

AGSA/02/2026: Request for proposal (RFP) for the provision and deployment of a data masking solution for a period of 60-months including configuration, maintenance and support.

No.	Question	Type	Answer
1	Where customers are reluctant to provide signed reference letters due to confidentiality, NDAs, or the sensitive nature of the solution, can alternative evidence be provided?	Technical	In instances where reference letters cannot be obtained, kindly refer to the amended information as per the erratum notice published for this tender on the AGSA website. This must be read together with the uploaded document titled Appendix D: Client References.
2	Can publicly available customer success stories be submitted instead of signed reference letters, with customer verification facilitated through the bidder if required?	Technical	In instances where reference letters cannot be obtained, kindly refer to the amended information as per the erratum notice published for this tender on the AGSA website. This must be read together with the uploaded document titled Appendix D: Client References.
3	After the clarification submission deadline, when will responses be published? Will questions submitted by bidders and the corresponding responses be shared with all participating bidders?	Commercial	The AGSA confirmed that clarification questions may be submitted until 20 July 2026 at 16h00. The enquiries will be consolidated and AGSA will issue one response and such response will be posted, within three business days after the last day of enquiries, onto the AGSA website (www.agsa.co.za) under tenders i.e. next to the same RFP document. Yes. AGSA confirmed that all clarification questions and responses will be shared with all prospective bidders and published on the AGSA website as part of the commitment to fairness, transparency, and equal access to information.
4	What Hypervisor platform are you using?	Technical	The AGSA is currently using the VMware version 7 as the Hypervisor platform.
5	Should we cater for PROD, QA, UAT, DEV as well as DR?	Technical	The bidder must cater for: • Development (DEV) • Testing (SIT- System Integration Testing) • Quality Assurance (UAT - User Acceptance Testing) • Pre-production (Pre-prod) • Production-like environments (QA) NB: The AGSA has the QA, UAT and Pre-prod environments, however, these environments are currently not masked.
6	Would you require the encryption keys to be stored on a HSM?	Technical	The intention of the AGSA is to use Azure key vault for storing encryption keys.
7	Data Discovery and Classification Amount of Data to be discovered and classified on the servers?	Technical	The volume of data to be scanned will depend on the findings identified during the discovery process. However, the AGSA currently maintains the following data volumes, which are expected to increase over time: - Oracle databases with approximately 1.52 Terabytes (TB) for PeopleSoft Finance and 427.35 Gigabytes (GB) for PeopleSoft HR - SQL databases with approximately 5 TB - Microsoft Dataverse - to be discovered NB: The proposed solution discovery and classification should not be limited to the volume of data and the number of systems.
8	Data Discovery and Classification Structured or Unstructured data to be scanned?	Technical	The AGSA requires both structured and unstructured data to be scanned.
9	Data Discovery and Classification What version of OS and DB software are running?	Technical	The AGSA currently operates the following operating system and database versions within the environment: a) OS: Windows Server Enterprise 2012 to 2025 b) Databases: Windows Server Enterprise 2012 to 2022 MS SQL versions and Oracle version is 12c and 19c.
10	Data Discovery and Classification What version of OS are the unstructured servers running on?	Technical	The unstructured data server operating system version is Windows server 2016.
11	Full database Encryption Please confirm the total number of servers to be encrypted. Please note this is licensed per server not a database. Please confirm the database and operating system versions on each server.	Technical	The AGSA does not require full database encryption, however, the proposed solution should be compatible with the native encryption tools included in the databases software.
12	If Native encryption Please confirm the database and operating system versions on each server. Please note its only Oracle and MS SQL supported	Technical	AGSA is currently not fully encrypting databases, however, the tool should support databases that are natively encrypted if the AGSA decide to use the functionality. The AGSA currently operates the following operating system and database versions within the environment: a) OS: Windows Server Enterprise 2012 to 2025 b) Databases: Windows Server Enterprise 2012 to 2022 MS SQL versions and Oracle version is 12c and 19c

AGSA/02/2026: Request for proposal (RFP) for the provision and deployment of a data masking solution for a period of 60-months including configuration, maintenance and support.

No.	Question	Type	Answer
13	File/Folder encryption Please confirm the total number of file servers that need to be protected by encryption.	Technical	The AGSA does not require file folder encryption, however, the proposed solution should be compatible with the native encryption tools included the OS.
14	Tokenization/Masking How many endpoints will the tokenization system have? (An endpoint is for example an instance of an applications that calls the tokenization REST API)	Technical	The primary endpoints are database instances rather than REST API clients. The initial scope includes approximately 6 Oracle database instances, with additional SQL server databases to follow. The long-term estate is estimated at approximately 2 000 database endpoints across multiple platforms, with the number expected to grow. The proposed solution should be capable of scaling to support this growth.
15	Tokenization/Masking Are you looking at doing Static Tokenization or Dynamic Tokenization?	Technical	The AGSA requires support for static tokenization during the initial implementation phase. However, the proposed solution must also support both static and dynamic tokenization capabilities to accommodate future business and security requirements.
16	Tokenization/Masking What version of OS and DB software are running?	Technical	The AGSA currently operates the following operating system and database versions within the environment: a) OS: Windows Server Enterprise 2012 to 2025 b) Databases: Windows Server Enterprise 2012 to 2022 MS SQL versions and Oracle version is 12c and 19c
17	Tokenization/Masking Do you have a QA, UAT or Dev environment that needs to work with a production database, but shouldn't be exposed to sensitive information? Are you using outside contractors for any of this work?	Technical	The AGSA has the QA and UAT environments, however, these environments are currently not masked. NB: The proposed solution should be scalable to mask these instances should masking be required in these environments in future.
18	Database & Environment Sizing (For Software Licensing) What is the estimated total volume of data (in Gigabytes/Terabytes) that requires masking across the in-scope target systems (Oracle, MS SQL Server, MS Dataverse, and Azure Synapse)?	Technical	The AGSA currently maintains the following data volumes, which are expected to increase over time: - Oracle databases with approximately 1.52 Terabytes (TB) for PeopleSoft Finance and 427.35 Gigabytes (GB) for PeopleSoft HR. - SQL databases with approximately 5 TB. NB: The proposed solution should not be limited to the volume of data and the supplier should provide the AGSA with the licensing model as part of the pricing schedule that illustrate licensing costs based on the data volumes.
19	How many non-production target database instances, schemas, or processor cores (CPUs) will require masking?	Technical	The AGSA uses the infrastructure as a service to host the IT environment, the proposed solution should not be limited by the VCPU or cores allocated to the servers.
20	Implementation & Scope of Discovery Is the automated PII discovery and classification scope strictly limited to structured databases, or should it include unstructured repositories (e.g., file shares, SharePoint)	Technical	The automated PII discovery and classification scope must include both structured databases and unstructured repositories.
21	Are there existing security tools (e.g., Microsoft Purview) in use that the proposed solution must integrate with, or should we include a standalone discovery component?	Technical	No, the proposed solution must include its own native discovery component, however, the proposed solution should be able to integrate with security tools such as Microsoft Purview and Microsoft Sentinel if required in future.