Software Asset Management (SAM) Statement of Work (SOW) – GDPR Assessment

(For use with the Microsoft SAM Services Program)

1. Description

As of May 25, 2018, the latest European Union data protection law, the General Data Protection Regulation (GDPR), is in effect. The GDPR imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to individuals in the European Union (EU), or that collect and analyze information tied to those individuals. The law also strengthens the rights for individuals in relation to their personal data, impacting any organization's business processes. Understanding and adhering to the requirements of the GDPR applies to organization regardless of where they are located, though applicability depends on the following:

- Customers that are/have a registered company/organization within the European Union; or
- Customers that offer goods or services to, or monitor the behavior of, European Union data subjects (persons) residing within the boundaries of the European Union.

The SAM GDPR Assessment is designed to provide the customer with insights on their existing practices and how they relate to the GDPR. To achieve this goal, the SAM GDPR Assessment utilizes a maturity model to communicate Findings and Recommendations. The maturity model construct for the SAM GDPR assessment is based on a similar model developed by Microsoft (Security Maturity Model v1) and is consistent with the Software Optimization Model (SOM). It provides insight in the overall level of programmatic aspects of an organization's GDPR practices in an all-up way to determine whether it is aware of the risks to do business in, or with, the European Union.

During the assessment Organizational and Technical aspects of the customer will be inventoried and analyzed providing insights into the practices of the organization compared to the construct of the maturity model provided. Per the GDPR requirements, the customer's data protection practices play a critical part in ensuring the secure processing of personal data. In order to do this we leverage a global standard security framework. A selected set of Center for Internet Security (CIS) v7 Controls™ that are specific to data management, asset management and operational procedures to compile a measurement scheme. Based on the responses from the customer on the questionnaire and the data collected in the asset management inventory, the analysis will provide guidance on privacy and security programs that will help outline a roadmap for enabling proper privacy practices.

This assessment does not provide an exhaustive review of all the elements of the GDPR, nor is it legal advice.

During the assessment, the SAM partner collects questionnaire information outlining the privacy and data protection practice position of the customer and the automated technical scans on all Microsoft product deployments, usage, and versions. The partner will use third-party tools, interviews with key customer stakeholders, to capture all information and data relevant to the assessment. With this information and data, the partner will provide an analysis of the findings as well as recommendations on additional uses of the data captured to show customers how to get more value from the SAM GDPR Assessment.

This assessment in no way guarantees compliance with the GDPR, but instead provides a foundation for understanding the data environment, processes, and capabilities as they relate to the GDPR and cybersecurity. In no event will the partner make any statements to customers that this SAM GDPR Assessment will bring them into compliance with the GDPR.

Given the current cybersecurity threats to data and potential impact to the privacy of individuals this assessment is useful, even if the customer does not meet the above qualifications.

Use of Intelligent Asset Manager (IAM) is required in this SAM GDPR engagement to receive Channel Incentives. All work contemplated under this Statement of Work (SOW) will be provided in accordance with the IAM Terms of Use ("TOUs"), available here.

In this SAM Assessment, the Effective Licensing Position (ELP) is optional. The choice of including the ELP in this assessment belongs to the SAM Engagement Manager in discussions with the customer and the partner.

2. Inputs

The partner will collect the following inputs from the customer's premises:

1. The customer's IT strategy and/or roadmap, including their current privacy and data protection concerns and action plans.
2. A complete background of the customer's existing IT infrastructure and environment, including on-premises, Cloud and outsourced installations for all locations and/or divisions, an understanding of remote employee and external contractor protocols for accessing the network, and corporate network connectivity to external networks.
3. Current IT infrastructure and organization diagrams including locations, IT group names, SAM tool(s) or supporting processes in use, and stakeholder names.
4. The customer's policies and procedures related to managing privacy, security and disaster recovery, if they exist.
5. Information on the customer's current efforts or future plans to comply with the GDPR, including what types of organizational and technical measures are currently in place and what future plans are under consideration.
6. Deployment inventory data coverage of no less than 90% from at least one (1) automated discovery tool for each customer location where Microsoft products are installed.

3. Data collection

This section lists steps partners must take to build the foundation for the required analysis and customer deliverables. Partners will ensure that all data collected will be stored securely and in accordance with the requirements set out in the IAM TOUs. The main category of data collection is data related to the GDPR assessment, findings, and recommendations. Partners must ensure that the data collected is complete and accurate. Any deviation or change to this scope needs to be approved by Microsoft, the partner and the customer.

Discovery and inventory of hardware and software assets: data collection requirements

Data coverage must reach at least 90% of all devices pertaining to this engagement. Data coverage is defined as the percentage of total devices for which all required installation data has been obtained. Where devices are not joined to the directory or network, manual collection of data is acceptable while maintaining the 90% data coverage requirement. Some specific guidance includes, but is not limited to:

1. Complete extraction of user accounts from the customer's Active Directory (AD) domain(s) and Lightweight Directory Access Protocol (LDAP) and/or workgroups.

2. Data extracted must be cross-referenced against a minimum of one (1) additional data source, including but not limited to:
    i. Records from existing network performance/security monitoring and management tools
    ii. Network management frameworks
    iii. Virtual machine performance monitoring
    iv. Security sources (anti-virus)
3. All accounts from trusted domains must be extracted to ensure no domains are missed.
4. Extraction of user accounts by group. Output includes a listing of user objects and the AD Groups they belong to.
5. Identification of active users in the past 90 days based upon the technique(s) employed by the customer (based on output from Step 1).
6. Complete extraction of data from the customer's current management and inventory tools and the calculation of current coverage levels of existing tool(s).
7. Inventory of any missing device, including but not limited to devices that:
    i. Do not report inventory
    ii. Are non-networked
    iii. Are unmanaged devices

Organizational / Technical Assessment: data collection requirements

For the Organizational topics, through interviews/data discovery, make sure to answer/identify:

Organizational Topic	Collection Method	Deliverables / Inventory Data
1. Governance	SAM GDPR Questionnaire - Start Here	Collect or be informed on the customer's IT strategy and/or roadmap, including their current privacy and security concerns and action plans.
	SAM GDPR Questionnaire - Organizational (GDPR)	**Answers on:** privacy policy, accountability, data protection officer (DPO)
2. Personal Data Handling	SAM GDPR Questionnaire - Organizational (GDPR)	**Answers on:** records of processing activities, data processing purpose binding, securing the processing, transfer
	AD Users & Computers *or equivalent*	An inventory of **File server(s)** and **Shared folder(s)** which potentially contain personal data, referenced against the Record(s) of Processing Activities in order to determine the completeness of the record(s) based on data locations.
	MAP Toolkit *or equivalent*	An inventory of **Databases** which potentially contain personal data, referenced against the Record(s) of Processing Activities in order to determine the completeness of the record(s) based on data locations. For Example MAP Toolkit Reports: • SharePointServerUsageTracker; "*Farm and Server Summary"* tab • SQLServerDatabaseDetails; "*DatabaseSummary"* tab • OracleDiscovery; "*Oracle Schemas"* tab
	Samples (manual) OR	An overview of 5 samples for each File server, Shared folder and database identified containing personal data and referenced against the Record(s) of Processing Activities to determine the completeness of the record(s).
	Optional: AIP Scanner or equivalent	*Personal data (in terms of the GDPR) inventory; referenced in detail against the Record(s) of Processing Activities (Shared Folders / Databases / Office 365 / SharePoint On-Premise)*
3. Data Subject Rights Management	SAM GDPR Questionnaire - Organizational (GDPR)	**Answers on:** quality management, access, consent

4. Risk Management	SAM GDPR Questionnaire - Organizational (GDPR)	**Answers on:** Privacy by Design / Default
5. Data Privacy Practices	SAM GDPR Questionnaire - Organizational (GDPR)	**Answers on:** Data Retention
6. Review Data Privacy Practices	SAM GDPR Questionnaire - Organizational (GDPR)	**Answers on:** Evaluation and Monitoring
7. Data Privacy Breach Management	SAM GDPR Questionnaire - Organizational (GDPR)	**Answers on:** Data Leaks

* Partner should be aware this table does not represent a complete list of GDPR requirements, but rather tracks the SAM deliverables to specific GDPR compliance areas to help a customer better map out its larger GDPR compliance strategy.

For the Technical topics, through interviews/data discovery, make sure to answer/identify:

Technical Topic	Collection Method	Deliverables / Inventory Data
1. Inventory and Control of Hardware Assets	SAM GDPR Questionnaire - Start Here	Enumerate all infrastructure platforms in-use by the customer.
	SAM GDPR Questionnaire - Technical (CISv7)	Answers to two (2) questions.
	MAP Toolkit *or equivalent*	Landscape overview to determine the extent of the organizations assets. For Example MAP Toolkit Reports: • InventoryResults; "*Hardware Inventory"* tab • ServerAndCloudEnrollment; "*Windows Server"* tab
	SAM GDPR Questionnaire - Start Here	Enumerate the core business applications in-use by the customer. Enumerate all applications/services in-use by the customer. (Include PaaS, SaaS, DaaS, IDaaS, …)
	SAM GDPR Questionnaire - Technical (CISv7)	Answers to two (2) questions.
	Manual or Automated Collection	An overview of all network devices with vendor, type and firmware revision (if using SCCM or other tools that capture this information as part of discovery process).
	MAP Toolkit *or equivalent*	Life-cycle management inventory to determine the current status of all software assets including operating systems, database engines and applications. Check the End-of-Life status, service pack levels and versions. For Example MAP Toolkit Reports: • LegacyWindowsServerInventory; *"ServerInventory"* tab • WindowsEnvironmentSummary; *"Hardware Inventory | Application Summary"* tab • LinuxEnvironmentSummary; *"Hardware Inventory"* tab
	Optional: MDM Tooling	*Life-cycle management inventory on mobiles devices including the apps. Check the End-of-Life status, service pack levels, and versions.*
3. Continuous Vulnerability Management	SAM GDPR Questionnaire - Technical (CISv7)	Answers to two (2) questions.
	WSUS / Other	An inventory of the patch management status of the customer's systems.
4. Controlled Use of Administrative Privileges	SAM GDPR Questionnaire - Technical (CISv7)	Answers to three (3) questions.
5. Secure Configuration for Hardware and Software on Mobiles Devices, Laptops, Workstations and Servers	SAM GDPR Questionnaire - Technical (CISv7)	Answers to two (2) questions.

6. Maintenance, Monitoring and Analysis of Audit logs	SAM GDPR Questionnaire - Technical (CISv7)	Answers to two (2) questions.
	Domain Controller Security Events, PowerShell Get-EventLog or other tooling	Detect failed logons (30 days) or abuse of privileges.
10. Data Recovery Capabilities	SAM GDPR Questionnaire - Start Here	Collect, or be informed on, the customer's disaster recovery plans.
	SAM GDPR Questionnaire - Technical (CISv7)	Answers to two (2) questions.
	Backup (Report) Tooling	Request a summarized (90 days) report on the current Backup and Restore status to determine the "recoverability" of the organization.
13. Data Protection	SAM GDPR Questionnaire - Technical (CISv7)	Answers to two (2) questions.
	WSUS / SCCM / Other	An inventory of the security measures taken and their status to determine the risks related to cyber threats and mitigation options. • Presence and status of System Center Endpoint Protection (SCEP), Windows Defender or other anti-virus software on all systems. • Presence and status of Firewall software on all systems.
	Optional: Encryption	*Use System Center Configuration Manager or other tools to detect and collect the presence and status of BitLocker or ~~an~~other encryption software.*
14. Controlled Access Based on the Need to Know	SAM GDPR Questionnaire - Technical (CISv7)	Answers to two (2) questions.
16. Account Monitoring and Control	SAM GDPR Questionnaire - Technical (CISv7)	Answers to two (2) questions.
	Group Policy Management	An inventory of the password policy setting information from Active Directory.
	AD Users & Computers, PowerShell Get-ADUser or other tooling	Extract a list of all accounts, including their status (enabled/disabled) and password options. A check within the organization should provide clearance on legitimacy of account enablement.
17. Implement a Security Awareness and Training Program	SAM GDPR Questionnaire - Technical (CISv7)	Answers to two (2) questions.
19. Incident Response and Management	SAM GDPR Questionnaire - Technical (CISv7)	Answer to one (1) question.

4. Analysis

The GDPR SAM Assessment data must be analyzed, reviewed, and agreed upon with the customer as an accurate point-in-time reflection of the customer's current deployment position. This data, along with the additional customer inputs provide a basis for the development of a solid GDPR Assessment unique to the customer. Based on the inputs and data collected, the partner will complete the following required analysis:

1. Aggregation and review of data from stakeholder interviews, noting any information that was either unavailable or challenging for the customer to gather.
2. Assess the customer's data protection practices, at the Organizational and Technical level, based on available policies and procedures related to privacy and data protection and the operational practices involved.
3. Review the customer's current IT environment (mapped to an optimized environment) compared to the customer's current position, including assessment of outdated product versions and editions, patch management policies, backup and disaster recovery practices, and more.

5. Deliverables

The following deliverable is **due to the customer** at the **beginning** of the engagement:

Letter of Engagement. This letter must include at a minimum:

i. A Statement of Work (SOW) for the engagement being performed, including a list of all customer deliverables

ii. Scope of the engagement, including any scope limitations

iii. Dates and timelines

iv. Partner project team members and their relevant Microsoft Certified Professional (MCP) credentials

v. List of key contacts that must include names, titles, phone numbers, and email addresses

vi. Planned disclosure of engagement deliverables to Microsoft

vii. Statement explaining that data collected by partners from customer's information system environment is transferred to Microsoft, and how Microsoft will use that data collected to generate reports necessary for partners to effectuate the SAM services.

viii. Consent from the customer to transfer data to Microsoft, any of its affiliates, and to the sub processors Microsoft may employ to generate the reports necessary for the SAM services, including consent to transfer Personal Information to the United States and other countries where Microsoft's sub processors are located. "Personal Information" means any information provided by Microsoft or collected by partner in connection with this Agreement (a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains, or (b) from which identification or contact information of an individual person can be derived. Personal Information includes, but is not limited to: name, address, phone number, fax number, and email address.
Additionally, to the extent any other information (such as, but not necessarily limited to, a personal profile, unique identifier, and/or IP address) is associated or combined with Personal Information, then such information also will be considered Personal Information.

ix. The Microsoft SAM Engagement data usage and privacy information document ("Data Usage Guide"). Find the current version here.

x. Reference the Data Usage Guide, where appropriate.

The Letter of Engagement must be in writing and signed by authorized representatives of the partner and customer.

The following deliverables are **due to the customer** at the **end** of the engagement:

1. GDPR Assessment Report. This report must contain at a minimum:

    i. An Executive Summary. A high-level summary of project background and scope, engagement result, high-level organizational and technical recommendations and next steps. The report will include a clear statement indicating the GDPR Assessment Report in no way guarantees compliance with the GDPR, but instead provides a foundation for understanding the data environment, processes, and capabilities as they relate to the GDPR and cybersecurity.

ii. An assessment of the customer's overall GDPR practices in relation to their current Organizational and Technical practices.

iii. A short-term GDPR action list roadmap using the provided GDPR and selected CIS control standards as a reference to assist the customer in better understanding protecting the rights of Data Subjects and the organization against the consequences of data leaks.

iv. An assessment of customer's technical and organizational -related policies and procedures, the strengths, weaknesses and areas of opportunity, including recommendations for improvement.

v. Provide directions for seeking assistance on acquiring additional resources on the GDPR and the CIS v7 Controls framework.

2. Additional Uses of Data. In this section of the report, the partner provides specific security related findings. Examples of information that can be included in this report are:
    a. A summary of current or upcoming end-of-life products, with upgrade path recommendations and life-cycle management
    b. A summary of outdated patching
    c. Familiarizing the customer with Microsoft Compliance Manager
    d. Third-party scan solution reports
    e. Critical findings which can be reflected to the report addendum: Optional CIS v7 Controls
3. Established Deployment Position (EDP). A document with details related to all hardware and software currently deployed within the customer's IT infrastructure.

The following deliverables are due to Microsoft as necessary Proof of Execution (POE) in order for the partner to collect Channel Incentives payment.

The SAM partner must notify the Microsoft SAM Engagement Manager when the POE is uploaded into the required system as designated by Microsoft (currently, CHIP). POE includes the following deliverables due to Microsoft upon the completion of the SAM Engagement and must be provided as necessary POE for the partner to collect Channel Incentives payment:

1. Letter of Engagement. This must be the same Letter of Engagement provided to the customer and signed by the customer and the partner **at the beginning of the engagement.**

2. Established Deployment Position (EDP). The EDP, an IAM generated Excel report, provides details related to the customers' Microsoft software deployments and usage data. The software deployments are identified using discovery tools and manual inputs as outlined in section 3. The partner must first input all relevant data into the Customer Inventory Data Contract (CIDC) template, which will be uploaded into IAM. The EDP will then be created by the partner using IAM which is to be given to the customer and Microsoft. EDPs produced outside of IAM will not be accepted as proof of execution. The EDP data must meet or exceed the minimum quality standards published in the current SAM Minimum EDP Quality Standards.
3. GDPR Assessment Report. This must be the same GDPR Assessment Report provided to the customer, as outlined above. This POE deliverable must have no PII within it.
4. Letter of Confirmation (China only)

    The Letter of Confirmation should be drafted after completion of the SAM engagement and requires customer's chop (stamp) or email from customer corporate domain confirming provision of SAM engagement.

    The Letter of Confirmation must include the following statement:

"This is to confirm Microsoft SAM partner <insert partner Name> has implemented SAM service <insert SAM Engagement Type> to customer <insert customer name>."

6. SAM resources

- SAM partner eligibility, program overview, and partner incentive guides
- Microsoft GDPR site
- CIS controls