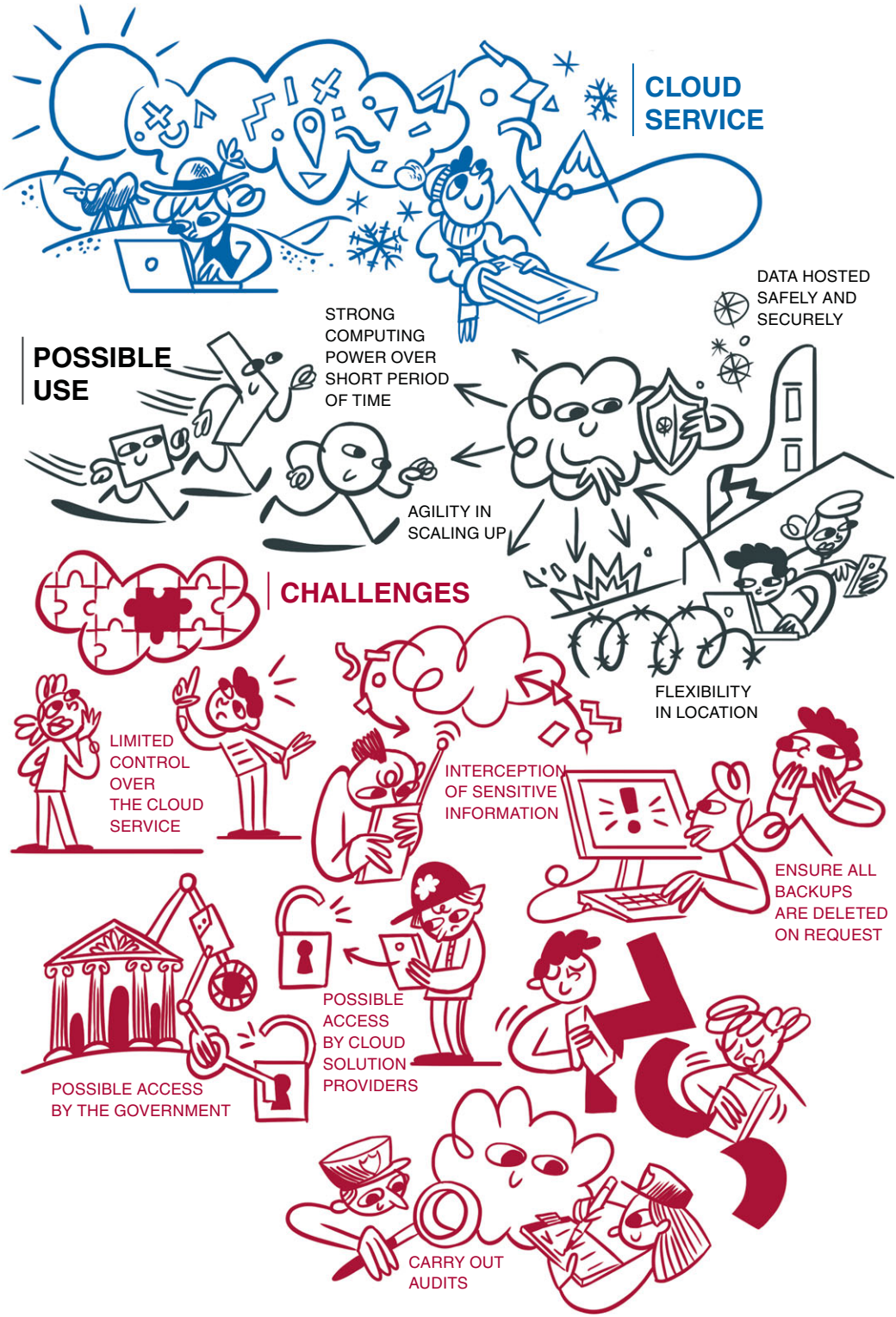

CHAPTER 10

# CLOUD SERVICES

**Paolo Balboni**

## 10.1 INTRODUCTION

The most widely used definition of "cloud computing" is the one published by the US National Institute of Standards and Technology (NIST),[1] according to which, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". The NIST document defines three service models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), and four deployment models: public, private, community and hybrid cloud environments,[2] although it should be borne in mind that new models are being developed all the time.

Cloud computing can facilitate and accelerate the creation and Processing of large collections of data and the production of new services and applications. It also makes deployment more agile. As humanitarian assistance is driven by information, cloud computing services and their related data Processing paradigm have become a helpful tool for Humanitarian Organizations. Their benefits include access to large amounts of computing power over short periods of time, elasticity and flexibility about the location and flow of data, and cost savings.[3]

However, Cloud Services can also bring risks and challenges for privacy and data protection. These can generally be grouped into two main categories: first, the lack of control over the data, and second, the absence of transparency about the Processing operation itself. For Humanitarian Action the following risks are of particular importance:

- the use of services from unprotected locations;
- the interception of sensitive information;
- weak authentication;
- data can be stolen from the Cloud Service provider, for instance by hackers;
- possible access by government and law enforcement authorities;[4]

1 Mell and Grance, *The NIST Definition of Cloud Computing*.

2 European Data Protection Supervisor (EDPS), "Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the Potential of Cloud Computing in Europe'", Opinion (Brussels, 16 November 2012), 4: https://edps.europa.eu/sites/default/files/publication/12-11-16_cloud_computing_en_0.pdf.

3 See Dara G. Schniederjans, Koray Ozpolat and Yuwen Chen, "Humanitarian supply chain use of cloud computing", *Supply Chain Management: An International Journal*, 8 August 2016: https://doi.org/10.1108/SCM-01-2016-0024.

4 On law enforcement access to the cloud see Chapter 11: Cloud and government access. For further considerations, see also, for example, Paolo Balboni and Enrico Pelino, "Law enforcement agencies' activities in the cloud environment: A European legal perspective", *Information & Communications Technology Law*, Vol. 22, No. 2, 2013, pp. 165–190.

- long data Processing chains of subcontractors out of effective control;
- further Processing, incompatible with the original purpose(s), by the cloud provider and/or its subcontractors;
- extra retention of data by the cloud provider and/or its subcontractors;
- unauthorized (International) Data Sharing.

The data protection implications of cloud computing were highlighted by the International Conference of Privacy and Data Protection Commissioners in its Resolution on Cloud Computing, adopted in Uruguay in 2012.[5]

In addition, those Humanitarian Organizations that enjoy privileges and immunities under international law should be aware that outsourcing Personal Data Processing to a Third Party Cloud Service provider may put their data at risk of loss of such privileges and immunities. More details on the possible implications of privileges and immunities in a cloud environment are set out in Section 10.9 – Privileges and immunities and the cloud, below.

The three main types of Cloud Service models can be described as follows:[6]

- **Infrastructure as a Service (IaaS):** an IaaS cloud offers access to the raw computing resources of a Cloud Service. Rather than purchasing hardware itself, the cloud customer purchases access to the cloud provider's hardware according to the capacity required.
- **Platform as a Service (PaaS):** a PaaS cloud offers access to a computing platform which allows cloud customers to write applications to run on that platform or another instance of it. The platform may in turn be hosted on a cloud IaaS.
- **Software as a Service (SaaS):** a SaaS cloud offers access to a complete software application which the cloud user accesses through a web browser or other software. Accessing the software in this manner eliminates or reduces the need to install software on the client machine and allows the service to support a wider range of devices. The software may in turn be hosted on a cloud platform or infrastructure.

There are also different types of cloud infrastructure. A private cloud is operated solely for a single organization, whether managed internally or by a Third Party, and hosted either internally or externally. In a public cloud, the services are rendered over a network that is open for public use. A community cloud is a cloud service jointly available to a number of organizations that shares common interests, concerns and/or requirements

5 See International Conference of Data Protection and Privacy Commissioners, Resolution on Cloud Computing, Resolution (34th International Conference of Data Protection and Privacy Commissioners, Punta del Este / Canelones, Uruguay, 26 October 2012): http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Cloud-Computing.pdf.

6 UK Information Commissioner's Office (ICO), *Guidance on the use of cloud computing*, Version: 1.1, 2 October 2012, 5–6: https://ico.org.uk/your-data-matters/online/cloud-computing.

(e.g. security, compliance requirements, jurisdiction, privileges and immunities, etc.). A hybrid cloud is a composition of two or more clouds that remain distinct entities but are bound together, offering the benefits of multiple deployment models.

Each of these models has advantages and disadvantages. A public cloud is more accessible, as the information is stored offsite and therefore is available from anywhere via the Internet. It offers the ability to scale up server capacity at short notice and can potentially save money. It can also be reviewed regularly with security and performance updates and improvements. On the other hand, as a public cloud is dependent on Internet connectivity there is the risk of losing control over data because of unknown or unauthorized data transfer from one jurisdiction to another, false deletion of data, retention after the termination of services, hacking and security attacks. It is difficult to identify where the data are stored in a public cloud at a particular point in time, and deletion is almost never possible because of the many unmonitored backups. In addition, there are many privacy and confidentiality concerns, such as the fact that the Processing may be subject to a range of different applicable legislation which could mandate compulsory and unauthorized release of data and the potential for authorities to exercise jurisdiction.

In a private/internal cloud, data are kept within the organization's internal network, and therefore are not publicly accessible. It offers a more controlled environment and a limited number of users, so creating less risk of Third Party disclosure. A private cloud can have the same usability, scalability and flexibility as a public cloud. Its disadvantages, though, are the cost and the fact that it may not have the latest performance and security upgrades/improvements.

A community cloud can be managed internally or by a Third Party and hosted internally or externally. So, the advantages and disadvantages of this typology depend on how it is managed. Interestingly, organizations that share common interests, concerns and/or requirements can have together more negotiating power towards the cloud provider and achieve customized service-level agreements (SLAs) which are fit for their similar purposes.[7]

A hybrid cloud allows organizations to determine which option to use, depending on the classification of information to be stored. Less sensitive information is usually sent to a public cloud, whereas more sensitive and confidential information is kept on a private or internal cloud. While this model offers cost savings, scalability, security and performance updates/improvements, it entails the same risks as a public cloud in terms of loss of control over data and unauthorized disclosure.

7 On cloud contracts negotiations, see Paolo Balboni, "Managing legal compliance risk in the cloud and negotiating personal data protection requirements with vendors", in *Cloud Computing Security: Foundations and Challenges*, CRC Press, Abingdon, UK, 2016, 267–276.

## 10.2 DATA CONTROLLER/DATA PROCESSOR RELATIONSHIP

As discussed in Section 4.5 – Data Controller/Data Processor relationship, the relationship between a Humanitarian Organization that puts Personal Data in the cloud and a cloud provider that it contracts with to do so is, generally speaking, that of a Data Controller and a Data Processor. However, in practice these roles may be more difficult to categorize than is at first apparent, as this will depend on how much discretion the cloud provider has, which should be defined in the agreement between the provider and the client. What is crucial is that these uncertainties should not affect the rights of Data Subjects, meaning that Humanitarian Organizations should be as transparent as possible about their use of Cloud Services and not allow cloud providers to disadvantage Data Subjects.

The use of Cloud Services by a Humanitarian Organization routinely involves the cloud provider hiring Sub-Processors. The contract with the provider should specify that Sub-Processors may only be used on the basis of an authorization given by the Data Controller (i.e. the Humanitarian Organization). The Data Processor (cloud provider) should have a clear duty to inform the Data Controller of any changes in this regard, with the Data Controller retaining the option of objecting to such changes or terminating the contract.

## 10.3 RESPONSIBILITY AND ACCOUNTABILITY IN THE CLOUD

The cloud client/provider relationship is a Data Controller/Data Processor relationship.[8] However, in exceptional cases the cloud provider may act as a Data Controller as well, in which case it has full (joint) responsibility for the data Processing and must comply with all relevant legal obligations for data protection. As the Data Controller, the cloud client (i.e. the Humanitarian Organization) is responsible for complying with legal obligations stemming from data protection law. Furthermore, the cloud client is responsible for selecting a cloud provider that complies with data protection legislation.

The notion of accountability expresses the direct compliance obligations that Data Controllers and Data Processors have under data protection law. This means that they must be able to ensure and demonstrate that their Processing activities comply with the relevant legal requirements, through the adoption and implementation of appropriate data protection policies and notices.

8 See Section 10.2 – Data Controller/Data Processor relationship.

**EXAMPLE:**
When a Humanitarian Organization contracts with a cloud provider to store Personal Data in the cloud, it will remain liable to the Data Subjects for any breaches of data protection that the provider commits. It is therefore essential for the Humanitarian Organization to take the following steps before Personal Data are stored in a cloud:

- undertake a DPIA on the proposed storage of Personal Data in the cloud, and be prepared to cancel the project if the results show that this would cause undue risk for individuals' data protection;
- perform due diligence on the Cloud Service provider to ensure that the provider will use due care and takes data protection/security seriously;
- discuss data protection openly with the provider and assess whether the provider seems ready and able to fulfil their data protection obligations;
- carefully review the contract with the provider before signature and ensure that it contains adequate data protection language; and
- for Humanitarian Organizations enjoying privileges and immunities, ensure that such privileges and immunities are properly built into the cloud solution design, and are respected.

## 10.4 APPLICATION OF BASIC DATA PROTECTION PRINCIPLES

All data protection principles apply to Cloud Services; special attention is paid here to a number of issues that are of particular relevance.

**The data protection discussion in this chapter builds on the principles set out in Part I, which examines them in greater detail.**

### 10.4.1 LEGAL BASES FOR PERSONAL DATA PROCESSING

Before engaging a cloud provider Humanitarian Organizations need to demonstrate that one of the following legal bases is present:[9]

- the vital interest of the Data Subject or of another person;
- the public interest, in particular based on an organization's mandate under national or international law;
- Consent;
- a legitimate interest of the organization;
- the performance of a contract;
- compliance with a legal obligation.

9 See Chapter 3: Legal bases for Personal Data Processing.

It is important in this regard to differentiate between the initial Processing of the Personal Data by the Humanitarian Organization and its Processing in the cloud. The Humanitarian Organization must have a legal basis for collecting and Processing the Personal Data in the first place, which can be any of the legal bases referred to in Chapter 3: Legal bases for Personal Data Processing. If the cloud provider acts as processor, the same legal basis will extend to the Processing in the cloud (which is to be regarded as a means of Processing). However, in the residual instance that the cloud provider acts as controller, a separate legal basis for the sharing of data with the cloud provider should be found. In any case, the Humanitarian Organization should perform a DPIA in order to identify the possible risks for individuals, including possible loss of exclusive "jurisdictional" control over the data by the Humanitarian Organization, and adequately mitigate them.

**EXAMPLE:**
A Humanitarian Organization collects Personal Data from vulnerable individuals on the basis that it is in their vital interest. In order to provide humanitarian services more efficiently, it then wants to store the data in a private cloud, and to this end engages a Cloud Service provider. The vital interest of the individuals is a sufficient legal basis for collecting the Personal Data and storing them in the cloud (with the provider acting as processor for the Humanitarian Organization), provided that the relevant DPIA has been carried out and the risks for the individuals have been adequately mitigated.

## 10.4.2 FAIR AND LAWFUL PROCESSING

Personal Data must be processed lawfully and fairly. The lawfulness of the Processing refers to the identification of an appropriate legal basis,[10] while the requirement for fairness is a broad principle that is generally connected to the provision of information as well as to the uses of the data. Humanitarian Organizations using Cloud Services should bear in mind that these Principles apply during all stages of Processing (i.e. collection, Processing and storage). Fundamental actions that Humanitarian Organizations should undertake in order to assure conformity with these fundamental data protection principles are: one, performing a DPIA before using Cloud Services, and two, monitoring ongoing compliance in the cloud environment during the service provisions by way of audits.

## 10.4.3 PURPOSE LIMITATION AND FURTHER PROCESSING

Humanitarian Organizations must determine and set out the specific purposes of Personal Data Processing. The purposes of the Processing need to be clarified and communicated to individuals at the time of collection.

**10** See Section 10.4.1 – Legal bases for Personal Data Processing.

Humanitarian purposes offer a wide basis upon which to justify Further Processing operations. Compatibility would, however, not be found if the risks for the individuals concerned outweigh the benefits of Further Processing. This depends on the particular case. For example, circumstances leading to a finding of incompatibility include risks that the Processing may run counter to the significant interests of the person to whom the information relates or of his/her family, in particular when there is a risk that the Processing may threaten their life, integrity, dignity, psychological or physical security, liberty or their reputation.

In cloud computing environments, the cloud client is responsible for determining the purpose(s) of the Processing prior to the collection of Personal Data from the Data Subject and must inform the Data Subject accordingly. Based on the prohibition that the cloud client must not process Personal Data for other purposes that are inconsistent with the original ones, a Cloud Service provider cannot unilaterally decide or arrange for Personal Data (and its Processing) to be transmitted automatically to unknown cloud data centres. Furthermore, the Cloud Service provider cannot use Personal Data for its own purposes (such as, for example, marketing, carrying out research for other purposes or profiling). It is worth pointing out that the same holds true for the Cloud Service provider subcontractors, as a typical cloud scenario may easily involve a larger number of them. In order to mitigate the risk of Further Processing, the contract between cloud provider and cloud client should include technical and organizational measures and provide assurances for the logging and auditing of relevant Processing operations on Personal Data that are performed by employees of the cloud provider or the subcontractors.

### 10.4.4 TRANSPARENCY

Transparency is an aspect of the fair and legitimate Processing of Personal Data and is also closely related to the provision of information to Data Subjects. The cloud client is obliged to provide Data Subjects, whose Personal Data or data related to them are collected, with detailed information; this includes the cloud client's identity, address and the purposes of the Processing; the recipients or categories of recipients of the data, including Data Processors, insofar as such further information is necessary to guarantee fair Processing; and information about their rights.

Transparency must also be guaranteed in the relationship(s) between cloud client, cloud provider and subcontractors (if any). The cloud client can assess the lawfulness of the Personal Data Processing in the cloud only if the provider informs the client about all relevant issues. A Data Controller contemplating the engagement of a cloud provider should carefully check the provider's terms and conditions of service and assess them from a data protection point of view.

Another aspect of transparency in cloud computing is the fact that the cloud client must be informed about all the subcontractors involved in the provision of the

respective Cloud Service, not merely those with which it is in a direct contractual relationship, and the locations of all data centres in which Personal Data are processed, as these elements may trigger International Data Sharing (see Section 10.7 – International Data Sharing).

### 10.4.5 DATA RETENTION

Humanitarian Organizations are advised to ensure that Personal Data are not held (whether by them or by Data Processors) for longer than is required to achieve the purposes for which they were collected, unless they have clear, justifiable and documented reasons for doing so; otherwise, data held by the organization and any relevant Third Parties should be destroyed. Deletion or destruction after completion of their Processing or a carefully structured data retention policy is recommended. When the purposes for which the Personal Data were collected have been achieved, then the Personal Data should be deleted both by the organization and any Third Parties that have had access to the data, unless they can rely on a relevant legal ground to hold that data. For example, data should only be retained in Cloud Services if they are related to a legitimate Processing purpose. Legitimate purposes in this regard might include possible future programmes, monitoring and evaluation, whereas for research purposes anonymized or aggregated data might be appropriate. Only the minimum amount of data necessary should be retained, in accordance with the data minimization principle.

The responsibility to ensure that Personal Data are erased as soon as they are no longer necessary lies with the cloud client. Erasure of data is a crucial issue not only throughout the duration of a cloud computing contract, but also upon its termination. It is also relevant if a subcontractor is replaced or withdraws. In such a case, the cloud client might either request a certificate of destruction by the Cloud Service provider or adequate evidence confirming that the data were transferred to a new Cloud Service provider.[11]

The principle of data erasure is applicable to Personal Data irrespective of whether they are stored on hard drives or other storage media (e.g. backup tapes). Since

11 Examples of measures for data deletion in the cloud include: the initial deletion from databases, storage and backup systems followed by data overwrite (e.g. using zeros and ones to overwrite data) or crypto-shredding (i.e. the practice of encryption of data and the destruction of the encryption keys), in order to ensure the complete deletion of the subject data. After the implementation of such a practice, evidence of deletion can be provided via extensive controls documentation of how the data are handled and deleted, and then the associated logs of the activities. As a caveat, it should be noted that providing 100 per cent assurance that data have been deleted is very difficult to achieve. For instance, to ensure this, a cloud customer would need to encrypt the data with a strong key before they store it in the cloud; never lose the key; and delete the key when they are done. This would bring the likelihood of full deletion close to 100 per cent (depending on the crypto-algorithm) since the CSP has never had access to both the key and the data at once.

Personal Data may be kept at the same time on different servers at different locations, it must be ensured that each instance is erased irretrievably (i.e. previous versions, temporary files and even file fragments should also be deleted).

Secure erasure of Personal Data requires that either the storage media are destroyed or demagnetized, or that the stored Personal Data are deleted effectively. Special software tools that overwrite Personal Data multiple times, in accordance with a recognized specification, should be used. The cloud client should make sure that the cloud provider ensures secure erasure in the above-mentioned sense and that the contract between the provider and the client contains clear provision for Personal Data erasure. The same holds true for contracts between cloud providers and subcontractors.

## 10.5 DATA SECURITY

Data security measures can be legal, technical and organizational. Legal measures may include not only contractual arrangements, but also Data Protection Impact Assessments (DPIAs). A holistic perspective must be adopted, which takes the following phases of contracting for Cloud Services into account:

- assessing the decision to use cloud computing (via DPIAs and a "go/no go" decision by management);
- the Cloud Service procurement process, including due diligence on prospective Cloud Service providers that takes both legal and technical perspectives into account;
- contracting (i.e. getting the right terms and conditions);
- operating, maintaining and decommissioning the service.[12]

A comprehensive data protection strategy is recommended, and attention should be paid to data protection issues in all phases before, during and after contractual arrangements. This should include an overall assessment of the contractual framework, including service-level agreements (SLAs), general (non-data protection) clauses (e.g. applicable law, variations to the contract, jurisdiction, liability, indemnification, etc.) and the general principle of "parallelism in/outside the cloud" (e.g. having the same data retention period for cloud or non-cloud Processing).

When a Humanitarian Organization decides to contract for cloud computing services, it should choose a cloud provider that can give sufficient guarantees for technical security and organizational measures governing the envisaged Processing, and

12 On procuring Cloud Services see, for example, Paolo Balboni et al., *Procure Secure: A Guide to Monitoring of Security Service Levels in Cloud Contracts*, European Union Agency for Cybersecurity, Attiki, Greece, 2012: www.enisa.europa.eu/publications/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts.

ensure compliance with those measures. Furthermore, a written contract with the Cloud Service provider must be signed, as there must be a binding legal act to govern the relationship between the Data Controller and the Data Processor. The contract must at a minimum establish that the Data Processor is to follow the instructions of the Data Controller and that the Data Processor must implement technical and organizational measures to adequately protect Personal Data, in accordance with the applicable data protection law.

In order to ensure legal certainty, the contract between the Humanitarian Organization and the Data Processor should also contain the following core data protection clauses:

- Provision of information on the location of the data centres, the identity and location of subcontractors and on any subsequent changes to the nature of the Processing. This should include the subject and time frame of the Cloud Service to be provided by the cloud provider; the extent, manner and purpose of the Processing of Personal Data by the cloud provider; and the types of Personal Data processed.
- Details about the cloud client's instructions to be given to the provider, with particular regard to the applicable SLAs and the relevant penalties (financial or otherwise including the ability to sue the provider in case of non-compliance).
- Clarification of the responsibilities of the cloud provider to notify the cloud client in the event of any Data Breach which affects the cloud client's data. Note that a security incident does not necessarily constitute a Data Breach.
- Recognition of the obligation to process Personal Data only for the explicitly mentioned and specified purposes, and to delete data at the end of the contract. There must be specification of the conditions for returning the data or destroying them once the service is concluded. Furthermore, it must be ensured that Personal Data are erased securely at the request of the cloud client.
- Confirmation, in case of a private cloud located outside the cloud client premises, that the data of the Humanitarian Organization are kept in separate servers.
- Specification of security measures that the cloud provider must comply with, depending on the risks represented by the Processing and the nature of the data to be protected.
- A confidentiality clause, binding both upon the cloud provider and any of its employees who may be able to access the data. Only authorized persons can have access to the data.
- An obligation on the provider's part to support the client in facilitating the exercise of Data Subjects' rights, e.g. to access, correct, delete their data, etc.
- An obligation on the provider's part to respect the cloud client's privileges and immunities, if applicable.
- A clause to the effect that Sub-Processors may only be commissioned on the basis of an authorization that can be generally given by the Data Controller (cloud client), in line with a clear duty for the Data Processor to inform the Data

Controller of any intended changes in this regard, with the Data Controller retaining at all times the possibility of objecting to such changes or terminating the contract. There should be a clear obligation for the cloud provider to name all the subcontractors commissioned. It must be established that contracts between the cloud provider and subcontractors reflect the stipulations of the contract between cloud client and cloud provider (i.e. that Sub-Processors are subject to the same contractual duties as the cloud provider). In particular, it must be guaranteed that both the cloud provider and all subcontractors act only on instructions from the cloud client. The chain of liability should be clearly set out in the contract.

- Arrangements for audits to be conducted during and at the end of the contract by the cloud client. The contract should provide for logging and auditing of relevant Processing operations on Personal Data that are performed by the cloud provider or the subcontractors.
- A general obligation on the provider's part to give assurance that its internal organization and data Processing arrangements (and those of its Sub-Processors, if any) are compliant with the applicable national and international legal requirements and standards.

With regard to the technical aspects of data security, the following are some important considerations for Humanitarian Organizations to bear in mind:[13]

- **Availability**: Providing availability means ensuring timely and reliable access to Personal Data. Availability in the cloud can be threatened by accidental loss of network connectivity between the client and the provider or of server performance caused by malicious actions such as (Distributed) Denial of Service (DoS) attacks. Other availability risks include accidental hardware failures both on the network and in the cloud Processing and data storage systems, power failures or other infrastructure problems. Data Controllers should therefore check that the cloud provider has adopted reasonable measures to cope with the risk of interferences such as backup Internet network links, redundant storage and effective data backup mechanisms.
- **Integrity**: Integrity relates to the maintenance of data quality which should not be maliciously or accidentally altered during Processing, storage or transmission. For IT systems, integrity requires that Personal Data undergoing Processing on these systems remain unmodified. Personal Data modifications can be detected by cryptographic authentication mechanisms such as message authentication codes, signatures or cryptographic hash functions. Interference with the integrity of IT systems in the cloud can be prevented or detected by means of Intrusion

13 Adapted from Article 29 Data Protection Working Party, "Opinion 05/2012 on Cloud Computing (WP196)", 1 July 2012, 14–17: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

Detection and Prevention Systems (IDS/IPS). These security tools are particularly important for the open network environments in which clouds usually operate.

- **Confidentiality**: In a cloud environment, encryption can significantly contribute to the confidentiality of Personal Data if applied correctly, although it does not render Personal Data irreversibly anonymous. It is simply a tool for the cloud client to ensure that the Personal Data they are responsible for can only be accessed by authorized persons who have the correct key. Personal Data encryption should be used for all data "in transit" and, when available, to data "at rest". This applies particularly for Data Controllers who plan to transfer Sensitive Data. Communications between cloud provider and client, as well as between data centres, should also be encrypted. When encryption is chosen as a technical measure to secure data, it is also important to guarantee the security of the key. Further technical measures aiming at ensuring confidentiality include authorization mechanisms and strong authentication (e.g. two-factor authentication). Contractual clauses should also impose confidentiality obligations on employees of cloud clients, cloud providers and subcontractors.
- **Isolation (purpose limitation)**: Isolation is an expression of the purpose limitation principle. In cloud infrastructures, resources such as storage, memory and networks are shared among many users. This creates new risks for data disclosure and illegitimate Further Processing. Isolation is meant to address this issue and ensure that data are not used beyond their initial original purpose and to maintain confidentiality and integrity. Isolation is achieved by adequate governance of the rights and roles for accessing Personal Data, and should be reviewed on a regular basis. The implementation of roles with excessive privileges should be avoided (e.g. no user or administrator should be authorized to access the entire cloud). More generally, administrators and users must only be able to access the information that is necessary for legitimate purposes (least privilege principle).
- **Intervenability**: Data Subjects have the rights of access, rectification, erasure, blocking and objection, as discussed below.[14]
- **Portability**: The use of standard data formats and service interfaces by the cloud providers is very important, as it facilitates interoperability and portability between different cloud providers. Therefore, if a cloud client decides to move to another cloud provider, any lack of interoperability may make it difficult or impossible to transfer the client's (Personal) Data to the new cloud provider, which is known as "vendor lock-in". The cloud client should check whether and how the provider guarantees the portability of data and services prior to ordering a Cloud Service. Data portability also refers to the ability of a Data Subject to obtain from the Data Controller a copy of data undergoing Processing in a commonly-used, structured, electronic format. In order to implement this right,

14 See Section 10.6 – Rights of Data Subjects.

it is important that, once the data have been transferred, no trace is left in the original system. In technical terms, it should become possible to verify the secure erasure of data.

The following are further IT security principles for Humanitarian Organizations to consider when moving to the cloud.

## 10.5.1 DATA IN TRANSIT PROTECTION

Data transmissions must be properly secured against eavesdropping and tampering. This is relevant not only for connections between the premises of the organization and the cloud application, but also for data paths inside the service and for connections between the application and other services (API).[15] A common solution is the encryption of network traffic, using network level traffic encryption (VPN),[16] transport layer security (TLS) or application level encryption. Due care must be taken to choose the correct protocols and implementation of encryption, as well as in the management of secret keys for the encryption itself. Dedicated fibre-optic connections can also be used, where they are convenient and the situation allows it.

## 10.5.2 ASSET PROTECTION

Protecting assets in cloud situations is different from protecting them in on-site arrangements. Consequently, several specific points need to be considered when evaluating a cloud solution.

### 10.5.2.1 PHYSICAL LOCATION

It is important to know the physical location(s) of data storage in order to understand which legislation applies, but also the likelihood of specific threats, such as power and network outages, actions by hostile groups and organizations and other country-specific threats. It is therefore important to obtain a detailed statement regarding the physical location of data centres and be aware that data exchanges between data centres in different locations can happen without the organization's knowledge.

For Humanitarian Organizations with privileges and immunities, it is also essential that the country in which data centres are stored has a legal obligation to respect privileges and immunities, and is known to respect them in practice.

15 API – an application programming interface is a set of subroutine definitions, protocols and tools for building application software: "API", in *Wikipedia*, accessed 13 January 2022: https://en.wikipedia.org/wiki/API.

16 VPN – A virtual private network extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network: "Virtual Private Network", in *Wikipedia*, accessed 16 January 2022, https://en.wikipedia.org/w/index.php?title=Virtual_private_network&oldid=1065922505.

#### 10.5.2.2 DATA CENTRE SECURITY

In Cloud Service arrangements, the physical security of data centres is fully controlled by the service provider; it is therefore important to have a clear idea of the security at the premises in which the data and applications are stored. This can be achieved by verifying the certifications (if any) obtained by the data centre and/or the contractual obligations underlying the relationship between the Cloud Service provider and the organization. The level of security guaranteed should match the level of security required by the application to be hosted in the cloud. Physical inspection could give useful information, but is unlikely to be possible in most cloud environments.

#### 10.5.2.3 DATA AT REST SECURITY

The level of security for data at rest depends on the type of service required and other arrangements with the service provider. However, it is reasonable to assume that data will be stored in shared storage media, so a clear statement of the service provider about the protection level and how it is achieved is required, along with any related Third Party certification. However, it is recommended not to rely only on cloud provider security for data at rest, at least for most Sensitive Data, but to add additional layers of protection, such as encryption.

#### 10.5.2.4 DATA SANITIZATION

Cloud environments are characterized by a high frequency of provisioning, deletion and migration of resources; in other words, data and applications can easily be moved around different parts of the shared infrastructure. If not correctly managed, this could lead to data disclosure, as other customers' applications will likely be run on the same hardware previously used by Humanitarian Organizations. Moreover, data could remain indefinitely in the cloud infrastructure. Measures should be taken to control this threat: using dedicated resources and/or verifying with the provider which measures are in place to erase or otherwise sanitize the data. The use of encryption, independently from the service provider, could offer an additional layer of protection.

#### 10.5.2.5 EQUIPMENT DISPOSAL

Equipment disposal is closely related to the previous point and a fair level of confidence should be achieved that no data or information could remain stored or possibly be disclosed when hardware is decommissioned or disposed of. The cloud provider should give some guarantee that this requirement can be met or other measures must be adopted (i.e. encryption).

#### 10.5.2.6 AVAILABILITY

Cloud Services must offer the required level of availability; service-level agreements (SLAs) are of paramount importance in this respect. The agreement should also be examined in terms of liabilities and responsibility. Verification of any publicly

available information, which could help in ascertaining the actual reliability of the service offered, is recommended.

### 10.5.3 SEPARATION BETWEEN USERS

In a cloud environment, the service provider is responsible for guaranteeing user separation. However, it is important when evaluating a cloud provider, and even more so when the provider and the related technology are not widely known, to assess the technology used and gather any information that can help in understanding how the separation is ensured. The separation is affected by several factors, such as the service model, the deployment model (public versus private cloud) and other factors. To assess the effectiveness of separation measures, a penetration test can be useful, but only to a limited extent: it is valid only for the specific time when the test is carried out and it only gives an indication about known issues. A background check of previous incidents and their management by the provider can also be extremely useful.

### 10.5.4 GOVERNANCE

The service provider should have a proper security governance framework, as this is the basis to control and coordinate all security efforts, and to manage changes in threat and developments in technology. The provider should then demonstrate that it possesses the required elements that are typically associated with a C* level manager (e.g. CSO, CISO, CTO) in charge of cloud security; that it has a properly implemented framework for security governance; that security and security risks are included in general risk and financial management; and that it complies with regulations and legal requirements. Conformance with recognized standards should be assessed.

### 10.5.5 OPERATIONAL SECURITY

The cloud provision service must be operated in accordance with strict security requirements and security must be embedded in standard operating procedures. The main elements are:

- Configuration and change management, to control what is in the production environment and related changes, to perform the required tests and receive proper authorization before making changes.
- Vulnerability management, to assess, identify and correct security issues that can arise in services and infrastructure.
- Monitoring, to detect anomalies, attacks and unauthorized actions that can undermine the security of the services.
- Incident management: when an incident occurs, the service provider must be able to address it by taking adequate measures in order to mitigate, contain and properly correct the issue. This includes communications and reports to the customers and law enforcement authorities.

### 10.5.6 PERSONNEL

The Cloud Service provider must have in place measures to assess the trustworthiness of the personnel involved in the service management. Proper background checks and screening should be implemented for any privileged or sensitive role. Operators should be trained and must understand and acknowledge their responsibilities.

### 10.5.7 DEVELOPMENT

Service providers usually develop large parts of their infrastructure. They should employ best practices and industry standards to ensure that threats are evaluated during development. Guidelines for secure design, coding, testing and deployment should be in place.

### 10.5.8 SUPPLY CHAIN

Cloud providers often use Third Party products and services to integrate or manage the services they offer. Any weakness along the supply chain can compromise the security of the entire Cloud Service and applications. The provider should describe how the Third Party suppliers are screened; the acceptance process for services and products; how security risks are managed; how the security posture of the service providers is verified; and how spare parts, updates and other changes are verified. This process is made even more important by the fact that Cloud Services can be layered, relying on other service providers lower down the chain. If possible, verification of the suppliers should be performed or agreements should be in place to prevent the cloud provider from using Third Party suppliers not acceptable to the organization.

Additional supply chain concerns relate to how the choice of technology that shares the same supply chain as organizations of a non-humanitarian nature may have a detrimental impact on the capacity of the Humanitarian Organization to rely on its neutral, impartial and independent exclusively humanitarian approach to security.[17]

### 10.5.9 USER MANAGEMENT

Depending on the service offered, the authorization process may, in part, be managed by the cloud provider. This process should be assessed to verify its compliance with best practices, regulations and the organization's needs, in order to ensure secure access to management interfaces. These interfaces allow the performance of actions that can be considered equivalent, to a certain extent, to physical actions performed inside a traditional data centre. Consequently, such actions need to be

17 Massimo Marelli, "The SolarWinds hack: Lessons for international humanitarian organizations", *International Review of the Red Cross*, Vol. 104, No. 919, 28 March 2022, pp. 1267–1284: https://doi.org/10.1017/S1816383122000194.

carefully guarded. Privileges should be fine-grained, so as to ensure the correct management of roles and privileges.

### 10.5.10 IDENTITY AND AUTHENTICATION

As with user management, access to any service interface should be strictly guarded. Implementation of identification and authorization processes should be assessed to conform to the security needs of the organization. Examples of different approaches are: two-factor authentication, use of TLS client certificates, single sign-on systems, etc. The methods adopted must be kept up to date with developments in security and the growing sophistication of the threats.

### 10.5.11 EXTERNAL INTERFACES

When management interfaces are exposed, this increases the attack surface available to hostile entities. The security of those interfaces should therefore be assessed against this threat; the availability of solutions such as private networks or equivalent measures to access private interfaces should be assessed.

### 10.5.12 SERVICE ADMINISTRATION

The architecture and management of administration systems should be carefully designed and implemented, as these systems are highly valuable for attackers. Thus, a description of administration systems management and procedures can be useful to assess the security posture of the service provider.

### 10.5.13 AUDITS

The service provider should make available the results of independent audits or allow the cloud customer either to directly perform an audit or to ask a trusted Third Party to carry out such an assessment. Audit data regarding the services (performance, downtime, security incidents and so on) should also be available for scrutiny. These audits should be regularly carried out, with a frequency which is adequate to the nature and purpose of the cloud service. The best practice in this regard, which is also the generally recognized rule for certification and attestation audits, is to set at least an annual frequency for these audits, and to carry out additional ad hoc audits in the event of a substantial or relevant change to the target of the audit.

### 10.5.14 SERVICE USAGE

The organization must have a clear understanding of the interactions with the Cloud Service: interfaces, data exchanges, authorization process for users, administration, workloads and any other aspect that can influence the service considered as the sum of cloud and organization activities. A detailed assessment of data flow, processes and architectures must be conducted prior to implementing a cloud solution. Proper procedures must be designed and implemented, personnel must be trained, and operators should be provided with the requisite knowledge about the cloud solution,

the usage, the relationship with the organization and other information related to correct use and management of the cloud solution.

## 10.6 RIGHTS OF DATA SUBJECTS

Data Subjects' rights (e.g. access, rectification, erasure, objection, etc. ) naturally extend to Processing in the cloud.[18] The Humanitarian Organization must verify that the cloud provider does not impose technical and organizational obstacles to these requirements, even in cases when data are further processed by subcontractors. The contract between the client and the provider should require that the cloud provider facilitates the exercise of the Data Subjects' rights, includes specific stipulations on how this collaboration will be provided and ensures that the same exercise of these rights is safeguarded in its relationship with any subcontractor.

## 10.7 INTERNATIONAL DATA SHARING

By their very nature Cloud Services may involve International Data Sharing of Personal Data with various parties located in different countries. Data protection laws restrict International Data Sharing; Humanitarian Organizations should therefore ensure that the use of Cloud Services is in compliance with any laws to which they are subject, if any, and with their own internal policies. This means, for example, that any contract with a cloud provider should indicate how the provider complies with legal requirements concerning International Data Sharing (e.g. through the use of contractual clauses with its entities and with subcontractors). Performing a DPIA[19] with specific attention to the impact of the International Data Sharing (such as a Data Transfer Impact Assessment) on the right and freedoms of the concerned Data Subjects contributes to further strengthen the lawfulness of such Processing from a data protection perspective and, where relevant, to preserve privileges and immunities for the Humanitarian Organizations which benefit from them.

## 10.8 DATA PROTECTION IMPACT ASSESSMENTS

Data Protection Impact Assessments (DPIAs) are important tools during project design to ensure that all aspects of data protection regulations and applicable risks are addressed. It is essential to carry out specific DPIAs tailored to cloud computing whenever there is interest in using Cloud Services.[20] DPIAs should clarify the Processing details and specifications, and also focus on the risks posed by them as

18 See Section 2.11 – Rights of Data Subjects.

19 See Section 10.8 – Data Protection Impact Assessments.

20 See Chapter 5: Data Protection Impact Assessments (DPIAs).

well as on mitigating measures. In this respect, it is important to note that DPIAs should be undertaken prior to the use of Cloud Services.

## 10.9 PRIVILEGES AND IMMUNITIES AND THE CLOUD

Beyond the considerations above, Humanitarian Organizations benefiting from privileges and immunities should also consider that data placed in the cloud may jeopardize the protection of such privileges and immunities, unless specific legal, technical and organizational measures are put in place. This consideration is key, particularly given that in Humanitarian Emergencies, the privileges and immunities of a Humanitarian Organization may be the first line of protection for the Personal Data of vulnerable individuals, particularly in conflicts and other situations of violence. This matter is closely connected to the one of "data sovereignty" in the cloud, i.e. the jurisdictional control or legal authority that apply to data being subjected to the country's laws because the cloud and/or the cloud provider are located within the country.[21]

Humanitarian Organizations should consider implementing the legal, organizational and technical measures suggested below, to ensure that their privileges and immunities are adequately protected in a cloud environment and to keep "sovereignty" over their data.[22]

### 10.9.1 LEGAL MEASURES

- Data should be hosted and processed by external Data Processors exclusively in jurisdictions where the privileges and immunities of the organization are formally recognized by status agreements recognizing the inviolability of files, archives, correspondence and communication wherever and by whomever the organizations' data are held, as well as immunity from every form of legal process. This legal protection should ideally be backed by a track record of such privileges and immunities being consistently respected.
- Data Processors and Sub-Processors should be bound by contractual obligation to notify any requesting authorities who seek to access data, that the data in question are covered by a Humanitarian Organization's privileges and immunities; to decline any requests for access by authorities, whether informal, administrative or through judicial process, and to redirect the authorities' request to the

21 See Marelli, "The SolarWinds hack", and particularly the section "'Data sovereignty' and 'digital sovereignty': Tools for protecting humanitarian principles in cyberspace".

22 Massimo Marelli, "Hacking humanitarians: Defining the cyber perimeter and developing a cyber security strategy for international humanitarian organizations in digital transformation", *International Review of the Red Cross*, Vol. 102, No. 913, April 2020, pp. 367–387: https://doi.org/10.1017/S1816383121000151.

Humanitarian Organization; to immediately notify the Humanitarian Organization of any request for access to its data, whether informal, administrative or through judicial process, the identity of the requesting authority and status of the request; and to assist the Humanitarian Organization with the provision of any information and documentation that may be necessary as part of any proceedings, whether informal, administrative or through judicial process, that may be required by the Humanitarian Organization in order to assert its privileges and immunities over the relevant data.

### 10.9.2 ORGANIZATIONAL MEASURES

- The data of the Humanitarian Organization should be held in segregated servers, and the data should be segregated from the data of other clients of the Data Processors and Sub-Processors.
- The servers hosting the data of the Humanitarian Organizations should be clearly marked with the emblem of the organization, and the indication "Legally Privileged Information" should be marked on the servers.
- Where possible, the servers hosting the data of Humanitarian Organizations should only be accessed with the authorization of both the Data Processors and of the Humanitarian Organization.
- Staff of the Data Processor and Sub-Processors should be properly informed of the privileged status of the data, and trained on the procedure to follow in case of requests for access by Third Parties.

### 10.9.3 TECHNICAL MEASURES

- Data hosted in a cloud environment should be encrypted and encryption keys held only by the Humanitarian Organization.
- If the cloud solution envisaged is a SaaS, and the Data Processors and Sub-Processors need to manage the service offered, arrangements should be made to ensure that such Data Processors and Sub-Processors may access the system to manage it, run updates, fix bugs and support users, without ever having access to clear (unencrypted) data.

## 10.10 CODES OF CONDUCT

Finally, it is worth mentioning that in 2021 the European Data Protection Board (EDPB) approved two codes of conduct[23] for the application of the GDPR to Cloud

23 See: Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe (https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202116_eucloudcode_en.pdf) and Opinion 17/2021 on the draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE) (https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202117_cispecode_en_0.pdf).

Services pursuant to Article 40, and a third one is currently being evaluated by the European Supervisory Authorities.[24] For Humanitarian Organizations which are subject to the GDPR, it will be recommendable to check whether a specific service is approved under one of the applicable codes of conduct. The adherence to a code of conduct must be seen just as a good starting point. In fact, given their specific issues and requirements, Humanitarian Organizations will still need to specifically and carefully consider all the matters indicated in this chapter.

**24** Cloud Security Alliance (CSA), "CSA Code of Conduct for GDPR Compliance", CSA, accessed 9 May 2022: https://cloudsecurityalliance.org/privacy/gdpr/code-of-conduct.