Annex 2 – Description of the implemented organizational and technical measures for personal data protection

Area	Safety measures
Information Security Management System	**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. **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

Area	Safety measures
	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 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 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

Area	Safety measures
	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.
Security of personal data processing operations	**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 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 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

Area	Safety measures
	ensured with solutions that permit tying specific actions to a specific person or IT system.
Physical security	**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 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.
ICT security.	**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 the validity of the operating system and

Area	Safety measures
	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 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.