

Request for Information for Cloud Backup and Restore, and Cloud External Key Management by the Norwegian Public Sector Cloud Marketplace

Information about the RFI

This Request for Information (RFI) is made by the Norwegian Public Sector Cloud Marketplace (MPS). It concerns Cloud backup and Restore solutions and Cloud External Key Management solutions.

MPS is dedicated to enhancing the accessibility of cloud services and delivering secure, cost-efficient solutions to the Norwegian public sector. The Norwegian public sector consists of approximately 5-600 public sector entities.

The purpose of this RFI is to increase our knowledge about solutions that strengthen control, security and resilience in cloud services. In particular, the RFI seeks to understand how these services can support increased control over data and encryption, as well as reduce reliance on cloud service provider managed services. This request aims to provide a deeper understanding of the market dynamics and critical considerations necessary for successful use of these services.

As part of an effort to address increased information security requirements, MPS is investigating a concept referred to as “Hardened Cloud”. You can read more about this concept on our website: [Forsterket allmenn sky](#). As part of this program, MPS is seeking information regarding the following services:

- Cloud Backup and Restore: Solutions that provide secure backup of data in cloud environments and enable timely and reliable restoration. This includes capabilities for defined Recovery Time Objectives (RTO), protection against data loss and immutable backups. The aim is to ensure data integrity and availability in support of controlled recovery processes.
- Cloud External Key Management: Solutions that enable customer-controlled management of cryptographic keys used by cloud services, through secure external key management. This includes capabilities to control the full key lifecycle management, such as key generation, storage, usage and revocation of keys. The aim is to ensure data confidentiality and to ensure that encrypted data remains under customer control.

Respondents may choose to respond to questions about both services or only one of the services.

The information received from this RFI is intended to be used in the assessment of the market and possibly preparation and planning of future procurement processes.

The content of the RFI is divided into the following sections:

- Contact information/ About the supplier
- Cloud backup and Restore
 - About the services
 - Information security and data protection
 - Price model/ Contract and commercials
- External key management
 - About the services
 - Information security and data protection
 - Price model/ Contract and commercials
- Other

1. General

1.1 Contact information/About the supplier

Company name

Company registration number

Is the company's name the same as the contracting entity?

(1) ☐ Yes

(2) ☐ No

If not, what is the name of the contracting entity?

If not, what is the contracting entity registration number?

In which country is the contracting entity located?

(1) ☐ Norway

(2) ☐ EU/EEA

(3) ☐ UK

(4) ☐ USA

(5) ☐ Other _____

Contact name for this RFI

Contact e-mail

Contact phone number

Do you have operations/ employees in the European Union/European Economic Area (EU/EEA)?

(1) ☐ Yes

(2) ☐ No

Do you have operations/employees in Norway?

(1) ☐ Yes

(2) ☐ No

Do you have employees with Norwegian security clearance?

(1) ☐ Yes

(2) ☐ No

Do you have employees with Norwegian police certificate?

(1) ☐ Yes

(2) ☐ No

Do you have employees in the following regions?

(1) ☐ Norway

(2) ☐ EU/EEA

(3) ☐ Outside EU/EEA

If you have employees in Norway, in which segments do you employ them?

- (1) ☐ Sales
- (2) ☐ Customer support (technical)
- (3) ☐ Technology/operations
- (4) ☐ R&D
- (5) ☐ N/A

Please provide estimated yearly turnover for your company for the last available full year

Is your holding company privately held or listed on a stock exchange?

- (1) ☐ Privately held
- (2) ☐ Listed on stock exchange

Are you interested in further dialogue/ meetings (digital or otherwise) with us regarding the scoped services to the Norwegian public sector? (If yes, please double-check the emailphone number you provided above is correct)

- (1) ☐ Yes
- (2) ☐ No

1.2 Provided services

Which of the following services does your company provide?

- (2) ☐ Cloud Backup and Restore
- (3) ☐ Cloud External Key Management
- (4) ☐ Both

2. Cloud Backup and Restore

2.1 About the services

How are Cloud Backup and Restore services deployed (ref: NIST SP 800-145 Definition of Cloud Computing)?

- (2) ☐ Private
- (3) ☐ Public
- (4) ☐ On-premises
- (5) ☐ Hybrid

Which service models does your service support?

- (1) ☐ IaaS (Infrastructure as a Service)
- (2) ☐ PaaS (Platform as a Service)
- (3) ☐ SaaS (Software as a Service)

Which platforms does your service support?

- (1) ☐ Microsoft (Azure)
- (2) ☐ Amazon Web Services (AWS)
- (3) ☐ Google Cloud
- (4) ☐ IBM Cloud
- (5) ☐ Oracle Cloud Infrastructure (OCI)
- (6) ☐ Other _____

Please insert URL-link(s) to the services you provide

Which of the following capabilities are included in your service offering?

- (1) ☐ Cloud backup (data backup and storage)
- (2) ☐ Cloud restore (data recovery capabilities)
- (3) ☐ Disaster recovery (system/workload)
- (4) ☐ Ransomware protection
- (5) ☐ Immutable backup
- (6) ☐ Other _____

Which workloads are supported by the backup service?

- (1) ☐ Cloud file storage
- (2) ☐ Cloud database
- (3) ☐ Cloud IaaS/PaaS configuration
- (4) ☐ Cloud SaaS (customer data contained within the SaaS)

Which restore capabilities does the service support?

- (1) ☐ Full system/environment restore (restore of an entire system, application or environment)
- (2) ☐ Bare-metal recovery (full system image restore to new or replacement infrastructure with no pre-existing software)
- (3) ☐ Point-in-time restore (restore data or systems to a specific previous point in time)
- (4) ☐ Cross-environment restore (restore between environments e.g. test<i>dev</i>prod)
- (5) ☐ Disaster recovery (recovery of services and data in a new or different environment during major outages or site failures)
- (6) ☐ Other _____

What restore granularity does the service support?

- (1) ☐ Full system/VM restore

- (2) ☐ Volume/disk restore
- (3) ☐ File-level restore
- (4) ☐ Application/object-level restore
- (5) ☐ Other _____

What Recovery Time Objective (RTO) levels are supported for backup and recovery?

- (1) ☐ > 24 hours
- (2) ☐ 4–24 hours
- (3) ☐ 1–4 hours
- (4) ☐ < 1 hour
- (5) ☐ Near-Zero RTO (continuous availability)

Is the stated RTO guaranteed (contract/SLA-backed)?

- (1) ☐ Yes
- (2) ☐ No

Are backups protected against modification or deletion after creation (immutable backups)?

- (1) ☐ Yes, default
- (2) ☐ Yes, configurable per customer
- (3) ☐ No

Do you offer air-gapped backup?

- (1) ☐ Yes, isolated environment
- (2) ☐ No

Is there any use of customer-related information/ data (such as content, metadata, access logs, configurations, usage data etc.) for service improvement/ analytics?

- (1) ☐ Never

- (2) ☐ Only anonymized/aggregated
- (3) ☐ Limited to only metadata
- (4) ☐ May be used if not opted out
- (5) ☐ Not disclosed

To which extent do you offer support for the customer?

- (1) ☐ Included in fully managed service
- (2) ☐ Implementation and onboarding support
- (3) ☐ Technical support and customer support
- (4) ☐ No support provided
- (5) ☐ Other _____

What support do you provide when a disaster recovery or backup restore is initiated?

- (1) ☐ Customer performs and manages the recovery independently
- (2) ☐ Guided recovery – the vendor provides documentation and guidance upon request
- (3) ☐ Assisted recovery – the vendor actively supports the customer through the recovery process
- (4) ☐ Managed recovery – the vendor manages and executes the recovery process on behalf of the customer
- (5) ☐ Other _____

2.2 Information security and data protection

Select the certifications/audit reports your company holds (Cloud Backup and Restore):

- (2) ☐ ISO 27001
- (3) ☐ FIPS 140-3 or 140-2
- (4) ☐ SOC2 Type II

- (5) ☐ CSA Star
- (6) ☐ Other _____

Which of the following standards does your company comply with/operate according to (Cloud Backup and Restore)?

- (1) ☐ NIST Cybersecurity Framework 2.0
- (2) ☐ BSI C5 – Basic Requirements
- (3) ☐ BSI C5 – Additional Requirements
- (4) ☐ NIST SP 800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information
- (5) ☐ FIPS 140-3 or 140-2
- (6) ☐ NSM ICT Security Principles (NSM Grunnprinsipper v 2.1)
- (7) ☐ The Code of Conduct for Information Security and Data Protection (Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren)
- (8) ☐ Other _____

Do you consider yourself a processor, controller or both according to GDPR (Cloud Backup and Restore)?

- (1) ☐ Processor
- (2) ☐ Controller
- (8) ☐ Joint controller
- (3) ☐ Both
- (10) ☐ None

Where is the data stored?

- (1) ☐ Norway
- (2) ☐ Sweden
- (3) ☐ Finland
- (4) ☐ Denmark

- (5) ☐ EU/EEA
- (6) ☐ Switzerland
- (8) ☐ Configurable per customer
- (7) ☐ Outside EU/EEA _____

Can it be guaranteed that customer-related information/data (such as content, metadata, access logs, configurations, usage data etc.) will not leave the location selected by the customer?

- (1) ☐ Yes (technically enforced)
- (2) ☐ Yes (contractually enforced)
- (3) ☐ No

Is there a risk that data may leave the EU/EEA under any of the following circumstances?

- (1) ☐ MLAT
- (2) ☐ Cloud Act
- (3) ☐ Emergency procedures
- (4) ☐ Customer misconfiguration of services
- (5) ☐ Technical failure
- (6) ☐ Support/operations
- (7) ☐ None

Can any third-party, including national authorities, access data without customer consent?

- (1) ☐ No
- (2) ☐ Yes, customer will always be notified
- (3) ☐ Yes, notification is not guaranteed

Security incident notification to affected customers (Cloud Backup and Restore)

- (1) ☐ > 72 hours
- (2) ☐ < 72 hours
- (3) ☐ < 24 hours

Data deletion upon termination of the contract (Cloud Backup and Restore)

- (1) ☐ Not guaranteed
- (2) ☐ Logical deletion (data removed from system, may still exist on storage)
- (3) ☐ Cryptographic deletion (data made unreadable by deleting encryption keys)
- (4) ☐ Verifiable deletion (deletion can be proven via logs or audit evidence)
- (5) ☐ Physical/media deletion (data destroyed by wiping or destroying storage media)

Does your company have sub-processors outside the EU/EEA (Cloud Backup and Restore)?

- (1) ☐ Yes
- (2) ☐ No

Under which contract is data protected in Norway/EU/EEA (Cloud Backup and Restore)?

- (1) ☐ Your company's own data processing agreement
- (2) ☐ The EU Commission's Standard Contractual Clauses (2010), art. 28
- (3) ☐ The EU Commission's Standard Contractual Clauses (2021), art. 28
- (4) ☐ The Danish data processing agreement (Datatilsynet, DK)
- (5) ☐ The Norwegian data processing agreement (Datatilsynet, NO)
- (6) ☐ Other _____

Under which contract is data protected if, for any reason, any part of the data leaves the EU (Cloud Backup and Restore)?

- (1) ☐ The EU Commission's Standard Contractual Clauses (2010), art. 46
- (2) ☐ The EU Commission's Standard Contractual Clauses (2021), art. 46

- (3) ☐ Binding Corporate Rules
- (4) ☐ U.S.-EU Data Privacy Framework
- (5) ☐ Other _____

2.3 Price model/Contract and commercials

Does your company operate with publicly available price lists (Cloud Backup and Restore)?

- (2) ☐ Yes
- (3) ☐ No
- (4) ☐ Partial

What are the main factors driving the costs of the Cloud Backup and Restore service?

- (1) ☐ Amount of data stored (GB/TB)
- (2) ☐ Number of systems/applications
- (3) ☐ How often backups are taken
- (4) ☐ How often data is restored
- (5) ☐ Retention period
- (6) ☐ Speed of recovery required
- (7) ☐ Support levels/Service Level Agreements (SLA)
- (8) ☐ Other _____

What is your licensing model for Cloud Backup and Restore?

- (1) ☐ Subscription-based
- (2) ☐ Consumption/usage based
- (3) ☐ User-based
- (4) ☐ Workload-based
- (5) ☐ Capacity-based (e.g. storage volume)

- (6) ☐ Hybrid (combination of two or more)
- (7) ☐ Other _____

Does your company currently have government entities or public sector entities (globally) as customers for Cloud Backup and Restore?

- (1) ☐ Yes
- (2) ☐ No

Do you sell directly or through resellers/channel partners or similar to the public sector (Cloud Backup and Restore)?

- (1) ☐ Directly
- (2) ☐ Resellers/channel partners or similar
- (3) ☐ We are resellers/channel partners or similar
- (4) ☐ We offer both solutions

Are there special licensing terms for public sector clients (Cloud Backup and Restore)?

- (1) ☐ Yes
- (2) ☐ No

3. Cloud External Key Management

3.1 About the services

How is the Cloud External Key Management service deployed (ref: NIST SP 800-145 Definition of Cloud Computing)?

- (2) ☐ Private
- (3) ☐ Public
- (4) ☐ On-premises
- (5) ☐ Hybrid

Which cloud service models does your External Key Management service support?

- (1) ☐ IaaS (Infrastructure as a Service)
- (2) ☐ PaaS (Platform as a Service)
- (3) ☐ SaaS (Software as a Service)
- (4) ☐ On-premises/hybrid support

Which platforms does your External Key Management service support?

- (1) ☐ Microsoft (Azure)
- (2) ☐ Amazon Web Services (AWS)
- (3) ☐ Google Cloud
- (4) ☐ IBM Cloud
- (5) ☐ Oracle Cloud Infrastructure (OCI)
- (6) ☐ Other _____

Please insert URL-link(s) to the External Key Management services you provide

Which encryption key management models do you support?

- (1) ☐ Customer managed encryption keys (CMEK)
- (2) ☐ Bring your own key (BYOK)/HSM
- (3) ☐ External key management services (EKM)/HSM (also called hold your own key – HYOK)
- (4) ☐ Provider managed keys (PMK)
- (5) ☐ Other _____

For CMEK: who is the defined legal owner of the encryption keys in the service agreement?

- (1) ☐ Customer
- (2) ☐ External key management provider
- (3) ☐ Cloud service provider
- (4) ☐ Shared (as defined in contract)
- (5) ☐ N/A – model not offered

For BYOK: who is the defined legal owner of the encryption keys in the service agreement?

- (1) ☐ Customer
- (2) ☐ External key management provider
- (3) ☐ Cloud service provider
- (4) ☐ Shared (as defined in contract)
- (5) ☐ N/A – model not offered

For EKM/HYOK: who is the defined legal owner of the encryption keys in the service agreement?

- (1) ☐ Customer
- (2) ☐ External key management provider
- (3) ☐ Cloud service provider
- (4) ☐ Shared (as defined in contract)
- (5) ☐ N/A – model not offered

For PMK: who is the defined legal owner of the encryption keys in the service agreement?

- (1) ☐ Customer
- (2) ☐ External key management provider
- (3) ☐ Cloud service provider

- (4) ☐ Shared (as defined in contract)
- (5) ☐ N/A – model not offered

For CMEK: who retains technical ownership of the encryption keys at all times (ability to generate, use, and authorize key usage)?

- (1) ☐ Customer exclusively (no provider involvement)
- (2) ☐ Customer primary control, external key management provider assists under strict customer-controlled conditions
- (3) ☐ Shared control between customer and external key management provider
- (4) ☐ External key management provider controlled
- (5) ☐ N/A – model not offered

For BYOK: who retains technical ownership of the encryption keys at all times (ability to generate, use, and authorize key usage)?

- (1) ☐ Customer exclusively (no provider involvement)
- (2) ☐ Customer primary control, external key management provider assists under strict customer-controlled conditions
- (3) ☐ Shared control between customer and external key management provider
- (4) ☐ External key management provider controlled
- (5) ☐ N/A – model not offered

For EKM/HYOK: who retains technical ownership of the encryption keys at all times (ability to generate, use, and authorize key usage)?

- (1) ☐ Customer exclusively (no provider involvement)
- (2) ☐ Customer primary control, external key management provider assists under strict customer-controlled conditions
- (3) ☐ Shared control between customer and external key management provider
- (4) ☐ External key management provider controlled
- (5) ☐ N/A – model not offered

For PMK: who retains technical ownership of the encryption keys at all times (ability to generate, use, and authorize key usage)?

- (1) ☐ Customer exclusively (no provider involvement)
- (2) ☐ Customer primary control, external key management provider assists under strict customer-controlled conditions
- (3) ☐ Shared control between customer and external key management provider
- (4) ☐ External key management provider controlled
- (5) ☐ N/A – model not offered

Under any circumstances, can the external key management provider access or use customer encryption keys?

- (1) ☐ No (technically impossible)
- (2) ☐ Yes, with explicit customer authorization
- (3) ☐ Yes, under specific operational scenarios (e.g. support, recovery)
- (4) ☐ Yes (provider has inherent access)

Can the customer revoke external key management provider access to keys in real time?

- (1) ☐ Yes, immediate and technically enforced
- (2) ☐ Yes, but with delay and dependencies on provider
- (3) ☐ No

Can the cloud service provider decrypt customer-related information/data (such as content, metadata, access logs, configurations, usage data etc.) without interaction with the external key management system?

- (1) ☐ No (cryptographically impossible without external key access)
- (2) ☐ Yes, under customer-controlled key retrieval only
- (3) ☐ Yes, under limited operational conditions (e.g. support, recovery)
- (4) ☐ Yes (provider has inherent ability to decrypt)

In which jurisdictions are keys, key metadata, and key backups physically located?

- (1) ☐ Norway
- (2) ☐ Sweden
- (3) ☐ Finland
- (4) ☐ Denmark
- (5) ☐ EU/EEA
- (6) ☐ Switzerland
- (7) ☐ Outside EU/EEA _____

In which jurisdictions are keys, key metadata, and key backups logically managed and accessible?

- (1) ☐ Norway
- (2) ☐ Sweden
- (3) ☐ Finland
- (4) ☐ Denmark
- (5) ☐ EU/EEA
- (6) ☐ Switzerland
- (7) ☐ Outside EU/EEA _____

How are encryption keys stored?

- (1) ☐ No dedicated key storage (keys are stored in software alongside the application)
- (2) ☐ Software-based key storage (keys are stored in a dedicated software vault or key management service)
- (3) ☐ Shared HSM (keys are stored in a certified hardware security module shared across customers)
- (4) ☐ Dedicated HSM (keys are stored in a hardware security module exclusively allocated to and controlled by the customer)

What is the availability in case of key management service outage?

- (1) ☐ Services stop
- (2) ☐ Temporary key caching
- (3) ☐ Full redundancy/failover

Is there any use of customer-related information/ data (such as content, metadata, access logs, configurations, usage data etc.) for service improvement/ analytics (External Key Management)?

- (1) ☐ Never
- (2) ☐ Only anonymized/aggregated
- (3) ☐ Limited to only metadata
- (4) ☐ May be used if not opted out
- (5) ☐ Not disclosed

Can the encrypted keys, data or metadata be subject to access requests under non-EEA laws (e.g. extraterritorial laws)?

- (1) ☐ No
- (2) ☐ Yes, customer is always notified
- (3) ☐ Yes, notification not guaranteed
- (4) ☐ Not disclosed

At what point is data encrypted?

- (1) ☐ Before leaving customer environment
- (2) ☐ Within provider infrastructure
- (3) ☐ At rest only
- (4) ☐ Not clearly defined

To which extent do you offer support for the customer (External Key Management)?

- (1) ☐ Included in fully managed service
- (2) ☐ Implementation and onboarding support

- (3) ☐ Technical support and customer support
- (4) ☐ No support provided
- (5) ☐ Other _____

3.2 Information security and Data protection

Select the certifications/audit reports your company holds (External Key Management):

- (2) ☐ ISO 27001
- (3) ☐ FIPS 140-3 or 140-2
- (4) ☐ SOC2 Type II
- (5) ☐ CSA Star
- (6) ☐ Other _____

Which of the following standards does your company comply with/operate according to (External Key Management)?

- (1) ☐ NIST Cybersecurity Framework 2.0
- (2) ☐ BSI C5 – Basic Requirements
- (3) ☐ BSI C5 – Additional Requirements
- (4) ☐ NIST SP 800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information
- (5) ☐ FIPS 140-3 or 140-2
- (6) ☐ NSM ICT Security Principles (NSM Grunnprinsipper v 2.1)
- (7) ☐ The Code of Conduct for Information Security and Data Protection (Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren)
- (8) ☐ Other _____

Do you consider yourself a processor, controller or both according to GDPR (External Key Management)?

- (1) ☐ Processor

- (2) ☐ Controller
- (3) ☐ Joint controller
- (4) ☐ None
- (5) ☐ Both

Where are the encryption keys/data stored?

- (1) ☐ Norway
- (2) ☐ Sweden
- (3) ☐ Finland
- (4) ☐ Denmark
- (5) ☐ EU/EEA
- (6) ☐ Switzerland
- (7) ☐ Outside EU/EEA _____
- (8) ☐ Configurable per customer

Can it be guaranteed that encryption keys/ customer-related information/ data (such as content, metadata, access logs, configurations, usage data etc.) will not leave the location selected by the customer?

- (1) ☐ Yes (technically enforced)
- (2) ☐ Yes (contractually enforced)
- (3) ☐ No

Is there a risk that encryption keys/ data may leave the EU/EEA under any of the following circumstances?

- (1) ☐ MLAT
- (2) ☐ Cloud Act
- (3) ☐ Emergency procedures
- (4) ☐ Customer misconfiguration of services
- (5) ☐ Technical failure

(6) ☐ Support/operations

(7) ☐ None

Can any third-party, including national authorities, access encryption keys/data without customer consent?

(1) ☐ No

(2) ☐ Yes, customer will always be notified

(3) ☐ Yes, notification is not guaranteed

Security incident notification to affected customers (External Key Management)

(1) ☐ > 72 hours

(2) ☐ < 72 hours

(3) ☐ < 24 hours

Data deletion upon termination of the contract (External Key Management)

(1) ☐ Not guaranteed

(2) ☐ Logical deletion (data removed from system, may still exist on storage)

(3) ☐ Cryptographic deletion (data made unreadable by deleting encryption keys)

(4) ☐ Verifiable deletion (deletion can be proven via logs or audit evidence)

(5) ☐ Physical/media destruction (data destroyed by wiping or destroying storage media)

Does your company have sub-processors outside the EU/EEA (External Key Management)?

(1) ☐ Yes

(2) ☐ No

Under which contract is data protected in Norway/EU/EEA (External Key Management)?

- (1) ☐ Your company's own data processing agreement
- (2) ☐ The EU Commission's Standard Contractual Clauses (2010), art. 28
- (3) ☐ The EU Commission's Standard Contractual Clauses (2021), art. 28
- (4) ☐ The Danish data processing agreement (Datatilsynet, DK)
- (5) ☐ The Norwegian data processing agreement (Datatilsynet, NO)
- (6) ☐ Other _____

Under which contract is data protected if, for any reason, any part of the data leaves the EU (External Key Management)?

- (1) ☐ The EU Commission's Standard Contractual Clauses (2010), art. 46
- (2) ☐ The EU Commission's Standard Contractual Clauses (2021), art. 46
- (3) ☐ U.S.-EU Data Privacy Framework
- (4) ☐ Binding Corporate Rules
- (5) ☐ Other _____

3.3 Price model/ Contract and commercials

Does your company operate with publicly available price lists (External Key Management)?

- (2) ☐ Yes
- (3) ☐ No
- (4) ☐ Partially

What are the main factors driving the costs of the External Key Management service?

- (1) ☐ Number of encryption keys managed
- (2) ☐ Level of control required (e.g. customer managed vs. external management)
- (3) ☐ Security level/compliance requirements
- (4) ☐ Support level/Service Level Agreements (SLA)

(5) ☐ Other _____

What is your licensing model for External Key Management?

- (1) ☐ Subscription
- (2) ☐ Per key operation (encrypt/decrypt)
- (3) ☐ Per key/key version managed
- (4) ☐ HSM capacity
- (5) ☐ Hybrid (combination of two or more)
- (6) ☐ Other _____

Does your company currently have government entities or public sector entities (globally) as customers for cloud external key management?

- (1) ☐ Yes
- (2) ☐ No

Do you sell directly or through resellers/channel partners or similar to the public sector (External Key Management)?

- (1) ☐ Directly
- (2) ☐ Resellers/channel partners or similar
- (3) ☐ We are resellers/channel partners or similar
- (4) ☐ We offer both solutions

Are there special licensing terms for public sector clients (External Key Management)?

- (1) ☐ Yes
- (2) ☐ No

4. Other

Is there anything else you believe we should be aware of in the process of going through with a procurement process within this topic?
