Annex B
Core Principles

- Data location

During the whole life cycle of data (generation, data processing, storage, backup, archival) the data must be located in Europe (Schengen/EU) for corporate and non critical data. The same requirement applies for all accesses to the data for reasons like administration and other operations. The CSP has to declare all locations where the data is stored or processed and where the data is accessed from.

- Encryption

Encryption shall be broadly offered and used wherever it is possible in a reasonable manner. Preferably national and international standards shall be used. The CSP has to manage all processes using encryption policies for storage, administration and data flows between customer and CSP infrastructures.

- Secure data life cycle

Access management, data processing, data destruction and reversibility of data are essential for cloud security. Therefore clearly defined, specific rules for access rights throughout the whole data life cycle must be in place. Customer data is owned by the customer and must be treated alike.

- Identity and access management (IAM)

Identities, authentication and authorization must be managed using processes. Specific roles need to be well defined and in place. A clear set of access rights for data, services and assets must be used. CSP must be able to control and manage all access rights, roles and privileges granted to users on its service and its infrastructure. Permissions and rights needs to be enforced.

- Human resources

CSP staff must be reliable and subject to security clearances (e. g. criminal record check) for critical positions (e. g, administrator). Skills should be managed.

- Management of subcontractors (3rd party management)

Cloud service providers' subcontractors need to be identified and mapped. This should be transparent for the cloud customer. Security requirements must be passed to subcontractors and regulated by the contracts. Liability clauses must also be part of the contracts.

- Legal and contractual aspects

Contracts should preferably be provided in the national language and only (exclusively) one European law should be applicable to the contract - preferably the national law of the customer. SLAs should contain all relevant information for the cloud service and be clearly advertised and explained to the customer. SLAs should be transparent in their terms. The contract needs to address precisely the exit scenario (e. g. reversibility, appropriate periods). Responsibilities and liabilities between customer and CSP must be well defined. Transparency on data location and applicable law must be part of the contract.

- Security incidents management and monitoring

CSP should rely on infrastructure supervision in order to detect, to assess and to remediate cloud security incidents. Internal processes for incident detection must be defined and operational. The incidents must be defined, categorized and communicated to the relevant authorities. This implies the collection of data and information about the incident. A proper solution and remediation must be found in case of an incident by the provider. Communication to the customers shall be defined and established and the customers have to be informed about the incident according to the definition of the communication.

- Compliance and Data protection

Sensitive data and data protected by national and European regulation must be labeled as such and must be handled in accordance with European and national regulations. Physical and logical access to the data needs to be secured and documented. The management of data handling should be documented in a policy.

- Change management

CSP must have a process based and well documented change management in place. It should be valid for all areas within the organization. It is especially critical for a stable cloud service delivery (e. g. revert back to a previous stable state in case of problems)

- Separation of production and non-production environments

Development, test and production environments should be separated in order to limit the impact of failure on one of these environments. While tests may be performed in the production environment developers should not have extended rights over the production infrastructure and real user data.

- Network and communication

Separation of tenants should be established for network communication. Depending on risk assessment the tenants' assets should be secured logically or physically. The perimeter has to be secured so that only legitimate data flows are authorized.

- Portability (reversibility) and Interoperability

There should be no technical or contractual barriers hindering the customer to switch providers. Customer data should be transferred back to the customer through formats, protocols and APIs. These need to be specified beforehand in the contract between the CSP and the customer. These formats, protocols and APIs must be reusable documented and accessible by the customer. It is recommended that these protocols, formats and APIS be publicly documented and available. The CSP must allow the outgoing customer to be able to use the data in a way so that its business continuity is not affected.

- Business continuity

CSPs should ensure the business continuity of its customers through reasonable performance and Service Level Agreements. Provider should ensure its capability to deliver its service in case of failure of a part of its infrastructure or platform. Redundant means for the service should be available at no additional costs and conform to the same set of requirements applied to the original service. CSP must have a tested and documented its business continuity management.

- Information Security Management

CSP should have a set of policies defining its processes managing information security and a proper mapping of its infrastructure and information systems. Roles and liabilities inside its organization should as well be defined.