|  |  |
| --- | --- |
| **2.3 Indicate the location of the Data Processing Center room**  Enter full address(s) | MS Azure Servers in Ireland and Netherland |
| **2.14 What is the Maturity level of PC Control.3 Privacy Compliance\_Data Breach Governance?**  **Description of the control:**   * Has the Supplier defined appropriate monitoring processes and tools in order to identify anomalous events in terms of security or potential internal and external attacks?   **Description of the effectiveness of the control:**   * indicate the specifications (e.g. tools used for monitoring, such as SIEM, DLP, etc.) |  |
| **2.20 What is the Maturity level of PC Control.9 Privacy Compliance\_Data Retention?**  **Description of the control:**   * has the Supplier implemented suitable tools to ensure the cancellation or return of all personal data following the performance of the services and / or services contracted with the Customer, unless regulatory obligations provide for the retention of the processed data? * does the Supplier guarantee the possibility of providing appropriate documentation proving the cancellation?   **Description of the effectiveness of the control:**   * indicate the specifications (e.g. identified criteria, flowcharts, definition of structured formats and data extraction methods for the response to the right of portability, etc.) |  |
| **2.21 What is the Maturity level of PC Control.10 Privacy Compliance\_DPIA?**  **Description of the control:**   * Has the Supplier put in place procedures to assist the Customer (Data Controller) in carrying out the data protection impact assessment? |  |
| **2.22 What is the Maturity Level of PC Control.11 Privacy Compliance\_Diritti Data Subjects?**  **Description of the control:**   * has a process been formalized that guarantees support to the Customer in managing the exercise of the rights of the interested parties?   **Description of the effectiveness of the control:**   * describe the process defined by the Supplier, adequately formalized in a specific procedure(s), for the management of requests for the exercise of rights by the interested parties, including the right to data portability, to provide adequate support to the Customer in the event that the requests refer to the data of ownership of the same * describe any supporting tools * describe roles and responsibilities involved |  |
| **2.23 Qual is the Maturity level of PC Control.12 Privacy Compliance\_PbD&D?**  **Description of the control:**   * Has a process been defined to ensure compliance with the principles of Privacy by Design and Privacy by Default?   **Description of the effectiveness of the control:**   * describe the ways in which the Supplier implements the principles of Privacy by Design and Privacy by Default |  |
| **3.1 Insert the network architecture**   * Provide a diagram of the architecture. * Describe the overall architecture and hosting networks required to provide the service. * Present the various infrastructure components used (routers, switches, firewalls, etc.) * Describe interconnections with external networks. |  |
| **3.2 Indicate the hardware used**   * List the hardware used for the provision of the service requested by the Customer: workstations, servers necessary for the operation of workstations, application servers, infrastructure components, etc. * For each resource, specify the vendor and describe the expected functions. * Specify whether servers are pooled with other customers or businesses. * If they are pooled, describe the measures taken to ensure the integrity and confidentiality of the Customer's data relating to the service. |  |
| **3.3 Indicate the software used**   * List the software used as part of the service provided. * Specify what elements are made available by the Service Provider and/or a Sub-Provider. * Describe the functions provided by the various software resources listed |  |
| **3.4 What is the Maturity Level of RM.1 Risk Management?**  **Description of the control:**   * does the Supplier adopt an IT Risk Management process, ensuring the carrying out and updating of the risk analysis, their assessment, and the treatment of residual risks?   **Description of the effectiveness of the control:**   * brief description of the IT Risk Management process, list of supporting documentation (methodology, policies, procedures) * brief description of the results emerged / summary illustration of the risk assessment with reference to the services carried out on behalf of the Client |  |
| **3.10 What is the Maturity level of GA.5 Access Management Control?**  **Description of the control:**  Are the following security measures provided for the applications used to access the Customer's proprietary data?   * disconnection following a fixed period of inactivity * account lockout following multiple failed attempts * limited maximum number of concurrent sessions for access to the application * session invalidated upon user log-off * generation of a new session ID against each new authentication. * any forms that require authentication credentials should not be pre-filled by the application   **Description of the effectiveness of the control:**   * describe which of the security requirements are implemented and complied with by the Supplier (by internal staff and third parties) |  |
| **3.11 What is the Maturity Level of THE GA.6 Control Minimization of the processing of personal data?**  **Description of the control:**   * are appropriate authorization profiles defined that allow access only to the information of competence (need to know), in line with the authorization process and with the needs of the Supplier? * consequently, is the processing of data allowed only to the subjects necessary and authorized to carry out the processing activities?   **Description of the effectiveness of the control:**   * ES. User management policy, the Privacy policy in which the principle of minimization is explained |  |
| **3.12 What is the Maturity level of the GA.7 Control Minimization of the processing of personal data?**  **Description of the control:**   * have methods been defined for masking/anonymization/pseudonymization of personal data in the face of the overturning of the Customer's ownership data present in the production environment in minor environments (testing, development, etc.)?   **Description of the effectiveness of the control:**   * indicate the specifications (e.g. presence of written procedures, tools used, methodologies adopted, etc.) |  |
| **3.13 What is the Maturity level of GA.8 System Administrators Control?**  **Description of the control:**   * are the System Administrators identified and appointed individually (Provision of the Privacy Guarantor of 27 November 2008 and subsequent amendments)? * Has the Supplier also activated a process for verifying the work of the System Administrators at least annually?   **Description of the effectiveness of the control:**   * describe the processes to support the verification activities carried out on system administrators |  |
| **3.14 What is the Maturity level of GA.9 System Administrators?**  **Description of the control:**   * are suitable systems adopted for the registration of logical access (computer authentication) to processing systems and electronic archives by System Administrators? * in particular, has the Supplier provided for the tracking and storage for at least 6 months of the logs of accesses and events of users with special privileges (eg administrative users) that access the data of ownership of the Customer and that these logs have characteristics of completeness, inalterability and possibility of verifying their integrity and include the time references and the description of the event?   **Description of the effectiveness of the control:**   * indicate the specifications (e.g. presence of written procedures, characteristics of the logs, retention, which tools are involved, etc.) * in particular, indicate whether the records of the System Administrators (access logs) have characteristics of completeness, inalterability, and possibility of verifying their integrity adequate to achieve the purpose of verification for which they are required |  |
| **3.21 What is the Maturity Level of SRS Control.1 Network and Systems Security?**  **Description of the control:**   * does the Supplier periodically implement Technical Risk Assessment activities (e.g., Vulnerability Assessment, Penetration Test) on systems (including systems that process personal data)?   **Description of the effectiveness of the control:**   * describe whether a formalised process is defined for periodic and event-based development (e.g. at each new project initiative that has a high impact on ICT systems, or in case of significant changes in IT systems) * indicate whether the process is carried out periodically and is formally documented through predefined templates * indicate whether a Penetration Test is carried out annually on the exposed transnational services * indicate whether periodically, at least annually, verification activities (e.g. Vulnerability Assessment and Penetration Test) are carried out by qualified and independent third-party companies regarding the presence of vulnerabilities on network systems and infrastructures * indicate the specifications (e.g. presence of written procedures, name of suppliers carrying out VA/PT, periodicity and method of action, etc.) |  |
| **3.22 What is the Maturity Level of SRS Control.2 Network and Systems Security?**  **Description of the control:**   * Are security patches and fixes for known system vulnerabilities, released by manufacturers, promptly tested and implemented by Vendor while minimizing vulnerability exposure time?   **Description of the effectiveness of the control:**   * Are software upgrade priorities and installation times defined? * Is a log kept of patches and their patched systems? * has the internal legislation to support these activities been defined? |  |
| **3.23 What is the Maturity Level of SRS Control.3 Network and Systems Security?**  **Description of the control:**   * has the Supplier defined and implemented a change management process to ensure that no unauthorized changes are made to the systems (e.g. tickets, etc.)? * are any changes to the configuration of the information systems supporting the processing carried out on behalf of the Customer tracked, stored, as well as protected from unauthorized changes (e.g. made unchangeably)?   **Description of the effectiveness of the control:**   * indicate the specifications (e.g. presence of written procedures, methods of tracking and storing logs, tools used, etc.) |  |
| **3.24 What is the Maturity Level of SRS Control.4 Network and Systems Security?**  **Description of the control:**   * Has the Supplier defined backup procedures aimed at ensuring the availability of the Customer's proprietary data and the possibility of recovery in the event of harmful events within a time compatible with what is defined in the Service Level Agreements (SLA)?   **Description of the effectiveness of the control:**   * indicate the presence of internal legislation to support * indicate whether the backups are stored in a secure manner in order to ensure the availability of the data owned by the Customer and if their access is limited only to authorized personnel (e.g. indicate the measures to protect the places where the backups of the data are processed on behalf of the Customer are stored) * indicate whether the Supplier carries out, on a periodic basis (at least annually), a restoration test of the information being backed up in order to verify the actual possibility of recovery |  |
| **3.26 What is the Maturity Level of SRS Control.6 Network and Systems Security?**  **Description of the control:**   * are security measures implemented at the perimeter level through appropriate tools (e.g. firewalls and IDS/IPS) in order to filter out abnormal traffic and prevent, where possible, attacks from outside or by unauthorized internal parties?   **Description of the effectiveness of the control:**   * indicate the specifications (e.g. presence of written procedures, list of perimeter security measures implemented, etc.) * indicate whether they are used for example: IDS - NIDS, HIDS, hybrid IDS; IPS (NIPS,WIPS,NBA, HIPS) * DoS, DdoS security policies have been created including a response plan to detected incidents * ISPs that implement DdoS security measures are used |  |
| **3.27 What is the Maturity Level of SRS Control.7 Network and Systems Security?**  **Description of the control:**   * does external access to systems and applications that process customer ownership data take place through Strong Authentication with at least one double authentication factor (e.g. UserID, password and OTP)?   **Description of the effectiveness of the control:**   * indicate specifications (e.g. presence of written procedures) * if the control is not implemented, explain the reasons/justifications for the exclusion of control |  |
| **3.28 What is the Maturity Level of SRS Control.8 Network and Systems Security?**  **Description of the control:**   * is the network appropriately segregated in such a way as to guarantee adequate protection to critical systems that process the data owned by the Customer?   **Description of the effectiveness of the control:**   * indicate the specifications (e.g. presence of written procedures, if the web servers are located within appropriate DMZs, etc.) |  |
| **3.29 What is the Maturity Level of SRS Control.9 Network and Systems Security?**  **Description of the control:**   * for all communications involving the Customer's proprietary data transmitted over public or third-party networks, are advanced encryption techniques used (e.g. TLS protocols, HTTPS, etc.)?   **Description of the effectiveness of the control:**   * indicate the specifications (e.g. presence of written procedures, encryption techniques adopted, any reasons that have led to the use of protocols that guarantee different levels of security) |  |
| **3.30 What is the Maturity Level of SRS.10 Network and Systems Security?**  **Description of the control:**   * Has the Supplier adopted encryption techniques to protect the Customer's proprietary data on systems, applications, DBs, removable media and PCs, as well as adequate guarantees for the protection of encryption keys?   **Description of the effectiveness of the control:**   * indicate the specifications (e.g. presence of written procedures, encryption techniques adopted and on which tools, what measures have been taken to protect encryption keys, etc.) * indicate the specifications (e.g. presence of written procedures, on which systems authentication, encryption and encrypted storage of the password is implemented, etc.)   **3.31 What is the Maturity level of BCM.1 Business Continuity Management?**  **Description of the control:**   * Has the Supplier adopted a Business Continuity plan that complies with industry standards?   **Description of the effectiveness of the control:**   * in the BCP the Supplier should describe which scenarios were considered during the analysis and the corresponding solutions (both organizational and technological) * the Supplier, in the event that it is requested by the Customer, must communicate the lists of those responsible (names and relative contact details) for the management of emergency situations |  |
| **3.32 What is the Maturity level of BCM.2 Business Continuity Management?**  **Description of the control:**   * Has the Supplier defined a Disaster Recovery plan?   **Description of the effectiveness of the control:**   * the Disaster Recovery site is located at a sufficient distance from the Primary site and manned * there are formalized recovery plans * there are processes to verify at regular time intervals, through DR tests, the recovery plan, in order to guarantee its effectiveness in case of disastrous events   **3.34 What is the CS.2 Cloud Security Control Maturity Level (if applicable)?**  **Description of the control:**   * with specific reference to the activities entrusted in the cloud, are there adequate mechanisms for isolating the data owned by the Customer with respect to data of other customers, to guarantee their confidentiality and integrity?   **Description of the effectiveness of the control:**   * indicate the specifications (e.g. description of the isolation mechanisms implemented) |  |
| **3.35 What is the CS.3 Cloud Security Control Maturity Level (if applicable)?**  **Description of the control:**   * with specific reference to the activities entrusted in the cloud, does the Supplier never use Sub-suppliers without having first requested specific written authorization from the Customer, assuming specific responsibilities in case of unauthorized subcontracting?   **Description of the effectiveness of the control:**   * indicate specifications (e.g. presence of written procedures) |  |
| **3.36 What is the Maturity level of CS.4 Cloud Security Control (if applicable)?**  **Description of the control:**   * with specific reference to the activities entrusted in the cloud, has the Supplier implemented mechanisms to allow the definitive cancellation and / or return of the Customer's ownership data that have been entrusted to it, in accordance with the defined retention times and the contractual agreements stipulated?   **Description of the effectiveness of the control:**   * indicate the specifications (e.g. presence of written procedures, mechanisms adopted, etc.) |  |
| **3.37 What is the CS.5 Cloud Security Control Maturity Level (if applicable)?**  **Description of the control:**   * with specific reference to the activities entrusted in the cloud, is the Supplier able to provide attestations and guarantees aimed at ensuring that the Customer's ownership data present in the cloud will be kept in compliance with the agreed purposes and methods, excluding duplication and communications to third parties?   **Description of the effectiveness of the control:**   * indicate specifications (e.g. written procedures, guarantees and attestations) |  |