

Information Security Practices

Content		Page
I.	Applicability of Information Security Standards	1
II.	Policies, Procedures and Certifications	1
III.	Measure Category and Broadcom Controls	2
IV.	Overview of Broadcom’s Technical and Organizational Measures as they relate to EU Law, Guidance and Jurisprudence	11

The content contained herein represents the status quo as of the date of publication. Our security policies and procedures are subject to change without further notice, as the technology and/or threat landscape evolve.

I. Applicability of Information Security Standards

The applicability and scope of various standards (and corresponding controls) may differ with respect to the requirements of a specific business unit, service, product or specific engagement (e.g., controls requirements for “on premise” solutions may differ from requirements for hosted, cloud-based, service offerings). Even though Broadcom’s information security controls align with many leading industry standards, Broadcom adopts a standards neutral approach in its commitment towards information security. Therefore, controls and standards referenced herein reflect a “minimum” standard of policies and procedures and are intended to provide a general confirmation of implementation of such standards across applicable Broadcom products and solutions.

II. Policies, Procedures and Certifications

Policies and procedures that regulate the use of information, including its processing, receipt, transmission, storage, distribution, access and deletion (“**Policies and Procedures**”), are documented and implemented, and address how confidential information is managed, and protected. Policies and Procedures are designed to comply with all applicable laws, rules and regulations in the countries in which Broadcom conducts business. The Policies and Procedures are approved by senior management, reviewed and updated to remain compliant with applicable law and current industry practices.

III. Measure Category and Broadcom Controls

Measure Category	Broadcom Controls
Measures of pseudonymization and encryption of personal data	<p>Broadcom follows industry standard practices regarding encrypting data in transit and at rest. Broadcom systems use encryption to protect transmitted records and files containing data that will travel across public networks, with encryption at a strength that is commercially reasonable given the nature of the data transmitted and the transmission method(s). Broadcom requires that systems used to process sensitive data, including personally identifiable information (PII), passwords, account information, etc., support encryption when in transit on the network and implement industry-standard practices regarding encryption of sensitive data stored at rest. Encryption use and applicable encryption standards are documented. The encryption strength of confidential information in transmission is defined. Cryptographic key management procedures are documented and automated. Products or solutions are deployed to keep the data encryption keys encrypted.</p>
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	<p>Broadcom continuously gathers and analyses information regarding new and existing threats and vulnerabilities, actual attacks on the organization or others, and the effectiveness of the existing security controls. Monitoring controls include related policy and procedure, virus and malicious code detection, intrusion prevention and detection, and event and system health and state monitoring. Related logging process provides an effective control to highlight and investigate security events.</p> <p>Robust controls are implemented over Broadcom communication networks to safeguard data, tightly control access to network devices through management approval and subsequent audits, disable remote communications if no business need exists, log and monitor remote access, secure remote access devices, and use strong authentication and encryption to secure communications. Defined Access Control Lists (ACLs) to restrict traffic on routers and/or firewalls are reviewed and approved by network administrators. IP addresses in the ACLs are specific and anonymous connections are not allowed. Only authorized devices connect to the Broadcom internal networks.</p> <p>Firewall management processes are documented. All changes to the firewall are performed via change management processes. Firewall access is restricted to a small set of super users/administrators with appropriate approvals.</p> <p>Periodic network vulnerability scans are performed, and any critical vulnerabilities identified are promptly remediated.</p> <p>Broadcom ensures that any personnel authorized by Broadcom to process Customer data is subject to an obligation of strict confidentiality. Broadcom personnel are required to agree to confidentiality obligations as a condition of employment.</p>

Measure Category	Broadcom Controls
<p>Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident</p>	<p>Protection against fire and measures in case of power outages are implemented in the data processing centers including backup.</p> <p>Effective controls are in place to protect against physical penetration by malicious or unauthorized people. Physical controls covering the entire facility are documented. Additional access restrictions are enforced for server/computer/telecommunications rooms compared to the general area.</p> <p>Components supporting the physical and environmental security plan are based on the nature of the facility (e.g. data center, office facility) and include: Climate control systems; Thermostat sensors; Raised floors; Smoke detectors; Heat detectors; Vibration alarm sensors; Fluid or water sensors; CCTV installation points; Fire suppression systems; Wireless access points; Entrance points of the facility; Uninterruptible power supplies (UPS); Batteries; Generators.</p> <p>Backup, redundancy/failover and offsite storage procedures are documented, and include Business Continuity and Disaster Recovery procedures. Procedures encompass the ability to fully restore or utilize redundant platform resources for applications and operating systems. Periodic testing of successful restoration from backup media and redundant failover solutions are demonstrated. The on-site staging area has documented and demonstrated environmental controls (e.g., humidity, temperature).</p>
<p>Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing</p>	<p>Cloud Offerings are subject to third party audits at least once per year during the term of the applicable governing agreement under Statement on Standards for Attestation Engagements (SSAE) No. 18, Reporting on Controls at a Service Organization ("SSAE 18") published by the American Institute of CPAs (AICPA). For those audits under SSAE 18, the resulting Service Organization Controls (SOC) Report includes: the auditor's opinion on the fairness of the presentation of Broadcom's description of controls that have been placed in operation, the suitability of the design of the controls to achieve the specified control objectives, and the auditor's opinion on whether the specific controls were operating effectively during the period under review. Additionally, the specific audit conducted depends on the applicable Cloud Offering and may include ISO 27001, ISO 27017, ISO 27018, SOC2, SOC3, HIPAA, PCI, IRAP, ISMAP, OSPAR, FedRAMP, and any other industry assessments and certifications which will be periodically renewed as appropriate. Broadcom certifications are available at https://www.broadcom.com/support/saas/compliance-audit-reports and VMware certifications are available at www.vmware.com/products/trust-center.html.</p>
<p>Measures for user identification and authorization</p>	<p>Authentication and authorization controls are appropriately robust for the specific levels of risk to the information, data, application and platform. Access rights are monitored to ensure that access adheres to the 'least privilege' principle commensurate with the user's job responsibilities. All access and security events are logged, and software is used that enables rapid analysis of, and anomaly detection in user activities. Access Control policy and corresponding procedures are documented. The access procedures define the request, approval, access provisioning, and de-provisioning, and monitoring processes. The access processes restrict user access (local or remote) based on user job function (role/ profile based, appropriate access) for applications, databases and systems to ensure segregation of duties.</p>

Measure Category	Broadcom Controls
	<p>End user access to data is only possible through application authorization. End users are logically and/or physically separated from back-end data. User access reviews are performed periodically (e.g., quarterly) for business-critical applications, to confirm that permissions and privileges are appropriate. Procedures are documented for the timely onboarding and off-boarding of users who have joined, left, or changed roles within the organization.</p> <p>The process for the management of privileged user accounts is defined. Organizational responsibility for the creation of privileged accounts is separate from general users (based on organization size). A review/governance process is in place and privileged accounts are reviewed periodically (e.g., quarterly) to ensure that access is restricted, appropriate and documented (requests, approvals) prior to account creation.</p> <p>Remote control of desktops is restricted to specific roles (e.g., helpdesk admin) and remote control is permitted only after the end user gives permission and until the end of the support session. Unauthorized remote connections from devices are disabled as part of standard configuration. The data flow in the remote connection is encrypted and multi-factor authentication is utilized during the login process. Dependent third-party service provider (i.e., subcontractor) remote access adheres to the same or similar controls, and any subcontractor remote access is based on documented valid business justification.</p> <p>Documented password policy covers all applicable systems, applications, and databases. Password best practices are deployed to protect against unauthorized use of passwords. The password policy includes the following components: Password is communicated separately from user ID; Password expiration; Password is not shared; Initial password generated is random; Forced initial password change; Minimum password length; Password complexity; Password history; Password lockout for failed password attempts. Passwords are saved only as one-way hash/encrypted files. Access to password files is restricted only to system administrators. If the authentication engine for application fails, the default action is always to deny access.</p>
<p>Measures for the protection of data during transmission</p>	<p>Confidential information transmission over the public internet always utilizes an encrypted channel. Encryption details are documented if transmission is automated. If manual encryption is required, approved and dedicated staff is responsible for encrypting/decrypting the data. Confidential information is encrypted while in transit over any network using secure protocols like HTTPS, SSL, SFTP, etc. VPN transmissions are performed over an encrypted channel. Electronic transmission of data to and from off-site locations is performed over an encrypted channel. Mobile computing (where permitted) is performed exclusively over encrypted channels. Wireless Access Points only allows authorized users to connect.</p> <p>Policies and procedures are established and adhered to for proper control of electronic mail and/or instant messaging systems. Preventative and detective controls block malicious e-mails/ attachments. Policy prohibits auto-forwarding of emails. Emails are encrypted via Transport Layer Security (TLS). Further acceptable solutions for email encryption include commercial options such as Pretty Good Privacy (PGP). Encryption technology used adheres to all legal requirements governing the use of such technology.</p> <p>Established controls exist to help protect customer data gathered via website applications hosted, developed, or supported by Broadcom. Multi-tiered architecture is established where the web presentation, business logic and data tier are separated into distinct servers and network zones. Website design forces removal of cached</p>

Measure Category	Broadcom Controls
	<p>data as part of the process upon session termination. Multi-factor authentication or IP address restriction is required to login if customer data is accessible through the website. Periodic penetration testing is performed against the website. Penetration tests include the following attributes: Cross Site Scripting (XSS); Injection flaws; Malicious file execution; Insecure direct object reference; Cross Site Request Forgery (CSRF); Information leakage and improper error handling; Broken authentication and session management; Insecure cryptographic storage; Insecure communications; Failure to restrict URL access. Monitoring tools/ solutions are in place to monitor website uptime. Restrictions are placed on web server resources to limit denial of service (DoS) attacks.</p> <p>Policies are defined and enforced for the safe and secure disposal and transmission of media containing confidential information in accordance with DoD and/or NIST standards wherever applicable.</p>
<p>Measures for the protection of data during storage</p>	<p>Servers and devices containing confidential information are encrypted leveraging system level encryption.</p> <p>Use of any portable media (e.g., laptops, removable hard drives, flash drives, removable disks, or tapes) is restricted, and the use of USB storage devices is prohibited in Broadcom environments. Customer information is not stored on any unencrypted portable media.</p> <p>Backup storage devices (e.g., flash drives, CD, DVD, authorized USB devices, backup tapes) are encrypted. Secure transportation procedures (e.g., inventory tracking, signed checklists) of media to and from off-site location are defined.</p>
<p>Measures for ensuring physical security of locations at which personal data are processed</p>	<p>Physical access to facilities where data is processed is restricted through the use of access control procedures for authorized users (e.g., badge access, security guards, etc.). Visitor access must be logged in a physical access log and visitors are escorted through restricted areas in the facility. Physical security plan for offsite facilities is documented. Access control is enforced at entry points and in storage rooms. Access to the off-site facility is restricted and there is an approval process to obtain access.</p> <p>Monitoring cameras (e.g., CCTVs) cover sensitive areas within the facility. The monitoring equipment (e.g., CCTV) feed is monitored by a qualified team. Alerting procedures are defined and notification is given to qualified personnel.</p> <p>Security guards are trained regarding their response to security events. Security guards perform periodic patrols of the facilities and restricted areas.</p> <p>All employment candidates, contractors and third parties are subject to background validation checks in accordance with applicable laws and regulations.</p> <p>Clean desk/clear screen policy is defined and enforced. Workstations are secured with access to the screen locked during prolonged absences during the day. Documents containing confidential information are secured in a locked file cabinet or office with access granted to only those individuals with a business need for such information. Offices, desks, and file cabinets are locked at the close of business.</p>

Measure Category	Broadcom Controls
Measures for ensuring events logging	<p>Security events are logged, monitored and addressed through timely and documented action. Network components, workstations, applications and monitoring tools are enabled to monitor and detect anomaly in user activity. Organizational responsibilities for responding to events are defined. Configuration checking tools and logs are utilized to record critical system configuration changes. The log permission restricts alteration by administrators. Retention schedules for various logs are defined and enforced.</p> <p>Servers, workstations and internet gateway devices are updated periodically with latest antivirus definitions that include zero-day anti-malware protection. Defined procedure highlights all anti-virus updates. Anti-virus tools are configured to run weekly scans, virus detection, real time file write activity and signature files updates. Laptops and remote users are covered under virus protection. Procedures to detect and remove any unauthorized or unsupported (e.g., freeware) applications are documented. Alert events include the following attributes: Unique identifier; Date; Time; Priority level identifier; Source IP address; Destination IP address; Event description; Notification sent to security team; Event status.</p>
Measures for ensuring system configuration, including default configuration	<p>Information systems are deployed with appropriate security configurations and reviewed periodically for compliance with security policies and standards.</p> <p>Standard security configuration is documented. Security hardening and procedures include security patches, vulnerability management, avoidance of default passwords, registry settings, and file directory rights and permissions.</p> <p>Security patch process and procedures, including patch prioritization, are documented.</p> <p>Penetration testing of the external perimeter is performed at least annually. For most recent testing results/report, follow-up is performed to eliminate or mitigate any issues rated as critical, high and medium risk. Tools/processes are in place to perform vulnerability monitoring, penetration testing, antivirus definition updates, firewall deployment and maintenance, application gateway (proxy) and guard testing.</p> <p>Documented operating system versions are implemented. Minimum Security Baselines (MSB) are established for various operating systems and versions. Multiple simultaneous logins to the environment are not allowed for any single administrator.</p>
Measures for internal IT and IT security governance and management	<p>Policies and procedures that regulate the use of information, including its processing, receipt, transmission, storage, distribution, access and deletion ("Policies and Procedures") are documented and implemented, and address how confidential information is managed and protected. Policies and Procedures are designed to comply with all applicable laws, rules and regulations in the countries in which Broadcom conducts business. The Policies and Procedures are approved by senior management, reviewed and updated to remain compliant with the law and current industry practices.</p> <p>IT operational procedures ensure secure operation of its IT assets. Operational procedures are documented and successfully executed. The operation procedures include the following components: Scheduling requirements; Handling errors (e.g., transport of data, printing, copies); Generating and handling special output;</p>

Measure Category	Broadcom Controls
	<p>Maintenance and troubleshooting of systems; Documented procedures to manage the SLAs/KPIs and the reporting structure for escalations.</p> <p>Problem Remediation Management Process/Procedures are documented. The problem management lifecycle includes the following discrete steps: Identification; Assignment of severity to each problem; Communication; Resolution; Training (if required); Testing/validation; Reporting.</p> <p>Changes to systems, networks, applications, data files structures, other system components, and physical/environmental changes are monitored and controlled through a formal change control process. Changes are tested, reviewed, approved and monitored during post-implementation to ensure that expected changes are operating as intended.</p> <p>The change management policy covers all changes to applications, operating systems and network infrastructures, including firewalls. Emergency change management procedures are specified, including factors leading to emergency change. The change management policy/procedure includes the following attributes: Clearly identified roles and responsibilities, including separation of duties; Impact or risk analysis of the change request; Testing prior to implementation of change; Security implications review; Authorization and approval; Post-installation validation; Back-out or recovery plans; Management sign-offs; Post-change review and notification.</p> <p>Emergency change procedures have stated roles and responsibilities for request and approval. The procedures include a post-change implementation validation. The procedures include post-emergency change documentation update.</p>
<p>Measures for certification/assurance of processes and products</p>	<p>There is an established Secure Software Development Life Cycle (“SSDLC”) Policy for defining, acquiring, developing, enhancing, modifying, testing and implementing information systems. Software Development Life Cycle (SDLC) methodology is documented and includes version control and release management procedures. SDLC methodology also includes validation of security requirements (e.g. Information Security [IS] sign-offs, periodic IS reviews, static/dynamic scanning). System documentation is managed by appropriate access controls. Code certification is performed to include security review when code is developed by third parties. Software vulnerability assessments are conducted internally or using external experts. Any vulnerability gaps identified are remediated in a timely manner. Developer access to production environments is restricted by policy and in implementation.</p> <p>All product teams are required to follow Broadcom's Secure Development Procedure which provides security standards, strategies and tactics for each phase of the product development lifecycle. These procedures include guidelines and requirements on what, when and how security activities should take place. Specifically, they include activities for all phases of the Secure Software Development Lifecycle, such as Training, Coding Guidelines, Architectural Risk Analysis, Code Analysis, Penetration Testing, as well as Vulnerability Response. In addition, Broadcom has processes to build privacy into products and services from the initial design phase and continuously improves its Privacy by Design (PbD) and Privacy by Default practices.</p> <p>Broadcom solutions are required to adhere to technical security standards and safeguards that are appropriate for their intended use and benefit. Security standards are determined after a comprehensive review is</p>

Measure Category	Broadcom Controls
	<p>conducted that assesses the type of data that will be handled by the solution, how and where the solution is implemented, relevant industry requirements and applicable laws and regulations. Prior to release of products to customers, antivirus/antimalware scanning is performed in accordance with industry standards and based on the risk profile additional penetration testing may be performed. Identified vulnerabilities are tracked in a central defect tracking system together with an associated risk rating. Identified Vulnerabilities are ranked using a risk rating (typically using the Common Vulnerability Scoring System [CVSS]) in accordance with the NIST Framework to determine their severity and the appropriate response.</p> <p>Penetration testing of the internal/external networks and/or applications is performed at least annually. The tests are usually performed externally by a reputable external organization. Customer environments are covered as part of the scope of the tests.</p> <p>Automated vulnerability scans of confidential information are performed periodically to identify, mitigate and remediate any vulnerabilities. Assets covered by such scanning include any servers, applications, endpoint desktops, laptops and network devices. All issues identified from the penetration tests and vulnerability scans rated as critical, high or medium risks are addressed through timely and documented remediation.</p> <p>Broadcom maintains certification against ISO/IEC 27001:2013 for security controls for facilities used in complying with customer-facing obligations under the applicable governing agreement. Broadcom will provide the customer with a copy of the applicable ISO/IEC 27001:2013 certification and accompanying Statement of Applicability identifying the controls that were evaluated as part of the certification process.</p>
Measures for ensuring data minimization	<p>Where Broadcom acts as a Data Controller, it only collects such and so much personal data as necessary for, and proportionate to the purposes of the processing, pursuant to the terms of the Broadcom Privacy Policy published at http://www.broadcom.com/privacy.</p> <p>Broadcom's products and services are developed and operated following the principle of Privacy by Design, so that such products and services will only collect and process the data necessary for and proportionate to the fulfillment of their intended functionalities. In many cases, customers have the ability to configure their products and services as best suited to their needs, in particular by exercising discrete choices on whether or not to use specific functionalities, and thereby control what data is collected and processed by the specific product or service. More detailed information about the core and optional features of the various products and services, and about the data they involve, may be found in those products' and services' transparency notices as available at https://www.broadcom.com/privacy.</p>
Measures for ensuring data quality	<p>Where Broadcom acts as a Data Controller, it takes technically feasible and commercially reasonable steps to ensure that the personal data it processes is accurate and relevant, pursuant to the terms of the Broadcom Privacy Policy published at http://www.broadcom.com/privacy.</p> <p>Where Broadcom acts as a Data Processor, it makes available technical and organizational means for the relevant Data Controller to perform through self-service facilities, or to obtain via service requests, the maintenance (e.g. rectification or erasure) of any personal data processed by Broadcom on its behalf.</p>

Measure Category	Broadcom Controls
Measures for ensuring limited data retention	<p>Broadcom embeds the principle of limited data retention into the design and operation of the services and systems it develops and maintains, and adheres to a defined record retention policy. Retention timelines for data in various systems, products and services will depend on the nature, scope and purpose of the system, product or service considered and of the data held therein; on the applicable contractual commitments; on the applicable legal and regulatory requirements; on the existence of a valid business need or legal obligation to retain the data.</p> <p>Data and other information related to support tickets raised by Broadcom customers are retained for 30 days after successful closure of the ticket and purged thereafter. More detailed information on the data retention timelines applicable to the various products and services offered by Broadcom may be found in those products' and services' transparency notices as available at https://www.broadcom.com/privacy.</p>
Measures for ensuring accountability	<p>Broadcom operates a global privacy program under the responsibility of the Global Privacy Officer. The program includes the creation and maintenance of records of data processing operations, the fulfillment of data subject rights, the handling of inquiries and complaints, the enforcement of privacy by design and privacy by default principles, the provision of up-to-date transparency information about Broadcom's data processing practices and of the data processing practices involved in the use of specific Broadcom products and services, the response to privacy events and incidents, and privacy training. More detailed information about these practices may be found in the documentation published at https://www.broadcom.com/privacy.</p>
Measures for allowing data portability and ensuring erasure	<p>Procedures are defined for instructing personnel on the proper methods for destroying media and storage devices on which confidential information is stored. Media and storage devices containing confidential information are wiped utilizing U.S. Department of Defense 5220.22-M or like industry standard procedures, which relate to the permanent and non-recoverable removal of data. Media and storage device destruction by a third party is accompanied by documented procedures (e.g., certificate of destruction) for destruction confirmation.</p>
Measures for detecting and responding to security incidents	<p>Broadcom follows a set of comprehensive incident response and vulnerability handling policies consistent with ISO 29147 and ISO 30111, and works closely with leading vulnerability research entities to actively monitor a large number of sources for vulnerability information, including vendor sites, public mailing lists, and security-related websites. To address validated vulnerability issues, we post security notices, patches, and remediation information on the Support website. Additionally, we may disseminate security notices and advisories to public mailing lists (mentioned above), and to various vulnerability-related organizations such as CERT and Mitre CVE.</p> <p>An Incident Response plan and associated procedures are documented and executed in the event of an information security incident. The incident response plan clearly articulates the responsibilities of personnel and identifies relevant parties to notify. Incident response personnel are trained, and the execution of the incident response plan is tested at least annually. The incident response process is executed as soon as Broadcom becomes aware of an incident.</p>

Measure Category	Broadcom Controls
	The incident management procedures address the following: Organizational structure is defined; Response team is identified; Response team availability is documented; Timelines for incident detection and disclosure are documented. The incident process lifecycle is defined including the following documented discrete steps: Identification; Severity rating; Incident classification and prioritization; Communication including, where appropriate, notification to the relationship (delivery) manager or other relevant contact as contractually defined; Resolution; Training (as appropriate); Testing; Reporting.
Measures for training personnel on information security and data privacy	Employees and any third parties who may access confidential information are required to take training at least annually relating to the security, privacy and protection of such information. Methods of training and awareness include: In-person and online educational programs; Exercises; Executive and management communications; Internal and external data privacy websites; Web line and helpline resources for reporting issues; Internal portals.
Measures for requiring the use of specific technical measures	Broadcom contractually requires all third-party data sub-processors it employs to implement technical, organizational and supplementary information security measures no less protective than the measures which Broadcom contractually commits to implement for its customers. To the extent technically feasible and commercially reasonable, such requirements specifically address the control of, and the access to any encryption keys used to protect the data of Broadcom and of its customers, with a view to minimizing the risk of such keys being exposed to any risk of undue access or interference.
Measures for increasing the transparency of data transfers and associated privacy impacts	<p>Broadcom conducts – and provides reasonable assistance for its customers to conduct – data transfer risk assessments in relation to the locations, especially non-adequate third-countries outside of the EU/EEA, where Broadcom and/or the sub-processors acting on its behalf may transfer customer personal data. Broadcom transparently discloses such destination locations in the transparency notices of the relevant products and services as published at https://www.broadcom.com/privacy.</p> <p>Broadcom follows a documented third-party vendor onboarding process to assess, manage and monitor its third-party vendors. Broadcom enters into contracts with sub-processors which incorporate data protection obligations substantially similar to those in this Information Security Practices document and the Data Processing Addendum. The terms of each sub-processor agreement ensures that Broadcom can meet its obligations to customers, including implementing required technical and organizational measures to protect Customer data, to assist with data subject requests and to protect personal data in compliance with applicable data privacy and protection laws and regulations.</p>
Measures for the handling, recording and reporting of government access requests to data	Broadcom has developed a process to govern the handling of government data access requests whereby such requests, if addressed at Broadcom, are acknowledged, assessed for validity and merit, challenged if questionable, disclosed to the extent feasible and permitted by applicable law to the persons concerned, and, if validated, fulfilled only to the minimum extent necessary for compliance with applicable laws, in line with applicable due process.

Measure Category	Broadcom Controls
Measures for ensuring that no backdoors exist	Broadcom does not introduce hidden functionality into its security technologies, nor intentionally leaves open any "backdoors" for exploitation, nor maintains any allow-lists for known cyber-threats. Broadcom adheres to the rigorous vulnerability management, patching and penetration testing practices and procedures described in this document.

IV. Overview of Broadcom's Technical and Organizational Measures as they relate to EU Law, Guidance and Jurisprudence

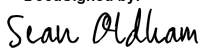
Measure Category	GDPR Art 32-33	EU SCCs 2021 Annex II	EDPB Supplementary Measures (Schrems II)	EDPB Data Breach Guidance
Measures of pseudonymization and encryption of personal data				
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services				
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident			Not relevant	
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing				
Measures for user identification and authorization				
Measures for the protection of data during transmission				
Measures for the protection of data during storage				
Measures for ensuring physical security of locations at which personal data are processed				

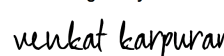
Measures for ensuring events logging	Not relevant		Not relevant	
Measures for ensuring system configuration, including default configuration	Not relevant			
Measures for internal IT and IT security governance and management				
Measures for certification/assurance of processes and products	Not relevant			
Measures for ensuring data minimization	Not relevant			Not relevant
Measures for ensuring data quality	Not relevant		Not relevant	Not relevant
Measures for ensuring limited data retention	Not relevant		Not relevant	Not relevant
Measures for ensuring accountability	Not relevant			Not relevant
Measures for allowing data portability and ensuring erasure	Not relevant		Not relevant	Not relevant
Measures for detecting and responding to security incidents		Not relevant	Not relevant	
Measures for training personnel on information security and data privacy				
Measures for requiring the use of specific technical measures	Not relevant			Not relevant
Measures for increasing the transparency of data transfers and associated privacy impacts	Not relevant			Not relevant
Measures for the handling, recording and reporting of government access requests to data	Not relevant			Not relevant
Measures for ensuring that no back-doors exist	Not relevant			Not relevant

Color Code	Not relevant or not applicable	Control available and deployed
------------	--------------------------------	--------------------------------

Approved by: Sean Oldham, Chief Information Security Officer Venkat Karpuram, Senior Director, Central Engineering Services

March 2024

DocuSigned by:

 EB655E4DE1B6432...

DocuSigned by:

 2B530EB0670D43A...