CSP providing data services for the health sector

SLA - Ready
Making Cloud SLAs readily usable in the EU private sector

An SME in the Health Sector who has built its SaaS application on an IaaS/PaaS from the CSP. Anyone in the health sector has to be compliant to mandatory sectorial standards and needs to have certain certifications. Furthermore, since this SME will process sensitive personal data, it also needs to encrypt the data in light of the applicable personal protection regulations in the EU. Even though many CSPs have such specific certifications, encryption possibilities and back up possibilities, in most cases the layers in the provided IaaS/PaaS where the customer of the SaaS CSP processes its sensitive and other data do not fall under these certifications, or encryption and back-up by default. This SME made the mistake in trusting that the provided certifications were applicable for that use, where it does not.

User Type: SME

User Maturity: Novice, Basic

Cloud Service lifecycle phase: Acquisition, Operation

Cloud usage: Processing Sensitive Data, Data Integrity

High priority practices

Feasibility of specials & customizations

Always assess, prepare and negotiate. The default cloud SLAs which are initially made available by providers may be less hard-coded, fixed and non-negotiable as customers may think. This is especially applicable now, as the cloud services market is still maturing

Data Management SLOs

The SLA may specify related SLOs contained in additional documents like the EC's "SLA Standardisation Guidelines". In particular, the Cloud Service Provider is expected to clearly define the used data classification scheme, data deletion mechanism, data portability format, and relevant links to the personal data protection SLOs (e.g., in relationship to the data deletion SLOs).

Metrics definitions associated to these SLOs should be based on a standardised model e.g., ISO/IEC 19086-2.

Security SLOs

This good practice improves the accountability level of the CSP. Beyond a list of applicable security certifications, as part of the SLA, the Cloud Service Provider is expected to present a set of quantitative/qualitative SLOs in areas like:

- Organisation of Information Security;
- Human Resources Security;
- Asset Management; Access Control;
- Cryptography;
- Physical and Environmental Security;
- Operations Security;
- Communications Security;
- Systems Acquisition;
- Development and Maintenance;
- Supplier Relationships;
- Information Security Incident Management;
- Business Continuity Management;
- Compliance.

It is important to note that in this case the structure/classification of the specified security SLOs should be consistent with that used in the security certifications the provider refers to. For example security SLOs in ISO/IEC 19086-4, along with their corresponding implementation guidance, are structured according to ISO/IEC 27002 and 27017.

Specified security SLOs/SQOs should make reference to the verifiable evidence associated to the corresponding and agreed metrics.

The security SLOs, and more in general the cloud SLA, should be specified in compliance with ISO/IEC 19086-1, ISO/IEC 19086-2, and ISO/IEC 19086-3. This will provide the CSC with details related to topics like SLO/SQO monitoring, applicable remedies, metrics specification, and core requirements.

Furthermore, for highly important security SLOs it is a good practice for customers to obtain from the CSP the information/tools required for monitoring the agreed security commitments continuously.

Particular attention should be paid to the "Information Security Incident Management" component, where it is expected for the Cloud Service Provider to notify consumers of the occurrence of any breach of its system, regardless of the parties or data directly impacted.

Metrics play an important role in critical SLA-Ready Common Reference Model security components. Metrics and standards for measuring performance and effectiveness of information security management should be established prior to agreeing on the cloud SLA. As a minimum, customers should understand and document their current metrics and how they will change when operations are moved into the cloud and where a provider may use different metrics. Agreed metrics should be compliant with a relevant standard like ISO/IEC 19086-2.

Personal Data Protection SLOs

The SLA may specify related SLOs contained in additional documents like the EC's "SLA Standardisation Guidelines". Metrics definitions associated to these SLOs should be based on a standardised model e.g., ISO/IEC 19086-2.

Medium priority practices

- SLA URL
- Findable
- Roles and Responsibilities
- Cloud SLA Definitions
- Revision Date
- Update Frequency
- General Carveouts
- Specified SLO Metrics

Low priority practices

- Choice of Law
- Previous versions and revisions
- SLA Duration
- Machine Readable Format
- Number of Pages
- Contact Details
- Contact Availability
- Service Credit
- Service Credits Management
- Maximum service credits (Euro amount) provided by the CSP
- SLA Change Notifications
- Unilateral Change
- Service Level Reporting
- Service Level Continuous Monitoring
- General SLOs
- Cloud Service Performance SLOs
- Service Reliability SLOs

Click and download your tailored tips on Cloud Service Level Agreements

SLA Ready has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644077