DATED **____________________ 2019**

[NAME OF ILOMAR ENTITY]

- and -

[SUPPLIER]

____

DATA PROCESSING AGREEMENT

____

THIS AGREEMENT is dated 2019

BETWEEN:

(1) [NAME OF ILOMAR ENTITY], a company registered in [x] with registration number [number] and whose registered office is at [address] (the "**Client**"); and

(2) [NAME OF SUPPLIER], a company registered in [x] with registration number [number] and whose registered office is at [address] (the "**Supplier**")

WHEREAS:

(A) The Client and the Supplier have entered into a contract for the supply of certain services (the "**Services**") on [date] (the "**Agreement**").

(C) The Parties wish to enter into this Data Processing Agreement (the "**DPA**") in order to govern the processing of any Client data. For the avoidance of doubt, this DPA replaces and/or overrides all data protection obligations set out in any other documentation in relation to the processing of the Client's data by the Supplier.

The Parties agree as follows:

1. DEFINITIONS AND INTERPRETATION

1.1 Terms and expressions used in this DPA and not defined herein or in the Agreement have the meanings assigned to them in Data Protection Legislation.

"**Data Protection Legislation**"	means: (i) the General Data Protection Regulation (EU) 2016/679 and any national implementing laws, regulation(s) and secondary legislation (the **"GDPR"**); and (ii) the European Privacy and Electronic Communications Directive (Directive 2002/58/EC), each as amended from time to time;
"**Regulator**"	means any regulatory, administrative, supervisory or governmental agency, body or authority with authority over either of the Parties or the Services;
"**Reportable Breach**"	means any unauthorised or unlawful processing, disclosure of, or access to, Personal Data provided by the Client and/or any accidental or unlawful destruction of, loss of, alteration to, or corruption of such Personal Data which is likely to result in a risk to the rights and freedoms of any Data Subject;

"**Service Recipients**"	means the Client and any other entity which receives the Services under the Agreement;
“**Sub-processor**”	means any third party to which the Supplier is permitted to sub-contract any element of the Services in accordance with the terms of the Agreement; and
"**Supplier Personnel**"	means all or any of directors, officers, employees and/or agents of the Supplier or its sub-contractors; and any other individuals engaged by or on behalf of the Supplier or any of its sub-contractors in performance of the Services or Supplier’s obligations under this DPA.

1.2 The index, the cover and the headings to Clauses are for convenience only and shall not affect the construction of this Agreement.

2. DATA PROTECTION

2.1 Schedule 1 to this DPA sets out the scope, nature and purpose of Data Processing by the Supplier under this DPA, and the applicable types of Personal Data and categories of data subject.

2.2 In respect of Personal Data processed by the Supplier on behalf of the Client, the Supplier acts as a Data Processor and the Client is a Data Controller. In Processing the Personal Data, the Supplier shall comply with all its obligations as a Data Processor under Data Protection Legislation. The Client shall comply with all its obligations as a Data Controller under Data Protection Legislation.

2.3 If the Supplier is or becomes aware of any reason that would prevent its compliance with Data Protection Legislation, including where Supplier is of the opinion that an instruction of Client is not in compliance with Data Protection Legislation, it shall notify the Client as soon as reasonably practicable.

2.4 ***Data Processing***. The Supplier shall only Process Personal Data in accordance with the provision of the Services as set out in the Agreement, the terms of this DPA and/or any other written instructions of the Client. The Supplier agrees that it will acquire no rights or interest in the Personal Data.

2.5 ***Security.*** Supplier shall implement and maintain appropriate technical and organisational measures to ensure the security of the Personal Data against unauthorised or unlawful processing, and accidental loss, destruction, or damage in accordance with the requirements set out in Schedule 2 to this DPA.

2.6 ***Supplier Personnel.*** Supplier shall take reasonable steps to ensure the reliability of all Supplier Personnel who may have access to the Client’s Personal Data, ensuring: (i) that access is strictly limited to those only individuals who need to access the Personal Data for the purposes of providing the Services; and (ii) that all such individuals are subject to confidentiality obligations in relation to the Client's Personal Data.

2.7 ***Supplier Co-operation.*** Supplier shall provide reasonable assistance to enable the Client to comply with its obligations under the Data Protection Legislation, including in relation to any data protection impact assessments, and consultations with Regulators.

2.8 ***Data Subject Rights.*** Supplier shall provide reasonable assistance to the Client to enable the Client to respond to requests regarding the exercise of Data Subject rights (including access requests) under the Data Protection Legislation. Supplier shall notify the Client as soon as possible if it receives any communication from a Data Subject regarding: (i) the exercise of their Data Subject rights; or (ii) any complaint or other communication regarding the Processing of Personal Data or compliance with Data Protection Legislation. Supplier shall not respond to any such communication without first consulting the Client.

2.9 ***Personal Data Breach.*** Supplier will notify Client, without undue delay upon becoming aware, and in any event, within 24 hours, of a Reportable Breach and provide sufficient information to allow the Client to meet any obligations to report such breach, or inform Data Subjects of the Reportable Breach as required under the Data Protection Legislation. Supplier shall co-operate with the Client and take reasonable steps as directed by the Client to assist in the investigation, mitigation and remediation of each such Reportable Breach.

2.10 ***Deletion or Return of Personal Data.*** Supplier shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Client Personal Data, at the option of Client, return (if feasible) to Client, or delete, and procure the deletion of, all copies of Personal Data, other than to the extent its retention is required by applicable Data Protection Legislation. This clause shall survive termination of this DPA.

2.11 ***Sub-processors.*** Supplier may disclose Personal Data to a Sub-processor only to the extent such disclosure is necessary for the Sub-processor's provision of the Services or part thereof, and provided that: (i) the Supplier imposes obligations on the Sub-processor, in writing, no less onerous than those set out in this DPA; and (ii) the Supplier will remain liable for the performance of such obligations by the Sub-processor or any breach of this DPA caused by the Sub-processor.

2.12 ***Data Transfer.*** The Supplier will not transfer Personal Data outside the European Economic Area unless it ensures that it complies with the obligations set out in Data Protection Legislation regarding the transfer of Personal Data outside the European Economic Area, for example by entering into EU approved standard contractual clauses.

2.13 ***Audit.*** At any time upon request from the Client, Supplier shall make available to the Client or a Regulator as required, all information necessary to demonstrate compliance with this DPA or as otherwise required, and at any time on reasonable notice, shall allow audits by the Client, a third party auditor instructed by the Client or a Regulator.

3. INDEMNITY

3.1 The Supplier shall indemnify the Client and any Service Recipients, and shall keep the Client and any Service Recipients indemnified for all time, against all losses, fees, damages, fines, costs or expenses arising out of or in connection with any breach by the Supplier of the provisions of this DPA, save where such breach arises as a result of Supplier acting in accordance with instructions from the Client.

4. STATUS OF THIS AGREEMENT

4.1 All data protection and other provisions, including all related definitions, set out within any other agreements or documentation which may pertain to the Supplier's processing of the Client's data which conflict with the terms of this Agreement shall, to the extent they so conflict, be replaced, notwithstanding any provision to the contrary in such agreements or documentation, with the wording set out in this Agreement.

4.2 In the event of any inconsistency or ambiguity between any other agreements or documentation which may pertain to the Supplier's processing of the Client's data and this Agreement, then the terms of this Agreement shall prevail.

5. GOVERNING LAW

5.1 This Agreement and any dispute or non-contractual obligation arising out of or in connection with it shall be governed by, and construed in accordance with, the laws of Belgium. The parties submit to the exclusive jurisdiction of the courts of Antwerp.

Signed for and on behalf of [NAME OF ILOMAR ENTITY]

By
Name
Title
Date

Signed for and on behalf of [NAME OF SUPPLIER]

By
Name
Title
Date

SCHEDULE 1

Data Collection	Specific Information regarding Client Personal Data
Nature of the Processing Activities	□ Automated □ Manual □ Storage □ Transferring □ Retrieval □ Analysis □ Printing □ Analysis □ Other: ________________________
Purpose of Data Processing	□ Operate payroll □ Provision of employee benefits, e.g., medical insurance □ Performance monitoring □ Send marketing material to customers □ Store archived records □ Information security management □ Premise/facility security management □ Customer relationship management □ Other: ________________________
Duration of the Processing Activities	□ During term of Agreement only □ Other: ________________________
Categories of Data Subjects involved with Client Personal Data	□ Current, former, and prospective employees, including contract or temporary employees, of Client □ Dependents, beneficiaries, spouses, and domestic partners of current, former, and prospective employees, including contract or temporary employees, of Client □ Customers of Client □ Vendors, service providers, and business contacts of Client □ Visitors to Client premises □ Other: ________________________
Type(s) of Personal Data to be Processed	□ Last name, first name □ Address □ Personal email address □ Professional email address □ Personal phone number □ Professional phone number

	□ Photo □ Image (via a video monitoring) □ Date of birth □ Place of birth □ CV/Résumé □ Location tracking data (e.g., GPS). □ Governmental and Personal identifiers (Social Security Number, Driver's License Number, etc.) □ Financial data (income, loan files, transactions, purchase and consumption habits, credit information, insolvency status, etc.) □ Employment data (employee files, career background, evaluations, reference, interviews, disciplinary measures, etc.) □ Data connection information (IP address, login information, credentials, etc.) □ Other; please list: ________________________________
Type(s) of Client Personal Data to be Processed by Avanade under this Implementation Contract – Special Categories.	□ Racial or ethnic origin □ Political opinions □ Religious or philosophical beliefs □ Trade union membership □ Sex life or sexual orientation □ Genetic data □ Biometric data □ Health data (mental or physical disabilities, family medical history, personal medical history, medical records, prescriptions, etc.) □ Financial account information, such as banking/ credit card data, account numbers, credit card numbers, etc. □ Data relating to criminal charges, convictions, and offenses □ Other; please list: ________________________________
Data Protection Officer	Name: Email:

Schedule 2 – Security Requirements

Topic	Requirement	Applicable
Identification	Define a unique login per user and prohibit accounts shared between several users.	□
Identification	All created accounts must respect LDC's naming convention	□
Identification	Avoid, that the user IDs (or logins) are those of the accounts defined by default by the software editors and disable the default accounts.	□
Authentication - Password	Apply appropriate complexity rules to users passwords.	□
Authentication - Password	Adopt a specific password policy for administrators. Change passwords, at least, every time an administrator leaves and in case of suspected compromise.	□
Authentication - Password	Require password renewal at a relevant and reasonable frequency.	□
Authentication - Password	Limit the number of attempts to access user accounts and temporarily block the account when the limit is reached.	□
Authentication - Password	Implement technical means to enforce authentication rules (e.g. account blocking if password is not renewed).	□
Authentication - Password	Use password managers to have different passwords for each service, while retaining only one master password.	□
Access rights - Need to know / least privileges	Define profiles in the systems by separating tasks and areas of responsibility (limiting users' access only to data strictly necessary for the accomplishment of their missions).	□
Access rights - Segregation of duties	Limit access to administration tools and interfaces to authorized persons only. In particular, limit the use of administrator accounts to IT teams and only for administrative actions that require it. Use lower privilege accounts for day-to-day transactions.	□
Access rights - Life cycle	Remove users' access permissions as soon as they are no longer authorized to access resources, and at the end of their contract.	□
Access rights - Reviews	Conduct an annual review of permissions to identify and delete unused accounts and realign the rights granted to each user's functions.	□
Authentication - Method	Prefer authentication methods using AD and ADFS when possible (users, systems, applications) and avoid the use of local accounts.	□
Authentication - Method	Prefer authentification methods using Single Sign On (SSO)	□
Authentication - Method	Use strong authentication.	□
Workstations	Provide an automatic session lock mechanism if the workstation is not used for a given period of time.	□
Workstations	Encrypt disks on workstations (Laptops)	□

Workstations	Install a software "firewall", and limit the opening of communication ports to those strictly necessary for the proper operation of applications installed on the workstation.	□
Workstations	Install only application available on the Software Center and limit the use of applications that require administrator-level rights to run to what is strictly necessary.	□
Workstations	Position a privacy filter on the screens of workstations used in public places or during travels (laptops)	□
Workstations	Use protection mechanisms against theft (e.g. safety cable, visible material marking).	□
USB	Disable autorun for removable media.	□
USB	The use of personal mobile media is prohibited. Limit the connection of mobile media (USB sticks, external hard disks, etc.) to the strict minimum and use only thoses provided by LDC.	□
USB	Encrypt mobile storage media (USB sticks, external hard drives, etc.)	□
Smartphones	In addition to the PIN code of the SIM card, activate the automatic locking of the terminal and require a secret to unlock it (password, scheme, etc.).	□
Smartphones	All corporate smarthphones should be included in the EMM solution.	□
Servers / Workstations	Workstations and servers must be included in the appropriate patching process on OS and applications. Critical updates should be installed as soon as possible after their publication.	□
Servers / Workstations	Servers and workstations must have an antivirus installed, enabled and up to date	□
Servers / Workstations	Hardening guides must be used for OS, databases, Web servers, etc.	□
Servers / Workstations	It is forbiden to install obsolete/unsupported or shortly obsolete/unsupported systems or applications. Only approved application/Operating System must be used.	□
Premise protection	Physically protect computer equipment by specific means (dedicated fire-fighting system, raising against possible flooding, redundancy of power supply and/or air conditioning, etc.).	□
Premise protection - Detection	Install intruder alarms and check them periodically.	□
Premise protection - Detection	Install smoke detectors and firefighting equipment and inspect them annually.	□
Premise protection - Access	Access controlled by badge on premises	□
Premise protection - Access	Distinguish building zones according to risks (for example, provide dedicated access control for the computer room).	□
Premise protection - Access	Maintain an up-to-date list of the persons or categories of persons authorized to enter each zone.	□
Premise protection - Access	Regularly review and update access permissions to secure areas and remove them if necessary.	□
Premise protection - Access	Within restricted areas, require visible identification (badge) for all persons	□

Premise protection - Access	Keep a record of access to rooms or offices likely to house equipment containing personal data	□
Premise protection - Visitors	Having visitors accompanied outside the public areas by a person belonging to the organization.	□
Premise protection - Visitors	Visitors (technical support staff, etc.) must have limited access. The date and time of arrival and departure must be recorded.	□
Maintenance	Record maintenance tasks in a handrail.	□
Maintenance	Interventions carried out by third parties must be supervised by a person from LDC.	□
Documentation	Document operating procedures, keep them up to date and make them available to all users concerned.	□
Documentation	Update IP Adress Management Software, TAD, CMDB as soon as a change occur	□
Documentation	Apply a clean desk Policy and store sensitive documents in locked and safe places.	□
Change Management	Any change must be recorded in the Change Management system, and follow proper approval workflow	□
Network	Require a VPN for remote access with strong user authentication (smart card, OTP, etc.).	□
Network	Implement a network segmentation (DMZ, FW, VLAN, etc.)	□
Network	Define network flows that are strictly necessary by filtering incoming and outgoing flows on equipment (firewall, proxy, servers, etc.) and in compliance with segmentation model.	□
Network	Use encrypted version of protocols, and only the compliant versions (in transit) with a sufficient hardening (key lenghts, algorithms, protocol versions, etc.)	□
Network	Use an intrusion detection system (IDS) to analyze network traffic and detect attacks.	□
Network	Separate production environnement from the others environnements (test, dev, etc.)	□
Network	Set up automatic hardware identification using network card identifiers (MAC addresses) to prevent the connection of an unknown device (NAC).	□
Network - Internet	Any user web browsing activity must go through a proxy with adequate URL filtering	□
Network - Internet	Any server web browsing activity must to go through FW and URL filtering	□
Network - Internet	Any cloud internet activity must to go through FW and URL filtering	□
Network - Internet	Any user web browsing from a server is prohibited	□
Network - Wi-Fi	Use appropriate encryption on Wi-Fi networks.	□
Network - Wi-Fi	Guests access (e.g. Wi-Fi) must exist and be separated from the internal network.	□
Administration	Ensure that no administration interface is accessible directly from the Internet. Remote maintenance/administration must be performed through a VPN and, if possible, use strong authentication (smart card, OTP, etc.).	□
Administration	Administration operations should be done via a dedicated and isolated network, accessible after strong authentication and with enhanced traceability.	□

Administration	Internal access to the DataCenter assets should be perform through secured jumphosts	□
Administration	External access to the DataCenter assets should be perform through a bastion	□
Data disposal	Securely delete data on equipments before they are scrapped, sent for repair to a third party or at the end of the rental contract.	□
Data disposal	Securely delete data on a workstation prior to its reassignment to another person.	□
Data disposal	Shred paper containing sensitive informations before throw them in the garbage	□
Awareness	All users must receive an appropriate awareness concerning IT security	□
Coding	Perform IT development and testing in an IT environment separated from the production environment (for example, on different computers or virtual machines).	□
Coding	Perform IT developments and tests on fictitious or anonymized data.	□
Coding	Code auditing must be performed when developping sensitive applications	□
Coding	Store passwords securely hashed to a minimum with a cryptographic hash function using a salt or key, and at best transformed with a function specifically designed for this purpose always using a salt or key. (A key should not be stored in the same database as the hashed passwords.)	□
Sub contracting	Integrate security requiremeent in the contracts with third parties	□
Sub contracting	All external employees must sign the third parties IT charter	□
Redundancy	Provide hardware redundancy of storage equipment, for example by using RAID technology	□
Redundancy	Use an UPS (Uninterruptible Power Supply) to protect equipment used for essential treatments	□
Redundancy	If data and system availability requirements are high, it is recommended to implement data replication to a secondary site.	□
Data storage	Encourage the storage of user data on a regularly backed up storage space accessible via the organization's network rather than on workstations.	□
Data backup	Perform frequent data backups based on business needs for each system.	□
Data backup	Protect data backed up to the same level of security as that stored on the operating servers (for example by encrypting backups, providing storage in a secure location, contractually supervising a backup outsourcing service).	□
Data backup	When backups are transmitted over the network, the transmission channel should be encrypted if it is not internal to the organization.	□
Data backup	Store backups on an external site, if possible in fireproof and waterproof vaults as long as required by the Data Retention policy.	□
Data backup	Dispose of backups at the end of the time specified in the Data Retention policy.	□
Business continuity	Regularly test backup recovery and business continuity or disaster recovery plan implementation.	□
Archiving	For each application, define an archive management process : what data should be archived, how and where is it stored, how is descriptive data managed?	□
Archiving	Implement specific access procedures for archived data, since the use of an archive must take place on an occasional and exceptional basis.	□
Data retention	A retention period must be defined for the data.	□
Security services - Scans	A vulnerability scan must be performed before go live and during the prduction phase on a regular basis. Vulnerabilities which are discovered during those scans must be remediated as soon as possible.	□
Security services - Pentest	Perform pentest on sensitive application/infrastructure before go-live and on a regular basis	□

Security services - SOC	If a workstation is compromised, search the source as well as any trace of intrusion in the organization's information system, to detect the compromise of other elements.	□
Security services - CERT	Conduct a security monitoring on software and hardware used in the organization's information system (CERT).	□
Regulations - GDPR	For each application, check if PII (Personally Identifiable Information) are processed/used	□
Regulations - GDPR	In the case PII are processed or used, complete the processing record	□
Data classification	Apply a classification on all data handled and security measures correlated with the classification level	□
Monitoring	A monitoring should be perform on assets (disk space, CPU, network bandwith, licenses, etc.).	□
Logs and incidents	Provide a system for logging user activities, anomalies and security-related events: - These logs must keep the events in compliance with Data Retention policy. - Logging must concern, at a minimum, users' access including their identifier, the date and time of their connection, and the date and time of their disconnection; - In some cases, it may also be necessary to keep details of the actions taken by the user, the types of data consulted and the reference of the record concerned.	□
Logs and incidents	Protect logging equipment and information from unauthorized access, including by making it inaccessible to people whose activity is being logged.	□
Email	Sensitive attachment sent by email must be encrypted	□
Email	All inbound emails must go through an antivirus and an antispam solution.	□
Email	Email authentication should be provided through the use of SPF, DMARK, DKIM	□