ClickMeeting

Description of the implemented organizational and technical measures for personal data protection *(Beschreibung der durchgeführten organisatorischen und technischen Maßnahmen zum Schutz personenbezogener Daten)*

Area */ Bereich*	**Safety measures** */ Sicherheitsmaßnahmen*	
Information Security Management System / ***Informationssicherheits-Managementsystem***	**Security policy.** A general security policy has been developed, along with specific security policies regarding organization security, information security, IT system security and security of people and property, all of them defining the basic objectives of the actions related to compliance therewith. The policies are subject to periodic reviews and revisions, to be approved by the Company's top management. The roles and tasks in security management processes have been defined. The individuals responsible for compliance with each respective security policy have been appointed. **Security standards.** General and specific security standards have been defined that implement the assumptions of the security policies in terms of information security, IT system security, and security of people and property. A periodic review and revision program was developed for the security standards. **Procedures and instructions.** Specific procedures and operating instructions have been developed for the implementation of the security standards in terms of information security, IT system security, and security of people and property. A periodic review and revision program was developed for the procedures and instructions regarding compliance with security standards. **Resource owners.** For every resource (whether physical or electronic) that is of value for the organization, a responsible person (Resource Owner) has been appointed as being in charge of managing the security of that resource. Processes for resource identification and collection by those whose employment is being terminated or who no longer use access to that resource have been put in place.	***Sicherheitspolitik.*** *Es wurden eine allgemeine Sicherheitsrichtlinie sowie spezifische Sicherheitsrichtlinien in Bezug auf die Sicherheit von Organisationen, Informationen, IT-Systemen und die Sicherheit von Personen und Sachwerten entwickelt, die alle die grundlegenden Ziele der Maßnahmen im Zusammenhang mit der Einhaltung dieser Richtlinien definieren. Die Richtlinien unterliegen regelmäßigen Überprüfungen und Überarbeitungen, die vom Top-Management des Unternehmens genehmigt werden müssen. Die Rollen und Aufgaben in Sicherheitsmanagementprozessen wurden definiert. Die Personen, die für die Einhaltung der jeweiligen Sicherheitsrichtlinien verantwortlich sind, wurden ernannt.* ***Sicherheitsstandards.*** *Es wurden allgemeine und spezifische Sicherheitsstandards definiert, die die Annahmen der Sicherheitsrichtlinien in Bezug auf Informationssicherheit, IT-Systemsicherheit und Sicherheit von Personen und Eigentum umsetzen. Für die Sicherheitsstandards wurde ein periodisches Überprüfungs- und Überarbeitungsprogramm entwickelt.* ***Verfahren und Anweisungen.*** *Für die Umsetzung der Sicherheitsstandards in Bezug auf Informationssicherheit, IT-Systemsicherheit und Sicherheit von Personen und Sachwerten wurden spezielle Verfahren und Betriebsanweisungen entwickelt. Für Verfahren und Betriebsanweisungen wurden ein periodisches Überprüfungs- und Überarbeitungsprogramm entwickelt.* ***Ressourcenbesitzer.*** *Für jede Ressource (ob physisch oder elektronisch), die für die Organisation von Wert ist, wurde eine verantwortliche Person (Ressourceneigentümer) ernannt, die für die Verwaltung der Sicherheit dieser Ressource verantwortlich ist. Prozesse zur Identifizierung und Erfassung von Ressourcen durch Personen, deren Beschäftigung beendet wird oder die keinen Zugriff mehr auf diese Ressource haben, wurden eingerichtet.* ***Datenschutzbeauftragter.*** *Um ein angemessenes Maß an Schutz personenbezogener Daten zu gewährleisten, wurde ein unabhängiger Datenschutzbeauftragter benannt und ernannt. Der Datenschutzbeauftragte berichtet*

Area / *Bereich*	Safety measures / *Sicherheitsmaßnahmen*	
	Data Protection Officer. To ensure proper level of personal data protection, an independent Data Protection Officer has been designated and appointed. The Data Protection Officer reports directly to the Company's top management. The Data Protection Officer has been included in all the processes connected with personal data processing. The Data Protection Officer has been granted sufficient access to any information and documentation connected with personal data processing. **Individuals authorized to process personal data.** Those who process personal data at the request and on behalf of the Company have been specifically indicated by name as authorized to process personal data. An internal personal data security and protection training scheme has been developed and put in place. All the individuals authorized to process personal data have been included in the internal personal data security and protection training scheme. Anyone who has access to data has been obligated to respect data confidentiality throughout the term of employment and thereafter. **Monitoring of legislative changes.** A system to monitor changes in personal data processing legislation has been developed and put in place, and the continuity of its operations has been ensured. **Access rights management.** Access rights management procedures have been developed for access to data storage devices, rooms, zones, buildings, IT systems and elements of the IT infrastructure and network. A procedure of monitoring and checking the access rights ad hoc and periodically has been provided. It has been made sure that the individuals authorized to process personal data are assigned minimum data access rights, depending on the requirements of their job titles and their tasks. A possibility of monitoring the processing operations has been introduced towards those who delete, add or modify personal data. **Securing personal data storage devices.** It has been made sure that keys and access codes to lockers are	*direkt an die Gesellschaftsführung. Der Datenschutzbeauftragte wurde in alle Prozesse im Zusammenhang mit der Verarbeitung personenbezogener Daten einbezogen. Der Datenschutzbeauftragte hat ausreichenden Zugang zu allen Informationen und Unterlagen im Zusammenhang mit der Verarbeitung personenbezogener Daten.* ***Personen, die zur Verarbeitung personenbezogener Daten berechtigt sind.*** *Personen, die auf Anfrage und im Auftrag des Unternehmens personenbezogene Daten verarbeiten, wurden namentlich als für die Verarbeitung personenbezogener Daten Verantwortliche bezeichnet. Ein internes Schulungsprogramm für die Sicherheit und den Schutz personenbezogener Daten wurde entwickelt und eingerichtet. Alle Personen, die zur Verarbeitung personenbezogener Daten berechtigt sind, wurden in das interne Schulungsprogramm für die Sicherheit und den Schutz personenbezogener Daten aufgenommen. Jeder, der Zugang zu Daten hat, ist verpflichtet, die Daten während der gesamten Beschäftigungsdauer und danach vertraulich zu behandeln.* ***Überwachung von Gesetzesänderungen.*** *Ein System zur Überwachung von Änderungen in der Gesetzgebung zur Verarbeitung personenbezogener Daten wurde entwickelt und eingerichtet, und die Kontinuität seiner Tätigkeiten wurde sichergestellt.* ***Zugriffsrechte-Verwaltung.*** *Es wurden Zugriffsrechteverwaltungsverfahren für den Zugriff auf Datenspeichergeräte, Räume, Zonen, Gebäude, IT-Systeme und Elemente der IT-Infrastruktur und des Netzwerks entwickelt. Es wurde ein Verfahren zur Ad-hoc- und regelmäßigen Überwachung und Überprüfung der Zugriffsrechte bereitgestellt. Es wurde sichergestellt, dass den Personen, die zur Verarbeitung personenbezogener Daten berechtigt sind, je nach den Anforderungen ihrer Berufsbezeichnungen und ihrer Aufgaben minimale Datenzugriffsrechte zugewiesen werden. Für diejenigen, die personenbezogene Daten löschen, hinzufügen oder ändern, wurde eine Möglichkeit zur Überwachung der Verarbeitungsvorgänge eingeführt.* ***Sichern persönlicher Datenspeichergeräte.*** *Es wurde sichergestellt, dass Schlüssel und Zugangscodes für Schließfächer Personen zur Verfügung gestellt werden, die zur Verarbeitung personenbezogener Daten gemäß dem Umfang der Berechtigung und dem Umfang der im Rahmen der Arbeitsstelle ausgeführten Aufgaben berechtigt sind.* ***Sicherung der Gebäude, Zonen, Räume oder Raumteile, in denen personenbezogene Daten verarbeitet werden.*** *Es wurde*

Area / *Bereich*	Safety measures / *Sicherheitsmaßnahmen*	
	provided to individuals authorized to process personal data in accordance with the scope of the authorization and the scope of tasks performed within the job position. **Securing the buildings, zones, rooms or parts of rooms where personal data are processed.** It has been made sure that: (i) keys, access codes and access rights in the access control system for access to buildings, zones, rooms or parts of rooms where personal data are processed are provided to individuals authorized to process personal data in accordance with the scope of their authorization and the scope of the tasks performed within their job position; (ii) buildings, zones, rooms or parts of rooms where personal data are processed are secured against unauthorized access in the absence of the individuals authorized to be in these rooms. Anyone who is not authorized to be in the rooms used for personal data processing may only stay there under the supervision of authorized persons. **Access to IT systems, elements of the IT infrastructure and networks.** It has been made sure that for every person authorized to access the IT system or an element of the IT infrastructure or network: (i) a unique ID is assigned that cannot be assigned to anyone else; (ii) authorization takes place using secure methods of transmitting the authentication data; (iii) the access password is subject to audit procedures and must be changed at predetermined intervals. **Threat and vulnerability management.** Security gaps are periodically scanned on the platforms and in the networks that process personal data so that general security standards connected specifically with system reinforcement are complied with. As a result of penetration tests, vulnerability scanning and compliance assessment, a corrective program is run on a periodic basis according to a risk-based approach to make use of the lessons learned. **Security of service providers and subcontractors.** The subcontractor and provider selection rules that	*sichergestellt, dass: (i) Schlüssel, Zugangscodes und Zugangsrechte im Zugangskontrollsystem für den Zugang zu Gebäuden, Zonen, Räumen oder Teilen von Räumen, in denen personenbezogene Daten verarbeitet werden, werden Personen zur Verfügung gestellt, die befugt sind, personenbezogene Daten im Rahmen ihrer Berechtigung zu verarbeiten, und in dem Umfang der Aufgaben, die in ihrer Arbeitsposition ausgeführt werden; (ii) Gebäude, Zonen, Räume oder Teile von Räumen, in denen personenbezogene Daten verarbeitet werden, sind gegen unbefugten Zugriff gesichert, wenn keine Personen in diesen Räumen befugt sind. Wenn jemand kein Zugangsrecht zu den zur Verarbeitung personenbezogener Daten genutzten Räumen hat, darf sich dort nur unter Aufsicht befugter Personen aufhalten.* ***Zugang zu IT-Systemen, Elementen der IT-Infrastruktur und Netzwerken.*** *Es wurde sichergestellt, dass für jede Person, die berechtigt ist, auf das IT-System oder ein Element der IT-Infrastruktur oder des IT-Netzwerks zuzugreifen, Folgendes gilt: (i) eine eindeutige ID zugewiesen wird, die niemand anderem zugewiesen werden kann; (ii) die Autorisierung erfolgt unter Verwendung sicherer Methoden zur Übermittlung der Authentifizierungsdaten; (iii) das Zugangspasswort unterliegt Prüfverfahren und muss in festgelegten Abständen geändert werden.* ***Risiko- und Schwachstellenmanagement.*** *Auf den Plattformen und in den Netzwerken, die personenbezogene Daten verarbeiten, werden regelmäßig Sicherheitslücken gescannt, damit die allgemeinen Sicherheitsstandards eingehalten werden, die speziell für die Systemverstärkung gelten. Als Ergebnis von Penetrationstests, Schwachstellenüberprüfungen und Konformitätsbewertungen wird regelmäßig ein Korrekturprogramm nach einem risikobasierten Ansatz durchgeführt, um die gewonnenen Erkenntnisse zu nutzen.* ***Sicherheit von Dienstleistern und Subunternehmern.*** *Die entwickelten Regeln für die Auswahl von Unterauftragnehmern und Anbietern gewährleisten ein angemessenes Maß an technischer und organisatorischer Sicherheit für die erbrachten Dienstleistungen und die ausgeführten Aufgaben. Die Prüfungsstandards und -mechanismen für Subunternehmer und Dienstleister wurden entwickelt und deren Umsetzung wurde garantiert.* ***Änderungsmanagement.*** *Es wurde eine dokumentierte Änderungskontrollrichtlinie eingeführt, die Anforderungen für die*

Area / *Bereich*	Safety measures / *Sicherheitsmaßnahmen*	
	have been developed guarantee adequate level of technical and organizational security of the services provided and the tasks performed. The subcontractor and service provider auditing standards and mechanisms have been developed and their implementation has been guaranteed. **Change management.** A documented change control policy has been put in place which includes requirements for approving, classifying and testing the back-out plan and the division of responsibilities between request, approval and implementation. Procedures for managing and responding to security breach incidents have been put in place to allow reasonable detection, testing, response, mitigation of consequences, and notification of any events that involve a threat to the confidentiality, integrity and/or availability of personal data. The response and management procedures are documented, checked and reviewed at least on an annual basis. **Additional security measures of the ClickMeeting software application.** The following standards have been developed and put in place: (i) regarding software production security. (ii) regarding the analysis of the risk of violating the basic rights and freedoms of data subjects and the risk of loss of personal data confidentiality, availability and integrity at every product life cycle stage; (iii) regarding compliance with the privacy protection principle at the software design stage; (iv) regarding compliance with the privacy protection principle in default settings at the software design stage. A training program regarding the rules of secure software production and a software security testing program have been developed.	*Genehmigung, Klassifizierung und Prüfung des Sicherungsplans sowie die Aufteilung der Zuständigkeiten zwischen Anforderung, Genehmigung und Implementierung enthält. Es wurden Verfahren zum Verwalten und Reagieren auf Sicherheitsverletzungen eingeführt, um eine angemessene Erkennung, Prüfung, Reaktion, Abschwächung von Folgen und Benachrichtigung über Ereignisse zu ermöglichen, die eine Bedrohung für die Vertraulichkeit, Integrität und/oder Verfügbarkeit personenbezogener Daten darstellen. Die Reaktions- und Managementverfahren werden mindestens einmal jährlich dokumentiert, überprüft und validiert.* ***Zusätzliche Sicherheitsmaßnahmen der ClickMeeting-Softwareanwendung.*** *Die folgenden Standards wurden entwickelt und eingeführt: (i) in Bezug auf die Sicherheit der Softwareproduktion. (ii) in Bezug auf die Analyse des Risikos der Verletzung der Grundrechte und -freiheiten betroffener Personen und des Risikos des Verlusts der Vertraulichkeit, Verfügbarkeit und Integrität personenbezogener Daten in jeder Phase des Produktlebenszyklus; (iii) in Bezug auf die Einhaltung des Datenschutzprinzips bei der Softwareentwicklung; (iv) in Bezug auf die Einhaltung des Datenschutzprinzips in den Standardeinstellungen bei der Softwareentwicklung. Ein Schulungsprogramm zu den Regeln der sicheren Softwareproduktion und ein Programm zum Testen der Software-Sicherheit wurden entwickelt.*
Security of personal data processing operations / ***Sicherheit der Verarbeitung personenbezogener Daten***	**Data collection security.** Personal data are secured against loss of accountability with solutions that permit tying specific actions to a specific person or IT system. **Security of access to data.** Personal data are secured against loss of confidentiality through: (i) secure	***Sicherheit der Datenerfassung.*** *Personenbezogene Daten werden mit Lösungen gegen den Verlust der Rechenschaftspflicht geschützt, mit denen bestimmte Aktionen an eine bestimmte Person oder ein bestimmtes IT-System gebunden werden können.* ***Sicherheit des Zugriffs auf Daten.*** *Personenbezogene Daten werden gegen den*

Area / *Bereich*	Safety measures / *Sicherheitsmaßnahmen*	
	access authentication methods for people and IT systems; (ii) monitoring of correct functioning and use of secure access authentication methods for people and IT systems; (iii) carried out and documented periodic (at least annual) reviews of access of all users, system accounts, test accounts and general accounts; (iv) implementation of session control mechanisms, including account blocking and session expiration after a predetermined time. **Data transfer/transmission security.** Personal data transferred through teletransmission are secured against loss of confidentiality and integrity using cryptographic data protection measures (data encryption in transit), and through segmentation of ICT networks (network segmentation). **Data storage security.** Personal data stored in data storage devices are secured against loss of confidentiality, availability and integrity through: (i) physical or logical data separation (data separation); (ii) real-time data copying mechanisms (data replication); (iii) mechanisms of creating incremental or full data backups at predetermined time intervals (data backup); (iv) mechanisms and procedures for data recovery, data source switching and backup restoration. Personal data stored in databases are secured against loss of integrity through the application of consistency rules in terms of semantics (definition of data type), in terms of entities (definition of basic keys) and in terms of reference (definition of foreign keys). **Data development security.** Personal data are secured: (i) against loss of confidentiality – access is provided only to authorized persons and IT systems; (ii) against loss of availability and integrity – backup mechanisms are applied; (iii) against loss of accountability – solutions that tie specific actions to a specific person or IT system are applied. **Data modification security.** Personal data are secured against	*Verlust der Vertraulichkeit geschützt durch: (i) sichere Zugangsauthentifizierungsmethoden für Personen und IT-Systeme; (ii) Überwachung der korrekten Funktionsweise und Verwendung sicherer Zugangsauthentifizierungsmethoden für Personen und IT-Systeme; (iii) regelmäßige (mindestens jährliche) Überprüfungen des Zugriffs aller Benutzer, Systemkonten, Testkonten und allgemeinen Konten werden durchgeführt und dokumentiert; (iv) Implementierung von Sitzungskontrollmechanismen, einschließlich Kontosperrung und Sitzungsablauf nach einer vorgegebenen Zeit.* ***Datentransfer- und Datenübertragungssicherheit.*** *Durch Fernübertragung übertragene personenbezogene Daten werden durch kryptografische Datenschutzmaßnahmen (Datenverschlüsselung während der Übertragung) und durch Segmentierung von IKT-Netzen (Netzsegmentierung) gegen Vertraulichkeits- und Integritätsverlust gesichert.* ***Sicherheit der Datenspeicherung.*** *Personenbezogene Daten, die auf Datenträgern gespeichert sind, sind gegen den Verlust der Vertraulichkeit, Verfügbarkeit und Integrität durch folgende Maßnahmen geschützt: (i) physische oder logische Datentrennung (Datentrennung); (ii) Echtzeit-Datenkopiermechanismen (Datenreplikation); (iii) Mechanismen zum Erstellen inkrementeller oder vollständiger Datensicherungen in vorbestimmten Zeitintervallen (Datensicherung); (iv) Mechanismen und Verfahren zur Datenwiederherstellung, Datenquellenumschaltung und Wiederherstellung von Sicherungen. In Datenbanken gespeicherte personenbezogene Daten werden durch Anwendung von Konsistenzregeln in Bezug auf Semantik (Definition des Datentyps), in Bezug auf Entitäten (Definition von Basisschlüsseln) und in Bezug auf Referenz (Definition von Fremdschlüsseln) gegen Integritätsverlust gesichert.* ***Sicherheit der Datenentwicklung.*** *Personenbezogene Daten sind geschützt: (i) gegen den Verlust der Vertraulichkeit - der Zugang wird nur autorisierten Personen und IT-Systemen gewährt; (ii) gegen Verlust der Verfügbarkeit und Integrität – Sicherungsmechanismen werden angewendet; (iii) gegen den Verlust der Rechenschaftspflicht – es werden Lösungen angewendet, die bestimmte Maßnahmen an eine bestimmte Person oder ein bestimmtes IT-System binden.*

Area / *Bereich*	Safety measures / *Sicherheitsmaßnahmen*	
	loss of confidentiality as access to the data is provided only to authorized persons and IT systems. Accountability of the personal data modification operations is ensured with solutions that permit tying specific actions to a specific person or IT system. **Data deletion security.** Personal data are secured against loss of confidentiality and availability through the provision of access to the data only to authorized persons and IT systems. Accountability of the personal data deletion operations is ensured with solutions that permit tying specific actions to a specific person or IT system.	***Sicherheit der Datenänderungen.*** *Personenbezogene Daten werden gegen Vertraulichkeitsverlust geschützt, da der Zugriff auf die Daten nur befugten Personen und IT-Systemen gewährt wird. Die Rechenschaftspflicht für die Vorgänge zur Änderung personenbezogener Daten wird mit Lösungen sichergestellt, mit denen bestimmte Aktionen an eine bestimmte Person oder ein bestimmtes IT-System gebunden werden können.* ***Sicherheit der Datenlöschung.*** *Personenbezogene Daten werden gegen den Verlust der Vertraulichkeit und Verfügbarkeit geschützt, indem nur befugten Personen und IT-Systemen Zugriff auf die Daten gewährt wird. Die Rechenschaftspflicht für Löschvorgänge von personenbezogenen Daten wird mit Lösungen sichergestellt, mit denen bestimmte Aktionen an eine bestimmte Person oder ein bestimmtes IT-System gebunden werden können.*
Physical security / *Physische Sicherheit*	**Security of personal data storage devices.** Personal data storage devices (documents, external data storage devices) are secured against unauthorized access through storage in office lockers with mechanical locks. The additional scope of the applied technical measures for the protection of personal data storage devices is established on a case-by-case basis, depending on the identified threats, the required degree of protection and the technical possibilities. **Security of the rooms where personal data are processed.** Rooms where personal data are processed are secured: (i) against unauthorized access – through application of mechanical locks, code locks, an access control system and a burglar alarm system; (ii) against destruction as a result of fire or flooding through application of a fire alarm and a burglar or attack alarm system. The additional scope of the implemented access control measures regarding access to rooms is established on a case-by-case basis, depending on the identified threats, the required degree of protection of the room and the technical possibilities. **Security of the buildings and areas where the rooms used for personal data processing are located.** The buildings and areas with the rooms used for personal	***Sicherheit von Speichergeräten für personenbezogene Daten.*** *Personenbezogene Datenspeichergeräte (Dokumente, externe Datenspeicher) werden durch Aufbewahrung in Büroschränken mit mechanischen Schlössern gegen unbefugten Zugriff gesichert. Der zusätzliche Umfang der angewandten technischen Maßnahmen zum Schutz personenbezogener Datenspeicher wird von Fall zu Fall festgelegt, abhängig von den erkannten Bedrohungen, dem erforderlichen Schutzgrad und den technischen Möglichkeiten.* ***Sicherheit der Räume, in denen personenbezogene Daten verarbeitet werden.*** *Räume, in denen personenbezogene Daten verarbeitet werden, sind gesichert: (i) gegen unbefugten Zugriff – durch Anwenden von mechanischen Schlössern, Codeschlössern, einem Zugangskontrollsystem und einem Einbruchmeldesystem; (ii) gegen Zerstörung durch Feuer oder Überschwemmung durch Anwendung eines Feuermelders und eines Einbruch- oder Angriffsmeldesystems. Der zusätzliche Umfang der durchgeführten Zutrittskontrollmaßnahmen für den Zugang zu Räumen wird von Fall zu Fall festgelegt, abhängig von den erkannten Bedrohungen, dem erforderlichen Schutzgrad des Raums und den technischen Möglichkeiten.* ***Sicherheit der Gebäude und Bereiche, in denen sich die Räume für die Verarbeitung personenbezogener Daten befinden.*** *Die Gebäude und Bereiche mit den zur Verarbeitung personenbezogener Daten genutzten Räumen sind durch den Einsatz von Zugangskontrollsystemen, eines Einbruch- und Angriffswarnsystems sowie durch die*

Area / *Bereich*	Safety measures / *Sicherheitsmaßnahmen*	
	data processing are secured against unauthorized access through application of access control systems, a burglar and attack alarm system, and surveillance by physical security guards. The internal and external zones where the rooms used for personal data processing are located are additionally secured to monitor and identify any threats or undesired events through the application of CCTV. The scope of the applied access control system measures for the buildings and areas with the rooms where personal data are processed is established on a case-by-case basis, depending on the identified threats, the required protection level for the building or zone and the technical possibilities.	*Überwachung durch physische Sicherheitskräfte gegen unbefugten Zugriff gesichert. Die internen und externen Zonen, in denen sich die für die Verarbeitung personenbezogener Daten verwendeten Räume befinden, sind zusätzlich gesichert, um Bedrohungen oder unerwünschte Ereignisse zu überwachen und zu identifizieren. Der Umfang der angewandten Maßnahmen des Zutrittskontrollsystems für die Gebäude und Bereiche mit den Räumen, in denen personenbezogene Daten verarbeitet werden, wird von Fall zu Fall festgelegt, abhängig von den erkannten Bedrohungen, dem erforderlichen Schutzniveau für das Gebäude oder der Zone und der technische Möglichkeiten.*
IKT-Sicherheit.	**Security of personal data storage devices.** The data storage devices used for personal data processing: (i) are secured against unauthorized access before their are installed in the hardware through access restriction and control using safes; (ii) are secured against loss of data confidentiality through the application of embedded procedures of cryptographic data protection (cryptographic protection of data storage devices); (iii) are secured against loss of availability through the application of systems for automated monitoring of performance, capacity utilization and availability time; (iv) are secured against unauthorized use with the procedures for use and configuration of IT infrastructure elements (configuration management); (v) intended for reuse are secured against data disclosure to any unauthorized person or IT system through the use of secure data deletion methods; (vi) intended for elimination are secured against reuse through permanent and deliberate mechanical destruction. **Security of the network infrastructure elements.** Elements of the network infrastructure used for personal data processing are secured: (i) against access by unauthorized persons and IT systems through secure access authentication methods; (ii) against access by unauthorized persons and IT systems and against loss of availability through monitoring of	***Sicherheit von Speichergeräten für personenbezogene Daten.*** *Die für die Verarbeitung personenbezogener Daten verwendeten Datenspeichergeräte sind: (i) vor dem Einbau in die Hardware durch Zugriffsbeschränkung und Kontrolle mit Tresoren gegen unbefugten Zugriff gesichert; (ii) durch die Anwendung eingebetteter Verfahren des kryptografischen Datenschutzes (kryptografischer Schutz von Datenspeichergeräten) gegen den Verlust der Vertraulichkeit von Daten gesichert; (iii) durch den Einsatz von Systemen zur automatisierten Überwachung von Leistung, Kapazitätsauslastung und Verfügbarkeitszeit gegen Verfügbarkeitsverlust gesichert; (iv) mit den Verfahren zur Nutzung und Konfiguration von IT-Infrastrukturelementen (Konfigurationsmanagement) gegen unbefugte Nutzung gesichert; (v) die Geräte, die zur Wiederverwendung bestimmt sind, durch die Verwendung sicherer Methoden zum Löschen von Daten gegen die Weitergabe von Daten an unbefugte Personen oder IT-Systeme gesichert sind; (vi) die Geräte, die zur Beseitigung bestimmt sind, sind durch dauerhafte und absichtliche mechanische Zerstörung gegen Wiederverwendung gesichert.* ***Sicherheit der Netzwerkinfrastrukturelemente.*** *Elemente der Netzwerkinfrastruktur, die für die Verarbeitung personenbezogener Daten verwendet werden, sind gesichert: (i) gegen den Zugriff durch nicht autorisierte Personen und IT-Systeme durch sichere Zugangsauthentifizierungsmethoden; (ii) gegen den Zugriff unberechtigter Personen und IT-Systeme und gegen den Verlust der Verfügbarkeit durch die Überwachung der Gültigkeit des Betriebssystems und der installierten Software; (iii) gegen den Zugriff*

Area / *Bereich*	Safety measures / *Sicherheitsmaßnahmen*	
	the validity of the operating system and the installed software; (iii) against access by unauthorized persons and IT systems and loss of availability with such software as Firewall, Intrusion Detection Systems, Intrusion Prevention Systems, Anti DDOS; (iv) against loss of availability through the application of replication, virtualization and automated scaling procedures, application of automatic availability, load and performance monitoring processes, application of backup power sources and automatic power source switching procedures, and application and procurement of support services provided by manufacturers and distributors. **Server security.** Servers used for personal data processing are secured: (i) against access by unauthorized persons and IT systems through the application of secure access authentication methods; (ii) against access by unauthorized persons and IT systems and against loss of availability through monitoring of the validity of the operating system and the installed software, and with such software as Firewall, Anti Virus; (iii) against loss of availability through the application of virtualization and automated scaling procedures, application of automatic availability, load and performance monitoring processes, application of backup power sources and automatic power source switching procedures, and application and procurement of support services provided by manufacturers and distributors. **Security of personal computers (desktop computers and laptops).** Personal computers used for personal data processing are secured: (i) against unauthorized access through the application of secure access authentication methods; (ii) against unauthorized access and loss of availability through monitoring of the validity of the operating system and the installed software, application of such software as Firewall, Anti Virus; (iii) against loss of availability through the application of backup power sources and automatic power	*durch nicht autorisierte Personen und IT-Systeme und den Verlust der Verfügbarkeit mit Software wie Firewall, Einbrucherkennungssystem, Einbruchsvorbeugungssystem, Anti-DDOS; (iv) gegen Verfügbarkeitsverlust durch Anwendung von Replikations-, Virtualisierungs- und automatisierten Skalierungsverfahren, Anwendung automatischer Verfügbarkeits-, Last- und Leistungsüberwachungsverfahren, Anwendung von Ersatzstromquellen und automatischen Stromquellenwechselverfahren sowie Anwendung und Beschaffung von bereitgestellten Unterstützungsdiensten von Herstellern und Händlern.* ***Serversicherheit.*** *Server, die für die Verarbeitung personenbezogener Daten verwendet werden, sind gesichert: (i) gegen den Zugriff nicht autorisierter Personen und IT-Systeme durch die Anwendung sicherer Zugangsauthentifizierungsmethoden; (ii) gegen den Zugriff durch nicht autorisierte Personen und IT-Systeme und gegen den Verlust der Verfügbarkeit durch Überwachung der Gültigkeit des Betriebssystems und der installierten Software sowie mit Software wie Firewall, Anti-Virus; (iii) gegen Verfügbarkeitsverlust durch Anwendung von Virtualisierungs- und automatisierten Skalierungsverfahren, Anwendung automatischer Verfügbarkeits-, Last- und Leistungsüberwachungsverfahren, Anwendung von Ersatzstromquellen und Verfahren zum automatischen Umschalten von Stromquellen sowie Anwendung und Beschaffung von Unterstützungsdiensten durch Hersteller und Händler.* ***Sicherheit von PCs (Desktop-Computern und Laptops).*** *PCs, die zur Verarbeitung personenbezogener Daten verwendet werden, sind gesichert: (i) gegen unbefugten Zugriff durch die Anwendung von Authentifizierungsmethoden für sicheren Zugriff; (ii) gegen unbefugten Zugriff und Verlust der Verfügbarkeit durch Überwachung der Gültigkeit des Betriebssystems und der installierten Software, Anwendung von Software wie Firewall, Anti-Virus; (iii) gegen den Verlust der Verfügbarkeit durch den Einsatz von Ersatzstromquellen und automatische Stromquellenumschaltverfahren, den Einsatz und die Beschaffung von Unterstützungsdiensten, die von Herstellern und Händlern bereitgestellt werden. Personalcomputer, die zur Verarbeitung personenbezogener Daten verwendet werden, sind in Datenspeichergeräten ausgestattet, die durch kryptografische Datenschutzmaßnahmen gesichert sind.* ***IKT-Netzwerksicherheit.*** *IKT-Netzwerke, die*

Area / *Bereich*	Safety measures / *Sicherheitsmaßnahmen*	
	source switching procedures, application and procurement of support services provided by manufacturers and distributors.. Personal computers used for personal data processing are equipped in data storage devices secured using cryptographic data protection measures. **ICT network security.** ICT networks used for personal data processing are secured: (i) against access by unauthorized persons and IT systems through secure access authentication methods; (ii) against access by unauthorized persons and IT systems and against loss of availability with such software as Firewall, Intrusion Detection Systems, Intrusion Prevention Systems, Anti DDOS; (iii) against loss of availability through multiplication of ICT links, application of automatic availability, load and performance monitoring processes, application of network devices backup power sources and automatic power source switching procedures, and application and procurement of support services provided by manufacturers and distributors of network devices and suppliers of ICT links.	*zur Verarbeitung personenbezogener Daten verwendet werden, sind gesichert: (i) gegen den Zugriff durch nicht autorisierte Personen und IT-Systeme durch sichere Zugangsauthentifizierungsmethoden; (ii) gegen den Zugriff durch nicht autorisierte Personen und IT-Systeme und gegen den Verlust der Verfügbarkeit mit Software wie Firewall, Einbruchsmeldesysteme, Einbruchsvorbeugungssysteme, Anti-DDOS; (iii) gegen Verfügbarkeitsverlust durch Multiplikation von IKT-Verbindungen, Anwendung automatischer Verfügbarkeits-, Last- und Leistungsüberwachungsprozesse, Anwendung von Sicherungsstromquellen für Netzwerkgeräte und Verfahren zum automatischen Umschalten von Stromquellen sowie Anwendung und Beschaffung von Unterstützungsdiensten, die von Herstellern und Händlern von Netzwerkgeräten und Anbietern von IKT-Verbindungen bereitgestellt werden.*