Avanade's Client Data Safeguards

The following terms describe the technical and organizational measures, internal controls and information security routines that Avanade maintains to safeguard data provided by or on behalf of our clients in connection with a client service engagement ("**Client Data**"). These security measures are intended to protect Client Data when in Avanade's environments (e.g., systems, networks, facilities) against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction. When Client Data includes personal data, our implementation of and compliance with these measures (and any additional security measures set out in the applicable client agreement) is designed to provide an appropriate level of security in respect of the processing of the personal data. Avanade may change these measures from time to time, without notice, so long as any such revisions do not materially reduce or degrade the protection provided for the Client Data.

STANDARD DATA SAFEGUARDS:

1. **Organization of Information Security**

   a) **Security Ownership.** Avanade will appoint one or more security officers responsible for coordinating and monitoring the security rules and procedures.

   b) **Security Roles and Responsibilities.** Avanade's personnel with access to Client Data will be subject to confidentiality obligations.

   c) **Risk Management Program.** Avanade will have a risk management program in place to identify, assess and take appropriate actions with respect to risks related to the processing of the Client Data in connection with the applicable agreement between the Parties.

2. **Asset Management**

   a) **Asset Inventory.** Avanade will maintain an asset inventory of its infrastructure, network, applications and cloud environments. Avanade will also maintain an inventory of its media on which Client Data is stored. Access to the inventories of such media will be restricted to personnel authorized in writing to have such access.

   b) **Data Handling.** Avanade will

      i. Classify Client Data to help identify such data and to allow for access to it to be appropriately restricted.

      ii. Limit printing of Client Data from its systems to what is minimally necessary to perform services and have procedures for disposing of printed materials that contain Client Data.

      iii. Require its personnel to obtain appropriate authorization prior to storing Client Data outside of contractually approved locations and systems, remotely accessing Client Data, or processing Client Data outside the Parties' facilities.

3. **Human Resources Security**

   a) **Security Training.** Avanade will

      i. Inform its personnel about relevant security procedures and their respective roles.

      ii. Inform its personnel of possible consequences of breaching the security rules and procedures.

      iii. Only use anonymous data in its training environments.

Avanade's Client Data Safeguards

4. **Physical and Environmental Security**

   a) **Physical Access to Facilities.** Avanade will implement and maintain procedures to limit authorized access to its facilities where information systems that process Client Data are located.

   b) **Physical Access to Components.** Avanade will maintain records of the incoming and outgoing media containing Client Data, including the kind of media, the authorized sender/ recipients, date and time, the number of media, and the types of Client Data they contain.

   c) **Component Disposal.** Avanade will use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) processes to delete Client Data when it is no longer needed.

5. **Communications and Operations Management**

   a) **Operational Policy.** Avanade will maintain security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Client Data.

   b) **Mobile Device Management (MDM)/Mobile Application Management (MAM).** Avanade will maintain a policy for its mobile devices that:

      i. Enforces device encryption.

      ii. Prohibit use of blacklisted apps.

      iii. Prohibits enrollment of mobile devices that have been "jail broken."

   c) **Data Recovery Procedures.** Avanade will

      i. Have specific data recovery procedures with respect to its systems in place designed to enable the recovery of Client Data being maintained in its systems.

      ii. Review its data recovery procedures at least annually.

      iii. Log data restoration efforts with respect to its systems, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.

   d) **Malicious Software.** Avanade will have anti-malware controls to help avoid malicious software gaining unauthorized access to Client Data, including malicious software originating from public networks.

   e) **Data Beyond Boundaries.** Avanade will

      i. Encrypt Client Data that it transmits over public networks.

      ii. Protect Client Data in media leaving its facilities (e.g., through encryption).

      iii. Implement automated tools where practicable to reduce the risks of misdirected email, letters, and / or faxes from its systems.

   f) **Event Logging.**

      i. For its systems containing Client Data, Avanade will log events consistent with its stated policies or standards.

Avanade's Client Data Safeguards

6. Access Control

a) Access Policy. Avanade will maintain a record of security privileges of individuals having access to Client Data via its systems.

b) Access Authorization. Avanade will

i. Maintain and update a record of personnel authorized to access Client Data via its systems.

ii. When responsible for access provisioning, promptly provision authentication credentials.

iii. Deactivate authentication credentials where such credentials have not been used for a period of time (such period of non-use not to exceed 90 days).

iv. Deactivate authentication credentials upon notification that access is no longer needed (e.g., employee termination, project reassignment, etc.) within two business days.

v. Identify those personnel who may grant, alter or cancel authorized access to data and resources.

vi. Ensure that where more than one individual has access to its systems containing Client Data, the individuals have unique identifiers/log-ins (i.e., no shared ids).

c) Least Privilege. Avanade will

i. Only permit its technical support personnel to have access to Client Data when needed

ii. Maintain controls that enable emergency access to productions systems via firefighter ids, temporary ids or ids managed by a Privileged Access Management (PAM) solution.

iii. Restrict access to Client Data in its systems to only those individuals who require such access to perform their job function.

iv. Limit access to Client Data in its systems to only that data minimally necessary to perform the services.

v. Support segregation of duties between its environments so that no individual person has access to perform tasks that create a security conflict of interest (e.g., developer/ reviewer, developer/tester).

d) Integrity and Confidentiality. Avanade will instruct its personnel to disable administrative sessions when leaving premises or when computers are otherwise left unattended.

e) Authentication. Avanade will

i. Use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) practices to identify and authenticate users who attempt to access its information systems.

ii. Where authentication mechanisms are based on passwords, require that the passwords are renewed regularly.

iii. Where authentication mechanisms are based on passwords, require the password to contain at least eight characters and three of the following four types of characters: numeric (0-9), lowercase (a-z), uppercase (A-Z), special (e.g., !, *, &, etc.).

iv. Ensure that de-activated or expired identifiers are not granted to other individuals.

v. Monitor repeated attempts to gain access to its information systems using an invalid password.

vi. Maintain industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

vii. Use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, as well as during storage.

f) Multi Factor Authentication. Avanade will implement Multi-Factor Authentication for internal access and remote access over virtual private network (VPN) to its systems.

7. Penetration Testing and Vulnerability Scanning of Avanade Systems.

a) At least annually, Avanade will perform penetration and vulnerability assessments on Avanade's IT environments in accordance with Avanade's internal security policies and standard practices.

b) Avanade agrees to share with Client summary level information related to such tests as conducted by Avanade to the extent applicable to the Services.

c) For clarity, as it relates to such penetration and vulnerability testing, Client will not be entitled to (i) data or information of other customers or clients of Avanade; (ii) test third party IT environments except to the extent Avanade has the right to allow such testing; (iii) any access to or testing of shared service infrastructure or environments, or (iv) any other Confidential Information of Avanade that is not directly relevant to such tests and the Services.

d) For any Avanade IT systems that are physically dedicated to Client, the Parties may agree to separate, written testing plans and such testing will not to exceed two tests per year.

8. Network and Application Design and Management. Avanade will

a) Have controls to avoid individuals gaining unauthorized access to Client Data in its systems.

b) Use email-based data loss prevention to monitor or restrict movement of sensitive data.

c) Use network-based web filtering to prevent access to unauthorized sites.

d) Use firefighter IDs or temporary user IDs for production access.

e) Use network intrusion detection and / or prevention in its systems.

f) Use secure coding standards.

g) Scan for and remediate OWASP vulnerabilities in its systems.

h) To the extent technically possible, expect that the Parties will work together to limit the ability of Avanade personnel to access non-Client and non-Avanade environments from the Client systems.

i) Maintain up to date server, network, infrastructure, application and cloud security configuration standards.

j) Scan its environments to ensure identified configuration vulnerabilities have been remediated.

9. Patch Management

a) Avanade will have a patch management procedure that deploys security patches for its systems used to process Client Data that includes:

i. Defined time allowed to implement patches (not to exceed 90 days for high or medium patches as defined by Avanade's standard); and

ii. Established process to handle emergency or critical patches as soon as practicable.

10. Workstations

a) Avanade will implement controls for workstations it provides that are used in connection with service delivery/receipt incorporating the following:

i. Software agent that manages overall compliance of workstation and reports at a minimum on a weekly basis to a central server

ii. Encrypted hard drive

iii. Patching process so that workstations are patched within the documented patching schedule

iv. Ability to prevent blacklisted software from being installed

v. Antivirus with a minimum weekly scan

vi. Firewalls installed

11. Information Security Breach Management

a) Security Breach Response Process. Avanade will maintain a record of its own security breaches in its systems with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the process for recovering data.

b) Service Monitoring. Avanade's security personnel will review their own logs as part of their security breach response process to propose remediation efforts if necessary.

12. Business Continuity Management

a) Avanade will have processes and programs that are aligned to ISO 22301 to enable recovery from events that impact its ability to perform in accordance with the Agreement.

SUPPLEMENTARY MEASURES. In addition, in accordance with regulatory guidance following the European Court of Justice "Schrems II" decision, Avanade further commits to maintaining the following additional technical, organizational and legal/contractual measures with respect to Client Data, including personal data.

Technical Supplementary Measures:

1. The Client Data in transit between Avanade entities will be strongly encrypted with encryption that:

a) is state of the art,

b) secures the confidentiality for the required time period,

c) is implemented by properly maintained software,

d) is robust and provides protection against active and passive attacks by public authorities, including crypto analysis, and

e) does not contain back doors in hardware or software, unless otherwise agreed with the applicable Client.

2. The Client Data at rest and stored by any Avanade entities will be strongly encrypted with encryption that:

a) is state of the art,

b) secures the confidentiality for the required time period,

c) is implemented by properly maintained software,

d) is robust and provides protection against active and passive attacks by public authorities, including crypto analysis, and

e) does not contain back doors in hardware or software, unless otherwise agreed with the applicable Client.

Organizational Supplementary Measures:

1. The Client Data transfer between Avanade entities and the processing by any Avanade entities will be in accordance with:

a) Avanade's internal policies and procedures to manage requests from public authorities to access personal data,

b) Avanade's internal data access and confidentiality policies and procedures,

c) Avanade's internal data minimization policies and procedures, and

d) Avanade's internal data security and data privacy policies and procedures.

2. Avanade will maintain a documented log of requests for access to personal data received from public authorities and the response provided, along with the legal reasoning and the involved parties.

3. Avanade will regularly provide reports of public authority requests for personal data, if any, to Avanade's Chief Compliance Officer

Legal/Contractual Supplementary Measures:

1. Avanade will maintain regularly updated assessment reports with respect to the surveillance laws and privacy practices for the countries in which Avanade processes Client Data where such country is not formally recognized as providing a lever of protection essentially similar to EU countries and will provide copies of applicable reports to clients upon request.

2. The Avanade entity/s processing Client Data certify that, unless otherwise agreed with the applicable Client, (a) it has not purposefully created back doors or similar programming that could

be used to access the system and/or personal data (b) it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and (c) to the best of Avanade's knowledge, applicable national law or government policy does not require the Avanade entity to create or maintain back doors or to facilitate access to personal data or systems or for the Avanade entity to be in possession or to hand over the encryption key without a legally valid order and following an appropriate legal review.

3. To the extent permitted under applicable law the Avanade entity/s processing Client Data will inform the client of Government Requests relating to Personal Data that Avanade is processing on behalf of the client. If, under applicable law, Avanade is not permitted to inform the client of a Government Request, Avanade will take reasonable steps to either (i) obtain administrative or judicial leave to inform the client at the earliest possible time or (ii) request that the respective Government Authority directly informs the client. In any event, Avanade will take reasonable steps before the courts or in administrative proceedings to challenge Government Requests it deems unlawful.
4. Avanade will advise the applicable client of any change in applicable law that would affect Avanade's ability to comply with the data transfer mechanism relied on.
5. The Avanade entity/s processing Client Data will allow the applicable client to verify if its personal data was disclosed to public authorities via agreed audit procedures as set out in the applicable client agreement.
6. The Avanade entity/s processing Client Data will not engage in any onward transfer of Client Data, or suspend ongoing transfers, without the client’s approval as required in the applicable client agreement or as otherwise required by law.
7. Nothing herein shall prejudice the rights of the data subject to recover damages from Avanade to the extent permitted by applicable law in the event Avanade discloses Client Data transferred in violation of its commitments contained under the chosen transfer tool.