

A European SME who has formally used CRM SaaS to keep track of its customer relationship management and sales cycle would like to switch certain part of its data to another account in the same CRM SaaS, and - when that did not work out - to switch that data to another CSP. This in turn requires the ability to migrate data between different environments or providers. However, the former CRM SaaS did not specify anything on data portability, data format, what data would exactly be possible to migrate, and what not, or whether metadata would be part of that. The SME settled for getting part of its data out in a structured, workable way, where the remainder of its data cannot be extracted or otherwise exported in a suitable way so basically lost the latter data and related analytics.

User Type: SME

User Maturity:

Novice, Basic,
Experienced

Cloud Service lifecycle phase:

Operation, Termination

Cloud usage: App

on a Cloud, Cloud
Bursting, Processing
Sensitive Data

High priority practices

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
- » Choice of law
- » Roles and responsibilities
- » Cloud SLA definitions
- » SLA duration
- » Contact details
- » Contact availability
- » SLA change notifications
- » Unilateral change
- » General Carveouts

Low priority practices

- » Revision date
- » Update Frequency
- » Previous versions and revisions
- » SLA language
- » Machine-readable format
- » Nr. of pages
- » Service Credit
- » Service credits assignment
- » Maximum service credits (Euro amount) provided by the CSP
- » Service Levels reporting
- » Service Levels continuous reporting
- » Feasibility of specials & customizations
- » Specified SLO metrics

[Click and download your tailored tips on Cloud Service Level Agreements](#)

