Implemented Controls and PRIVaaS Framework based on LGPD and GDPR

ID	Name	Glossary/Explanation	Controls and PRIVaaS Objectives	LGPD Requirements	GDPR Requirements
1	Confidentiality Agreement	Protects the rights over information exchanged during negotiations and service execution	Mitigating unauthorized data access risks in data mining processes.	Security Principle: Art. 6, Item VII – Adequate security against unauthorized access	Art. 5(1)(f) – Integrity and confidentiality
2	Team Training and Awareness	Keeps the team updated with best security and privacy practices	Keeps team skilled in privacy-preserving techniques, minimizing re-identification risks throughout processes.	Prevention Principle: Art. 6, Item VIII – Prevention of damage	Art. 39(1)(a) – Awareness and training
3	Create Specific Cloud Instance	Segregation of servers within the cloud environment to ensure security	Isolates sensitive data processing within dedicated environments, enhancing compliance with PRIVaaS data segregation requirements.	Security Principle: Art. 6, Item VII – Protection in a secure environment	Art. 32(1)(b) – Security of processing
4	Databricks Security Controls	Implementation of robust security controls in the Databricks platform	Implementing an environment guided by PRIVaaS standards ensures robust security measures in data processing environments.	Security Principle: Art. 6, Item VII – Integrity and confidentiality of data	Art. 32(1) – Security of processing
5	Segregation of Duties	Implementation of SoD to prevent power abuses	Enforces role-based access to data, preventing unauthorized access and ensuring compliance with security mandates.	Security Principle: Art. 6, Item VII – Minimization of unauthorized access risks	Art. 5(1)(f) – Integrity and confidentiality
6	Databricks Configuration by Specialist	Ensures configurations are done by certified specialists for security and privacy	Configurations aligned with privacy and security standards, meeting compliance needs for safe data handling.	Accountability Principle: Art. 6, Item X – Good practices and governance	Art. 24(1) – Responsibility of the controller
7	Certifications of Specialists	Ensures professionals have the necessary certifications	Configurations aligned with privacy and security standards meet compliance needs for safe data handling. Re-identification risk analysis verifies that these technical skills are sufficient.	Accountability Principle: Art. 6, Item X – Qualification of professionals	Art. 24(1) – Responsibility of the controller
8	Regular Audits	Audits conducted by specialized companies and Internal Compliance	Provides ongoing evaluation of data privacy measures, reinforcing PRIVaaS's goal of maintaining secure and compliant data processes.	Accountability and Reporting Principle: Art. 6, Item X – Audits for compliance	Art. 39(1)(b) – Monitoring and audits
9	PAM Tool	Manages privileged access and records user sessions for future audits	PRIVaaS manages privileged access, enhancing security and ensuring that data access complies with privacy regulations.	Security Principle: Art. 6, Item VII – Access control and activity monitoring	Art. 32(1) – Security of processing
10	Record Data Transfer via Video	Records data transfer to cloud servers	Synergy with PRIVaaS and PAM manages privileged access, enhancing security and ensuring data access compliance with privacy regulations for users needing to manipulate raw data.	Accountability and Reporting Principle: Art. 6, Item X – Operation documentation	Art. 30(1) – Records of processing activities
11	Store Copy in Secure Location	Ensures data is stored in a secure location with appropriate measures	Ensures data storage compliance by keeping sensitive information in controlled environments, mitigating privacy risks highlighted by PRIVaaS. Enables application at anonymization levels.	Security Principle: Art. 6, Item VII – Protection against unauthorized access	Art. 32(1) – Security of processing
12	Destroy Base After Secure Copy	Ensures data is securely stored and then destroyed	Enforces data lifecycle management aligned with PRIVaaS principles, reducing risks of re-identification post-analysis.	Accountability Principle: Art. 6, Item X – Secure data elimination	Art. 5(1)(e) – Storage limitation
13	Initial Audit for Databricks Logs	Initial verification of active logs in the Databricks platform	Audits log data to ensure compliance and monitor access, aligning with privacy preservation goals. Importanto for check if PRIVaaS Framework is correctly applied.	Accountability and Reporting Principle: Art. 6, Item X – Continuous monitoring	Art. 30(1) – Records of processing activities
14	Verify Logs After Data Update	Log verification after each data update process	Important for check if PRIVaaS Framework and all controls are correctly applied.	Transparency Principle: Art. 6, Item VI – Maintenance of clear records	Art. 30(1) – Records of processing activities
15	Formal Databricks Training	Provides formal training on the Databricks platform	Provides formal training on secure data configurations. Educates teams on privacy-preserving data configurations within Databricks, necessary for fulfilling PRIVaaS guidelines Framework.	Accountability Principle: Art. 6, Item X – Training and qualification	Art. 39(1)(a) – Awareness and training
16	Login restrict from corporate devices	Restricts access to corporate devices to ensure security	Enhances data security by limiting access points, crucial for maintaining PRIVaaS integrity.	Security Principle: Art. 6, Item VII – Prevention of unauthorized access	Art. 32(1) – Security of processing
17	DLP - Data Leak Prevent	Tool to prevent data loss, identifying information leaks	Prevents unauthorized data sharing, directly supporting PRIVaaS's emphasis on minimizing data leakage risks.	Security Principle: Art. 6, Item VII – Protection against data loss	Art. 32(1) – Security of processing
18	VLANs Segmentation	Network segmentation to isolate Databricks from other networks	Isolates data traffic to secure zones, protecting sensitive data flows as per PRIVaaS recommendations.	Security Principle: Art. 6, Item VII – Network segregation for security	Art. 32(1) – Security of processing
19	Block USB Ports	Prevents data transfer to portable devices	Prevents unauthorized data extraction via physical devices, a critical aspect of maintaining PRIVaaS data security.	Security Principle: Art. 6, Item VII – Prevention of data leaks	Art. 32(1) – Security of processing
20	Disk Encryption	Encryption to protect data against unauthorized access in case of device theft or loss	Protects data stored on devices, ensuring alignment with PRIVaaS requirements for data at rest security.	Security Principle: Art. 6, Item VII – Protection against unauthorized access	Art. 32(1)(a) – Pseudonymization and encryption of personal data
21	Information Classification per MIP	Data classification to ensure secure use and auditing	Categorizes data based on sensitivity, crucial for applying and automatize PRIVaaS anonymization and protection measures effectively.	Accountability Principle: Art. 6, Item X – Data classification for security	Art. 30(1) – Records of processing activities
22	Communicate Processing to ANPD	Legal requirement to communicate data processing to ANPD	Legal compliance step necessary for PRIVaaS alignment, ensuring data processing is transparent and regulated.	Transparency Principle: Art. 6, Item VI – Communication to national authority	Art. 33 – Data transfer outside the EU
23	Define Legal Basis for Data Processing	Ensures data can be shared according to a legal basis	PRIVaaS supports the necessary legal compliance steps, ensuring that data processing is transparent and regulated, which mitigates liability for incidents.	Lawfulness Principle: Art. 7 – Legal bases for data processing	Art. 6(1) – Lawfulness of processing
24	Data Protection Impact Assessmet	DPIA to demonstrate data collection, processing, usage, and risk mitigation	PRIVaaS assesses privacy risks to ensure compliant data practices, aligning with privacy and security needs.	Accountability Principle: Art. 6, Item X – Demonstration of risk mitigation measures	Art. 35 – Data protection impact assessment
25	Data Inventory	Maintain an updated inventory of personal data	Maintains data visibility and inventory, essential for privacy management and compliance with PRIVaaS requirements.	Transparency Principle: Art. 6, Item VI – Maintenance of clear records	Art. 30(1) – Records of processing activities
26	Data Anonymization in Process Phases	Removal or modification of information that identifies a person	PRIVaaS applies anonymization during ETL and processing to prevent re-identification and ensure privacy compliance.	Security Principle: Art. 6, Item VII – Protection of anonymized data	Art. 32(1) – Security of processing
27	Data Encryption in Transit and at Rest	Protection of data in transit and storage with encryption	Secures data throughout its lifecycle, meeting PRIVaaS's stringent security standards. PRIVaaS secures data throughout its lifecycle, ensuring compliance with encryption standards.	Security Principle: Art. 6, Item VII – Protection of data in transit and at rest	Art. 32(1)(a) – Pseudonymization and encryption of personal data
28	Hashing of CPF and CNPJ	Transformation of input data into unique hash values to protect identities	PRIVaaS secures data throughout its lifecycle, meeting stringent security and encryption standards. Applied Anonymization Techniques.	Security Principle: Art. 6, Item VII – Protection against identification of data subjects	Art. 32(1) – Security of processing
29	Secure Link	Use of encrypted links for secure data sharing	Uses secure links and encryption in transit for data sharing, ensuring PRIVaaS compliance and protection against unauthorized access.	Security Principle: Art. 6, Item VII – Protection of data traffic	Art. 32(1) – Security of processing
30	Isolated from the Internet	Servers without internet connection to prevent data leaks	PRIVaaS restricts external access to data environments, enhancing security and meeting privacy standards.	Security Principle: Art. 6, Item VII – Isolation of servers for security	Art. 32(1) – Security of processing
31	Network Configuration	Network configurations to block unauthorized access to the platform	Configures networks to block unauthorized access, supporting PRIVaaS security in data handling	Security Principle: Art. 6, Item VII – Access control and network security	Art. 32(1) – Security of processing
32	Multi-Factor Authentication	Use of multiple factors to confirm user identity	PRIVaaS strengthens access control with multi-step authentication, ensuring only authorized access to sensitive data.	Security Principle: Art. 6, Item VII – Verification of user authenticity	Art. 32(1) – Security of processing