
- recording the issue of authorizations and access to data.

Document Name Information Security Guidelines for contractors			
Document types system 03 Guidelines / Directives			
Version Version 1, 01.03.2020	Valid from 01.03.2020	Classification Public	Page 7/17

4.6 Cryptography and / or pseudonymisation

The use of coding procedures to ensure the orderly and effective protection of confidentiality, authenticity or integrity of personnel-related data and information requiring protection. Measures in the processing of personal data that are suitable to make it more difficult to identify the data subject

This includes in particular:

- Encryption of data carriers and hard disks of PCs, laptops, mobile devices and directories.
- Secure storage of data on mobile data media.
- Organizational instruction for the encryption of data.
- Encrypted storage of personal data.
- Encryption of data backup media.
- Encryption of access to the network and network connections.
- Use of pseudonyms, procedures for pseudonymisation of data.
- Use of methods for the anonymization of data.

4.7 Protection of buildings

Actions must be taken to prevent unauthorized physical access to the organisation's information and information-processing facilities, as well as preventing their damage or deterioration.

This includes in particular:

- specifying secure areas.
- implementing access prevention.
- specifying personnel with access authorization.
- managing personnel-related access authorizations.
- rules for accompanying visitors and external personnel.
- monitoring areas outside opening hours.
- recording access by personnel.

4.8 Protecting operating equipment / information data

Appropriate action must be taken to prevent the loss, damage or theft or deterioration of operating equipment / information data and to prevent breaks in the production activities of the organisation.

This includes in particular:


- rules for the secure positioning of operating equipment.
- protecting operating equipment against over-voltage, power failures, fire and water.
- protecting information and information processing systems against theft.
- rules for the regular maintenance of operating equipment.
- implementing a process for the secure deletion, disposal and destruction of operating equipment.

4.9 Operating procedures and responsibilities

Measures must be taken to ensure the orderly and secure operation of systems and procedures for processing information.

This includes in particular:

- documenting operating procedures, in the form of operating manuals, for example.

Document Name Information Security Guidelines for contractors			
Document types system 03 Guidelines / Directives			
Version Version 1, 01.03.2020	Valid from 01.03.2020	Classification Public	Page 8/17

- securing IT systems.
- the separate processing of production and test data.
- ensuring the separation of clients / separation of client data.
- Requirements covering a separation of functions must be implemented. The functions that cannot be linked and therefore are not be handled by more than one person simultaneously, must be specified, documented and justified. As a general principle operational functions must not be linked with monitoring functions.

4.10 Data backup

Actions must be taken to ensure that information and data / personnel-related data requiring protection are protected against accidental destruction or loss.

This includes in particular:

- the creation of a data security concept.
- the regular execution of data protection measures.
- The data security media must be stored separately from the production systems.

4.11 Protection against malware by managing weaknesses and patches

The misuse of technical weak points must be prevented by the installation of current virus protection software and the implementing of patch management.

Regular checks must be carried out to detect possible weak points.

This includes in particular:

- Regular status monitoring of security updates and system vulnerabilities.
- Use of anti-malware software.
- Regular installation of security patches and updates.

4.12 Protocolling and monitoring

Actions must be taken to ensure that checks can be made at a later stage to determine if and by whom (personnel-related) data in IT systems have been entered, modified or deleted.

These actions include in particular:


- the recording of access authorizations and access to data.
- regular checks on user authorizations.
- the recording of activities and regular evaluation of user and system activities

4.13 Network security management

Appropriate protection for the network must be implemented so that information and the infra-structure components are protected.

This includes in particular:

- the implementation of a network management system.
- the introduction of a user authentication system for external connections and connections between individual systems.
- ensuring the protection of diagnosis and configuration ports.

Document Name Information Security Guidelines for contractors			
Document types system 03 Guidelines / Directives			
Version Version 1, 01.03.2020	Valid from 01.03.2020	Classification Public	Page 9/17

- Security gateways at transfer points / network limits.
- the isolation of sensitive systems.

4.14 Information transfer

Actions must be taken to ensure that personnel-related data and information and data requiring protection cannot be read, copied, modified or removed during electronic transfer or while they are transported or stored on data-carriers and that it is possible to check and discover at which points a transfer of personnel-related data and information and data requiring protection is possible by data transfer facilities. (This includes a description of the facilities used and transfer protocols, such as identification and authentication and encoding to the latest state of technology, automatic call-back, etc.)

This includes in particular:

- the secure transport and delivery of data / documents depending on the need to protect the data.
- the recording of data transfers.
- the description of interfaces between systems and external data connections
- the appropriate protection of emails containing sensitive information / data.
- the agreement of contracts for the protection of trade secrets with third parties and sub-suppliers.

4.15 Network separation

Groups of information services, clients, users and information systems should be separated from each other in networks.

This includes in particular:

- separating groups of information services, clients, users and information systems from each other.
- To reduce the risk that personnel-related data and information and data requiring protection are read on the network while they are being transferred between IT systems, these must be segmented.
- Direct connections by an Internet client via remote access (e.g., via VPN or RAS) to the company's network must be prevented by appropriate measures.

4.16 Obtaining, developing and maintaining systems


Actions and processes must be implemented to ensure that information security is an integral part of information systems over their entire lifetime.

This includes in particular:

- specifying security-specific rules and regulations covering the introduction of new information systems and the expansion of existing information systems.
- specifying rules for the development and alignment of software and systems.
- the development of guidelines for safe system development.
- monitoring external system development activities.
- the protection of test data.

4.17 Relationships with suppliers

Security measures to reduce the risks associated with the involvement of external parties should be agreed with sub-suppliers / sub-contractors and documented.

Document Name Information Security Guidelines for contractors			
Document types system 03 Guidelines / Directives			
Version Version 1, 01.03.2020	Valid from 01.03.2020	Classification Public	Page 10/17

This includes in particular:

- the written addressing of security matters in contracts with sub-suppliers
- checking the security of sub-contractors
- the determination of technical organizational measures (TOMs) when processing personal data.
- the ongoing review of the contractor and its activities.

4.18 Managing information security incidents

Consistent and effective actions for the management of information security incidents (theft, system failure, data loss, etc.) must be implemented.

This includes in particular:

- the immediate reporting of information security incidents to the customer.
- the recording of security incidents.
- the implementing of processes for introducing action to prevent / prevent the recurrence of information security incidents.

4.19 Information security aspects of business continuity management/emergency management

System availability must be maintained in difficult situations such as crises or major damage. This must be ensured by an emergency management system. Requirements covering information security should be specified when planning the continuity of operations and recovery following an emergency.

This includes in particular:

- the creation of redundancies for critical components.
- assessing risks and planning actions to ensure continuation of the company's activities.
- the creation of emergency action plans.
- the regular execution of tests of the effectiveness of the emergency actions
- early information to the customer in the event of an emergency.

4.20 Compliance with legal and contractual requirements

The implementation of measures to prevent breaches of legal, official or contractual obligations and any security requirements.

This includes in particular:


- the agreement of confidentiality obligations with employees and sub-suppliers.
- ensuring compliance with legal obligations within the framework of the cooperation.
- the return of all data, operating equipment and information data to the customer at the end of the contract.

4.21 Data protection requirements and data protection management

Protection in the private sphere, as well as the protection of personnel-related data should be ensured in accordance with relevant legislation, regulations and if appropriate, the terms of a contract.

This includes in particular:

- the appointment of a data protection officer.
- the establishment of a data protection management system.

Document Name Information Security Guidelines for contractors			
Document types system 03 Guidelines / Directives			
Version Version 1, 01.03.2020	Valid from 01.03.2020	Classification Public	Page 11/17

- the creation of procedure directories.
- the establishment of a management system for data protection in an emergency.
- the execution of regular checks / audits.
- compliance with legal requirements within the framework of contract data processing.
- the immediate reporting of data protection incidents to the customer.

4.22 Information security checks

Regular checks must be made to ensure that information processing is carried out in accordance with the defined security measures. The contractor must carry out regular checks in this regard. The contractor will grant the customer the right to carry out regular checks at the contractor's premises.

5 Contractor's duty to inform


The external partner must inform the client immediately about information security incidents, in case of serious disruptions of the operating process, suspicion of data protection violations or other irregularities in the processing of the client's data; in particular, incidents that allow access by unauthorized persons.

If the data of the Customer is endangered at the external partner's premises by seizure or confiscation, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall inform the Customer immediately. The Contractor shall inform all persons responsible in this context without delay that the sovereignty and ownership of the data lies exclusively with the Customer.

The notifications are to be sent to the central e-mail address: cybersecurity@montaplast.com.


6 Review of the implementation of security measures

Montaplast reserves the right to check the implementation of the security requirements set out in Section 4. The current version of ISO 27001, the VDA questionnaire and/or an individual assessment is used for the review. Alternatively, compliance with information security can also be proven by a valid ISO 27001 certificate, a TISAX assessment or another equivalent verification.


Document Name Information Security Guidelines for contractors			
Document types system 03 Guidelines / Directives			
Version Version 1, 01.03.2020	Valid from 01.03.2020	Classification Public	Page 12/17

7 Annex Security measures depending on the form of cooperation


Technical and organisational security requirements depending on the form of cooperation (Measures marked with AV are only relevant if personal data are processed in the order)			Forms of cooperation					
No	Reference ISO 27001/ DSGVO	Technical-organisational measure	1. external data processing	2. data processing on systems of the contractor	3. on-site access	4. remote access or direct coupling	5. system provision by the client	6. physical objects/information
01	A.05A .06A .07A .08	Organisation of information security Definition of guidelines, processes and responsibilities with which information security can be implemented and controlled. <u>General requirements:</u> <ul style="list-style-type: none"> - Information Security Policy. - User guidelines for the handling of equipment and behaviour when using information technology. - Processes for the management of data media. - Definition of roles and responsibilities. - Obligation of the employees to maintain secrecy and data secrecy. - Regular implementation of training and awareness measures. 	x	x	x	x		x
02	A.06 A.14 A.18 Art 25 (1)	Privacy by Design Systems and applications should be designed and implemented in such a way as to minimise the amount of personal data processed. Key elements of data minimisation are the separation of personal identifiers and content data, the use of pseudonyms and anonymisation. Furthermore, the deletion of personal data must be implemented in accordance with a configurable retention period. <u>General requirements:</u> <ul style="list-style-type: none"> - No more personal data is collected than is necessary for the purpose. - DSGVO compliant deletion of the processed personal data is guaranteed. - Privacy by Design is taken into account when systems and applications are modified and introduced. 	AV	AV	AV	AV		AV
03	A.06 A.14 A.18 Art 25 (2)	Privacy by Default Systems and applications must be set up in such a way that data-protection-friendly pre-setting's/defaults are available and that as little personal data as possible is collected. <u>General requirements:</u> <ul style="list-style-type: none"> - Simple exercise of the right of withdrawal by the person concerned by means of technical measures. - Tracking functions that monitor the person concerned are deactivated by default. - All pre-setting's of options meet the requirements of the DSGVO with regard to data protection-friendly pre-setting's (e.g. no pre-setting's of opt-ins). 	AV	AV	AV	AV		

Document Name Information Security Guidelines for contractors			
Document types system 03 Guidelines / Directives			
Version Version 1, 01.03.2020	Valid from 01.03.2020	Classification Public	Page 13/17


Technical and organisational security requirements depending on the form of cooperation (Measures marked with AV are only relevant if personal data are processed in the order)			Forms of cooperation					
No	ReferenceISO 27001/ DSGVO	Technical-organisational measure	1. external data processing	2. data processing on systems of the contractor	3. on-site access	4. remote access or direct coupling	5. system provision by the client	6. physical objects/information
04	A.09 Art 32 (1) b	Access control implementing measures to ensure that those authorised to use the data processing procedures can only access personal data or sensitive information and data subject to their access authorisation <u>General requirements:</u> <ul style="list-style-type: none"> - Creation of an authorisation concept. - Implementation of access restrictions. - Avoiding the concentration of functions and establishing a separation of functions. - Implementation of an authorisation assignment process. - Regular review of allowances. - Logging of the assignment of authorisations and data access. 	x	x	x	x		
05	A.10 Art 32 (1) a	Cryptography and / or pseudonymisation the use of encryption procedures to ensure the proper and effective protection of the confidentiality, authenticity or integrity of personal data or sensitive information. <u>General requirements:</u> <ul style="list-style-type: none"> - Encryption of data carriers and hard disks of PCs, laptops, mobile devices and directories. - Secure storage of data on mobile data media. - Organisational instructions for the encryption of data - Encrypted storage of personal data. - Encryption of data backup media - Encryption of access to the network and network connections <ul style="list-style-type: none"> - Use of pseudonyms, procedures for pseudonymisation of data. - Use of procedures for the anonymisation of data. 	x	x		x		
06	A.11 Art 32 (1) b	Protection of buildings Preventing of unauthorised physical access to, damage to and interference with the organisation's information and information processing equipment. <u>General requirements:</u> <ul style="list-style-type: none"> - definition of security restricted areas. - Implementation of access protection. - Determination of persons authorised to enter. - Management of personal access authorisations. - Rules for the escort of visitors and external staff. - Monitoring of the rooms outside the closing times. - Logging of the access. 	x	x				x

Document Name Information Security Guidelines for contractors				
Document types system 03 Guidelines / Directives				
Version Version 1, 01.03.2020	Valid from 01.03.2020	Classification Public	Page 14/17	

Technical and organisational security requirements depending on the form of cooperation (Measures marked with AV are only relevant if personal data are processed in the order)			Forms of cooperation					
No	ReferenceISO 27001/ DSGVO	Technical-organisational measure	1. external data processing	2. data processing on systems of the contractor	3. on-site access	4. remote access or direct coupling	5. system provision by the client	6. physical objects/information
07	A.11 Art 32 (1) b Art 32 (1) c	Protection of equipment / information assets Prevention of loss, damage, theft or impairment of values and interruptions of the organisation's operations <u>General requirements:</u> <ul style="list-style-type: none"> - Safe placement of operating equipment. - Protection against overvoltage, power failure, water and fire. - Protection against theft. - Regular maintenance. - Process for the safe extinguishing, disposal and destruction of equipment. 	x	x				x
08	A.12 Art 32 (1) b	Operating procedures and responsibilities Ensuring the proper and secure operation of information processing systems and procedures. <u>General requirements:</u> <ul style="list-style-type: none"> - Documentation of operating procedures. - Curing of the backend systems. - Separate processing of production and test data. - Multi-client capability. - allocation of tasks and segregation of duties of functions which are incompatible with each other. 	x	x				
09	A.12 Art 32 (1) c	Data backup / restore: Measures to ensure that personal data or sensitive information and data are protected against accidental destruction or loss. <u>General requirements:</u> <ul style="list-style-type: none"> - Creation of a data backup concept. - Performing regular data backups. - Separate storage of the data backup media. 	x	x				
10	A.12 Art 32 (1) b	Protection against malware and patch management Preventing the exploitation of technical weaknesses by using up-to-date virus protection software and implementing patch management. Regular checks are carried out to detect weak points. <u>General requirements:</u> <ul style="list-style-type: none"> - Regularly monitor the status of security updates and system vulnerabilities. - Use of anti-malware software. - Regular installation of security patches and updates. 	x	x	x	x		

Document Name Information Security Guidelines for contractors			
Document types system 03 Guidelines / Directives			
Version Version 1, 01.03.2020	Valid from 01.03.2020	Classification Public	Page 15/17

Technical and organisational security requirements depending on the form of cooperation (Measures marked with AV are only relevant if personal data are processed in the order)			Forms of cooperation					
No	ReferenceISO 27001/ DSGVO	Technical-organisational measure	1. external data processing	2. data processing on systems of the contractor	3. on-site access	4. remote access or direct coupling	5. system provision by the client	6. physical objects/information
11	A.12 Art 32 (1) d	Logging and monitoring Measures to ensure that it can be subsequently checked and established whether and by whom (personal) data have been entered, modified or removed from IT systems. (All system activities are logged; the logs are kept by the contractor for at least 3 years). <u>General requirements:</u> <ul style="list-style-type: none"> - Logging of the assignment of authorisations and data access. - Checking user permissions. - Logging of activities and regular evaluation of user and system activities. 	x	x		x		
12	A.13 Art 32 (1) b	Network security management Adequate protection must be implemented for the network so that information and infrastructure components are protected. <u>General requirements:</u> <ul style="list-style-type: none"> - Implementation of network management. - User authentication for external connections and connections between systems. - Protection of the diagnostic and configuration ports. - Security gateways at the transfer points / network boundaries. - Isolation of sensitive systems. 	x	x		x		
13	A.13 Art 32 (1) b	Transmission of information Methods to ensure that personal data or sensitive information and data cannot be read, copied, altered or removed without authorisation during electronic transmission or during their transport or storage on data carriers, and that it is possible to verify and establish to which bodies personal data or sensitive information and data are to be transmitted by data transmission equipment. (Description of the equipment used and transmission protocols, e.g. identification and authentication, state-of-the-art encryption, automatic call-back, etc.) <u>General requirements:</u> <ul style="list-style-type: none"> - Secure transport and dispatch of data / documents depending on the protection requirements of the data. - Logging of data transmissions. - Description of interfaces between systems and external data connections. - Appropriate protection of emails containing sensitive information / data. - Conclusion of contracts to protect business secrets with third parties and subcontractors. 	x	x				

Document Name Information Security Guidelines for contractors			
Document types system 03 Guidelines / Directives			
Version Version 1, 01.03.2020	Valid from 01.03.2020	Classification Public	Page 16/17

Technical and organisational security requirements depending on the form of cooperation (Measures marked with AV are only relevant if personal data are processed in the order)			Forms of cooperation					
No	ReferenceISO 27001/DSGVO	Technical-organisational measure	1. external data processing	2. data processing on systems of the contractor	3. on-site access	4. remote access or direct coupling	5. system provision by the client	6. physical objects/information
14	A.13 Art 32 (1) b	Network separation Groups of information services, clients, users and information systems should be kept separate in networks. <u>General requirements:</u> <ul style="list-style-type: none"> - Logical client separation. - Data separation by segmentation of networks of different clients. - Separation of networks for remote access. 	x	x		x		
15	A.14 Art 25 (1) Art 25 (2)	Acquisition, development and maintenance of systems Measures to ensure that information security is an integral part of the life cycle of information systems. <u>General requirements:</u> <ul style="list-style-type: none"> - definition of safety regulations and requirements for the use of new information systems and for the extension of existing information systems. - Establishing rules for the development and adaptation of software and systems. - Guidelines for safe system development. - Monitoring of outsourced system development activities. - Protection of test data. 	x	x	x	x		
16	A.15 Art 28)	Supplier relations or order processing Measures for information security, to reduce risks in connection with the access of suppliers to the values of the company, should be agreed with sub-suppliers / subcontractors and documented. <u>General requirements:</u> <ul style="list-style-type: none"> - Written addressing of security issues in contracts with sub-suppliers. - Definition of technical organisational measures (TOMs) when processing personal data. - Verification of the safety of subcontractors. - Continuous review of the contractor and his activities. 	x	x	x	x	x	x
17	A.16	Management of information security incidents Consistent and effective measures shall be implemented for the management of information security incidents (theft, system failure, data loss etc.). <u>General requirements:</u> <ul style="list-style-type: none"> - Processes for immediate information of the client. - Logging of security incidents. - Processes for handling and preventing information security incidents. 	x	x	x	x	x	x
18	A.17 Art 32 (1) c	Information Security Aspects of Business Continuity Management Maintaining system availability in difficult situations such as crisis or damage events must be maintained. An emergency management must ensure this. The requirements regarding		x				

