SafeCloud

Legal Recommendations

D2.3

Project reference no. 653884

January 2017

European Commission

Horizon 2020
European Union funding
for Research & Innovation

Document information

Scheduled delivery	16.01.2017
Actual delivery	16.01.2017
Version	2.0
Responsible Partner	UniNE

Dissemination level

Public

Revision history

Date	Editor	Status	Version	Changes
06.12.2016	Y. Bauer	Draft	1.1	Initial draft after Y1 Review meeting
07.12.2016	N. Tissot	Draft	1.2	Initial comments
08.12.2016	H.Mercier	Draft	1.2	Initial comments
22.12.2016	Y. Bauer	Draft	1.3	Extended draft
23.12.2016	N. Tissot	Draft	1.4	Comments
23.12.2016	H.Mercier	Draft	1.4	Comments and overall document structure
27.12.2016	Y. Bauer	Draft	1.5	Final structure and extended content
03.01.2017	N. Tissot	Draft	1.5	Comments
06.01.2017	H. Mercier	Draft	1.6	Review of current version
09.01.2017	N. Tissot	Draft	1.6	Comments
10.01.2017	H. Mercier	Draft	1.7	Extended review of current version
10.01.2017	N. Tissot	Draft	1.7	Comments
11.01.2017	Y. Bauer	Draft	1.7-2	Enhanced draft after review
11.01.2017	N. Tissot	Draft	1.7-2	Comments
11.01.2017	H. Mercier	Draft	1.8	Version ready for internal review
12.01.2017	D. Bogdanov	Draft	1.8	Cybernetica review
12.01.2017	L. Yazdanov	Draft	1.8	Cloud&Heat review
13.01.2017	B. Ferreira / P. Sousa	Draft	1.9	Maxdata review
13.01.2017	Y. Bauer	Draft	1.9	Final complete review
13.01.2017	H. Mercier	Final	2.0	Final version for resubmission

Contributors

Y. Bauer (UniNE)
H. Mercier (UniNE)
N. Tissot (UniNE)

Internal reviewers

D. Bogdanov (Cybernetica)
L. Yazdanov (Cloud&Heat)
Bruno Ferreira (Maxdata)
Paulo Sousa (Maxdata)

Acknowledgements

This project is partially funded by the European Commission Horizon 2020 work programme under grant agreement no. 653884.

More information

Additional information and public deliverables of SafeCloud can be found at http://www.safecloud-project.eu

Glossary of acronyms

Acronym	Definition
API	Application programming Interface
CEDIDAC	Center of Business Law (Centre du droit de l'entreprise)
DETEC	Department of the Environment, Transport, Energy and Communication
DPA	United Kingdom Data Protection act 1998
DPD	Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data
EC	European Community
ECJ	European Court of Justice
GDPR	Regulation 2016/679 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation)
IaaS	Infrastructure as a Service
ICO	Information Commissioner's Office
ICT	Information and Communication technologies
JIPITEC	Journal of Intellectual property, Information Technology and E-commerce Law
LIS	Laboratory Information System
MIM	Man in the middle
REST	Representational state transfer
SaaS	Software-as-a-Service
SS	Secure Storage
SQ	Secure Queries
SSH	Secure Shell
VM	Virtual Machine
WAN	Wide Area Network

Table of contents

Executive summary

This deliverable addresses the data protection problematics issues that are of importance for the compliance of the SafeCloud platform with the General Data Protection Regulation (GDPR).

In the first part of the document, we summarize the GDPR, the SafeCloud use cases, and the impact of the GDPR on these use cases.

In the second part of the document, we extend the analysis of the four GDPR issues relevant to SafeCloud. First, we examine the mere notion of data, with the aim to define what is the view of the legislator in relation to encrypted personal data. Second, we address the concept of controller in a cloud computing environment and study the legal duties and obligations of compliance that stem from this concept. Third, we assess the legal duties of the controller towards the data subject, with an emphasis on the new right to erasure or right to be forgotten. Fourth, we examine data security in relation to medical data, which is paramount to the Maxdata use cases.

Finally, in the third part of the document, we discuss our ongoing work and the outlook for the second half of the project.

1 Introduction

The SafeCloud project is far reaching and is going to set a new state of the art for information and communication technologies, in particular in the domain of cloud computing security. Besides the technology, the SafeCloud innovations will also challenge the legal framework surrounding its implementation on business applications.

This document focuses on data protection and, more specifically, on the issues raised by the General Data Protection Regulation (GDPR), which will become applicable in Spring 2018. Indeed, and according to Recital 4 of this regulation, the processing of personal data should be designed to serve mankind. The European legislator, on this basis, decided to harmonize data protection law at the European level, with both the purpose to offer a coherent framework for the right to data protection, and to encourage the development of the digital single market. As a result, compliance with the GDPR is necessary for companies who plan to process personal data in Europe. Even if SafeCloud puts privacy by design at the center of the consortium's goals, the legal question in relation to compliance might arise.

After a presentation of the five use cases in which parts of the SafeCloud platform will be commercially implemented, we survey four issues, and for each of them we make recommendations to mitigate the legal risks and ensure compliance. These issues provide an overview of the data protection questions surrounding the SafeCloud project.

First, what is considered personal data? As the regulation only applies to processing of personal data, other types of data fall out of the scope of the regulation. The case of anonymised or encrypted data is of particular importance in the SafeCloud environment in order to reduce the risks caused by the duties of the controller who processes personal data.

The second issue is liability. Who is liable? The concept of controller is crucial in the GPDR, as it allocates duties to the entity who is liable to guarantee the legality of the processing.

Third, what are the duties of the controller? A controller is liable for the lawfulness of the processing. Especially, he must ensure that the data subject's rights are respected. Such rights go from the access to the rectification or the erasure of the data in certain situations. Beside these obligations, the controller is also liable for the security of the data processed. These obligations for the controller are especially important in relation to particular types of data such as medical data, which is our fourth issue.

We mention that the focus of this document is an introduction to the precise legal issues related to the GDPR that could arise due to the specificities of the SafeCloud project. Their extended treatment and other questions such as the legal aspects related to the location of the data processed, data in transit, and the standards and codes of conduct adopted by the industry, will be addressed in deliverable D2.6.

The rest of this deliverable is organized as follows. In Section 2, we summarize the SafeCloud architecture and use cases. We describe the impact of the GDPR on SafeCloud in Section 3. In Sections 4 to 7, we present our four issues. Finally, Section 8 summarizes our ongoing work and the road ahead.

2 SafeCloud architecture and use cases

In this section, we revisit the SafeCloud architecture and use cases. Most of the content is taken from the deliverables D1.1, D2.1, D3.1, D4.1, D5.1, D5.2 and D7.9, which should be consulted for more details.

2.1 General SafeCloud architecture

The components of the general SafeCloud framework are shown in Figure 1. The framework consists of three separate layers, each providing solutions in their own domain. The technological solutions provide different security guarantees at different costs. Generally, stricter security guarantees impose greater limitations or performance costs on the applications using the solution. The three layers of the SafeCloud framework are secure communications, secure storage and secure query processing.

The secure communications layer provides solutions that improve the security aspects of communication channels over some untrusted environment. We provide three solutions for this layer. First, the vulnerability-tolerant channels solution (SC1) gives communication channels that are built on multiple redundant security mechanisms to ensure that failure of any of the mechanisms does not cause a security failure in the channel. Second, the protected channels solution (SC2) introduces multiple methods to reduce the risk of fake certificates used by the parties. We also make it more difficult to run port scans and do enumeration of the network infrastructure. Third, the route-aware channels solution (SC3) deploys methods to improve confidentiality and detect route hijacking. All the solutions are built on top of the Java secure socket API.

The secure storage layer consists of three solutions that provide confidentiality and integrity guarantees for data stored in an untrusted environment. The secure block storage (SS1) and the secure file system (SS3) give similar secure storage benefits but with different level APIs. The secure data archive (SS2) provides an entangled immutable data store for protection against tampering and censorship. It is exposed to applications as a REST API.

The solutions in the secure queries layer make it possible to store data in untrusted environments while still being able to process the data in some useful way. All the solutions in this layer provide SQL query processing in an untrusted environment but differ in degrees of which data is kept private from the different parties and what queries can be performed. The deployment model is also different. The privacy only refers to the keys or indexes needed for the queries. Any data that is not directly required in the query processing is kept private anyways. The secure database server (SQ1) and the secure multi-cloud database server (SQ2) do not reveal the keys to the untrusted domain. In the secure multi-cloud application server (SQ3) there are multiple different data owners that each act as a different trusted domain. The data of one trusted domain should remain private from other trusted domains. For this reason, we must keep some additional data private from the trusted domain, which is not necessary in the first two use cases.

Secure communication	State of the art: TLS secure channels	**Solution:**	**SC1 - Vulnerability-tolerant channels**	**SC2 - Protected channels**	**SC3 - Route-aware channels**
		Gives:	Tolerance to vulnerabilities in components	Decreased risk of fake certificates; resistance to port scans and enumeration of network infrastructure	Improved confidentiality with warnings about route hijacking and making harder access to communication
		API:	Extended secure socket API	Extended secure socket API	Extended secure socket API
		Provided by:	INESC-ID, TUM	INESC-ID, TUM	INESC-ID, TUM
Secure storage	State of the art: Encrypted storage	**Solution:**	**SS1 - Secure block storage**	**SS2 - Secure data archive**	**SS3 - Secure file system**
		Gives:	Block storage on individual data centers with fine control over data placement	Entangled immutable data storage for protection against tampering and censorship	Distributed secure file storage leveraging the secure block storage
		API:	Key/value	REST (S3 or similar)	POSIX-like
		Provided by:	UniNE, INESC TEC	UniNE, INESC TEC	UniNE, INESC-ID
Secure queries	State of the art: CryptDB	**Solution:**	**SQ1 - Secure database server**	**SQ2 - Secure multi-cloud database server**	**SQ3 - Secure multi-cloud application server**
		Gives:	Privacy of data against the server	Privacy of data against non-colluding servers	Privacy of data against non-colluding servers and clients
		API:	SQL	SQL	SQL
		Provided by:	INESC TEC	INESC TEC, Cyber	Cyber

Figure 1: SafeCloud architecture components.

2.2 Cloud&Heat use cases

Cloud&Heat operates a very large number of small datacenters, most of them located in individual homes and small office buildings that cannot be physically protected like modern massive data enters. For this reason, Cloud&Heat customers are sometimes reluctant to use its services to store sensitive data. The strong data integrity, privacy and anti-tampering provided by SafeCloud are thus perfectly suited for the C&H architecture.

In the context of the SafeCloud project Cloud&Heat wants to distribute data across several datacenters to increase integrity. However, cross-datacenter deployment involves data moving over WAN, thus it is important to provide secure communication between the datacenters. Moreover, one needs to assess and address the possible performance degradation due to inter-datacenter communication.

2.2.1 Cloud Block Storage

Cloud Block Storage is a block level storage that provides persistent storage for Virtual Machines (VMs) on the cloud. Cloud&Heat performs triple replication of a VM persistent storage within a datacenter to provide access to the data in case of hardware components failure. The company plans to implement cross-datacenter replication to ensure customer data availability even if one of the datacenters goes offline.

For small companies such as Cloud&Heat that have highly distributed datacenters, building a private communication network would require large upfront investments. The only option is to use available Wide Area Network (WAN). However, it requires ensuring that when under attack one cannot derive the service endpoint and access the data in transit.

Cloud Block Storage will use available WANs while taking advantage of the private communication middleware (SC1, SC2, SC3) and secure block storage (SS1) developed in the context of the SafeCloud project.

Available open source products use SSH to perform secure data transfer. In addition to SSH, Cloud&Heat will use private communication middleware with extended port-knocking technique to defend against MiM attacks.

2.2.2 SafeCloudBox

SafeCloudBox is a Software-as-a-Service (SaaS) application that delivers cloud storage for end-users. The application consists of two parts: end-user storage box (it could be a private computer infrastructure or virtual resources on a trusted cloud) and public cloud storage.

Today, many cloud based storage solutions are offered by popular cloud providers or companies that use Infrastructure-as-a-Service (IaaS) from the providers to build storage services. The examples include Google Drive, Microsoft OneDrive, Amazon Cloud Drive and Dropbox. It is common that private data is stored on the cloud without cryptographic data protection mechanisms. As a result, a potential attacker can access the data to tamper with it or read it. Moreover, mobile devices rarely have the capacity to store all the data. Therefore, in order to access the data a customer always needs to connect to the cloud. It brings the following problems. First, access to the cloud usually requires WAN communication, which leads to a high latency and a low throughput. So it is preferable to keep one copy of all the data (or at least the most important data) locally to eliminate the performance slowdown. Second, vendor lock-in. A customer cannot easily move data from one storage provider to another if one of them goes bankrupt or the other one offers storage at a lower price. In order to move the data, the customer needs to download it, which can be costly. Usually cloud providers charge for external data traffic.

The Cloud&Heat SafeCloudBox is a solution to address the aforementioned problems. First, we plan to offer a storage box that will be deployed on the customer side. All customer's data initially will be stored locally in the box and then only encrypted data will be replicated to the cloud. It allows them to easily switch cloud providers. Second, we would like to take the advantage of our highly distributed datacenters. Customer's data can be stored on the closest datacenter to deliver higher performance. Third, customers will have the option to define the storage policy that reflects their data availability and budget constraints, such as storing one or multiple copies of the data on the cloud or using the cloud as an archival storage.

SafeCloudBox will take advantage of secure data archive (SS2) and secure file system (SS3) developed in the context of the SafeCloud project, to ensure that customers data is safely stored on the cloud

2.3 Maxdata use cases

Maxdata develops healthcare software solutions for electronic requisition, clinical pathology, anatomic pathology, immunohematology (blood banking and transfusion), epidemiologic surveillance (Healthcare Associated Infections) and responsibility terms management. Maxdata will integrate the SafeCloud secure queries technologies with its CLINIdATA® eHealth web application such that this software package, as a whole, can be sold to healthcare institutions. CLINIdATA® main modules are a healthcare laboratory information system (LIS) and an epidemiological surveillance system dedicated to supporting Hospital Infection Control Committees.

Maxdata will use SafeCloud's secure queries technologies and the secure file system to deploy its healthcare software products on the cloud under the Software-as-a-Service model, allowing Maxdata to reach clients located in many developed economies and offer a highly competitive product both in terms of features in price. It is expected that this international growth will allow Maxdata to grow revenue up to 400% by the year 2025.

Using the cloud offers strong advantages, but might also create privacy or security problems, as the data owner lacks the ability to control how and where data is stored, or who can access the data in question by relying on another cloud provider.

Taking advantage of the benefits of the SafeCloud framework, CLINIdATA® may be deployed on the cloud in three different scenarios depending on the customer type and on the features that the customer wants to access, as described next.

2.3.1 SaaS Deployment

For small and medium healthcare organizations that want to reduce costs on infrastructure, CLINIdATA® will be offered using the Software-as-a-Service (SaaS) where all components are deployed on cloud providers contracted by Maxdata. Healthcare organizations subscribe access to the software and pay per use. Different kinds of cloud providers are used for the different layers of CLINIdATA®:

- CLINIdATA® stateless application server – i.e., CLINIdATA® processing component - is deployed on a trusted private cloud owned by a cloud provider, which is trusted for processing but not for long-term storage.
- CLINIdATA® data is stored in a set of untrusted public cloud providers. Availability and integrity are guaranteed by the mechanisms already existing in most of the public cloud providers (e.g., Amazon, Google). Confidentiality of private data, including personal data, is guaranteed by the SafeCloud secure multi-cloud database server (SQ2) and the SafeCloud secure file system (SS3).
- Secure channels are used for the communication between the trusted and the untrusted clouds.

Figure 2 depicts the way CLINIdATA® is integrated with the SafeCloud framework in a SaaS deployment. Before the initial deployment, the healthcare organization defines the location (e.g., country, state) where data may be processed and stored. Cloud providers are selected accordingly.

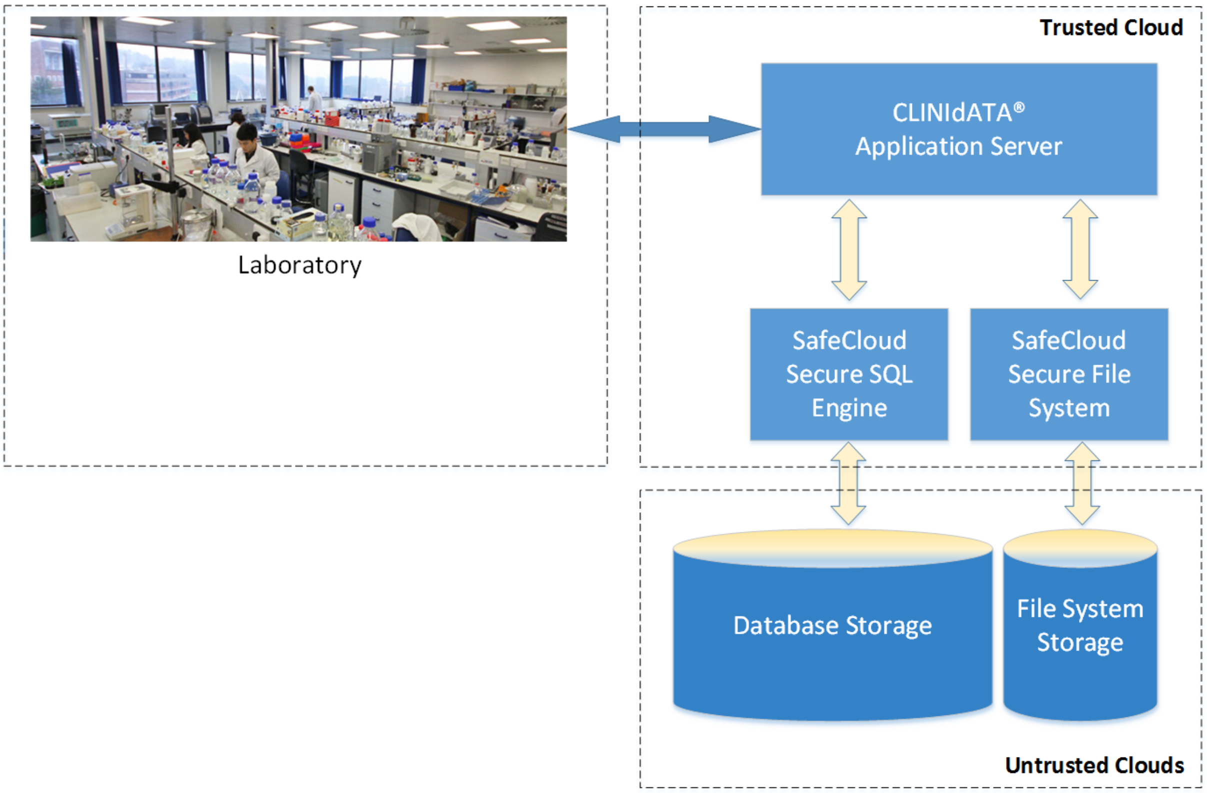
Laboratory
Trusted Cloud
CLINIdATA® Application Server
SafeCloud Secure SQL Engine
SafeCloud Secure File System
Database Storage
File System Storage
Untrusted Clouds

Figure 2: SaaS deployment: integration between CLINIdATA® and the SafeCloud framework.

2.3.2 Hybrid deployment

For large healthcare organizations that want to reduce costs on infrastructure but do not trust on any kind of cloud provider, CLINIdATA® computation/processing will be installed on premises making use of SafeCloud components to access data securely stored on untrusted cloud providers, which are less expensive and more reliable than local storage. In summary:

- CLINIdATA® stateless application server – i.e., CLINIdATA® processing component - is deployed on premises.

- CLINIdATA® data is stored in a set of untrusted public cloud providers. Availability and integrity are guaranteed by the mechanisms already existing in most of the public cloud providers (e.g., Amazon, Google). The SafeCloud Secure SQL Engine (SQ2) and the SafeCloud Secure File System (SS3) guarantee confidentiality of private data, including personal data. Untrusted cloud providers are able to store the data but also to do some processing on top of it without disclosing any sensitive information. This allows reducing the amount of computation done on organizations premises.
- Secure channels are used for the communication between the laboratory premises and the untrusted clouds.

Figure **3** depicts the way CLINIdATA® is integrated with the SafeCloud framework in a hybrid deployment. Before the initial deployment, the healthcare organization defines the location (e.g., country, state) where data may be stored. Cloud providers are selected accordingly.

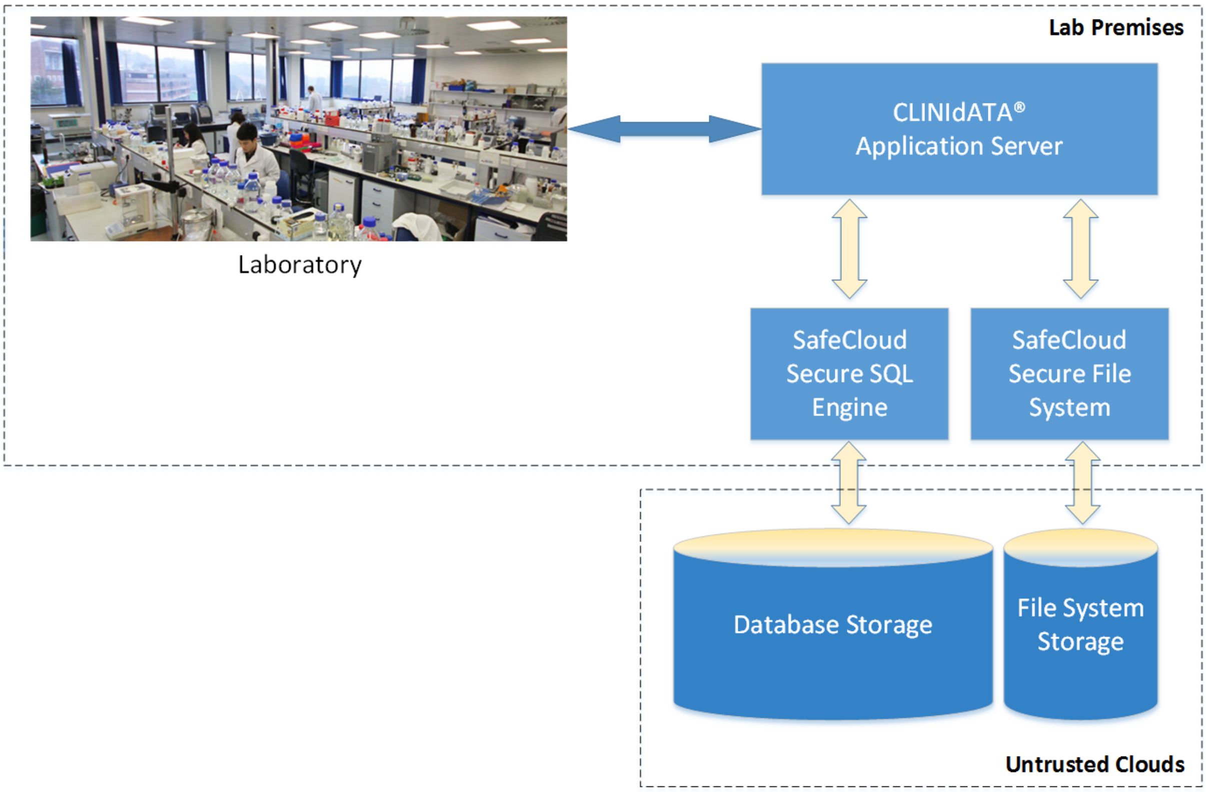

Figure 3: Hybrid deployment: integration between CLINIdATA® and the SafeCloud framework.

2.3.3 Analytics Deployment

For groups of healthcare organizations that want to share analytics on their combined data without revealing the private data of each organization, CLINIdATA® computation/processing will be installed on premises making use of SafeCloud components to access data securely stored on untrusted cloud providers in a way that each healthcare organization is only allowed to put in its private data but cannot make direct queries for data – only aggregated queries are possible. In summary:

- CLINIdATA® stateless application server – i.e., CLINIdATA® processing component - is deployed on premises.

- CLINIdATA® data is stored in the following way:
    - The private data of each organization is stored on its premises. The Secure SQL Engine of each organization participates in a secure multi-party communication protocol to produce the results of aggregated queries.
    - To tolerate cases where some of the organizations Secure SQL Engines are offline, private data is secret-shared and shares are stored in a set of untrusted public cloud providers. Availability and integrity are guaranteed by the mechanisms already existing in most of the public cloud providers (e.g., Amazon, Google). The SafeCloud secure multi-cloud application server component (SQ3) will address the confidentiality of private data, including personal data. The secure multi-cloud application server uses additive secret sharing, and allows a set of SQL operations on encrypted data. However, these operations must be used cautiously because they can leak information. For example, if we calculate the average height of a person in different age groups and the oldest person is alone in the 110+ group, his/her height will leak. We counter this by not returning results when a group has less than a predefined number of members. Likewise, if we can construct queries on two different groups that have a single individual in their intersection, then the difference of the query results will leak that individual's value. Protection against this leakage is not currently enforced, but provided with auditing. The aggregate operations over encrypted data allowed by the secure multi-cloud application server will be discussed in detail in the upcoming deliverable D3.5. The legal issues surrounding the confidentiality of these operations are discussed in Chapter 4 and will be analyzed further over the second half of the project.
    - In this scenario, the SafeCloud Secure SQL Engine is also responsible for ensuring that each healthcare organization can only make aggregated queries for data.
- Secure channels are used for the communication between the hospital premises and the untrusted clouds.

Figure 4 depicts an example of how CLINIdATA® is integrated with the SafeCloud framework in an analytics deployment. In this example, two Portuguese hospitals that share analytics on epidemiological surveillance using SafeCloud components to protect their own private data, while sharing aggregated information. Before the initial deployment, the healthcare organizations define the location (e.g., country, state) where data may be stored. Cloud providers are selected accordingly.

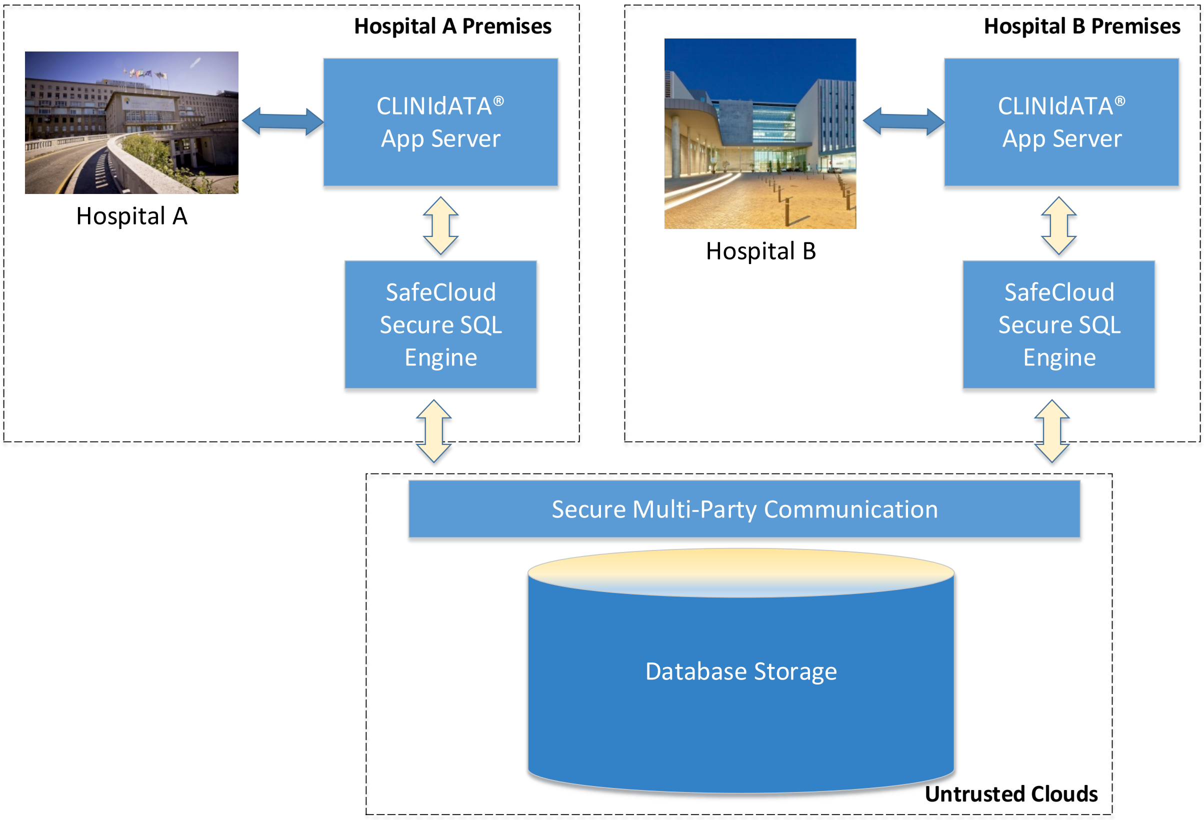

Figure 4: Analytics deployment: integration between CLINIdATA® and the SafeCloud framework.

3 Impact of the GDPR on SafeCloud

This section summarizes the impact of the GDPR on the SafeCloud project. The results are described in Table 1. Each relevant article of the GDPR includes a short description and its impact on the SafeCloud platform.

Article	Description	Relevance with SafeCloud
1	This article describes the fundamental rights at stake that inspire data protection legislation.	No direct relevance, but the whole data protection system is designed to protect these objectives in a coherent way
2	This article determines what type of behavior triggers the application of the GDPR	Secure and confidential ways of processing personal data provided by SafeCloud might keep some parties out of the scope of the regulation
3	Determines to which legal body the regulation applies depending on its location	
4	Provides numerous definitions of concepts used further in the regulation	
5	Lay down fundamental principles that must govern any personal data processing	These principles must be followed by each controller as general rules, for their own processing, and when they delegate it
6	This article describes situations in which data processing is considered as lawful	
7	Defines how consent, the major ground for lawfulness must be given	Controllers who will collect and process data will have to be able to prove a lawful consent
8	Provides special legal condition for children's consent	No direct relevance, but the controller must pay attention for specific conditions in relation to children
9	Establishes a special legal regime for categories of data that are considered as especially sensitive	As Maxdata's use cases will focus on the storage and processing of medical data, compliance with special rules related to sensitive data such as medical data will be mandatory
10	Provides special conditions for criminal convictions and offences	
11	Precises that when a controller has no obligation under the GDPR to keep personal data and when the identification of the data subject is not necessary anymore	
12	The controller has an obligation to be transparent and to inform the data subject of the processing and its modalities	
13	Determines the information the controller must transmit to the subject when collecting personal data	The controller using SafeCloud must be able to provide the information required in order to lawfully process personal data
14	This article follows the same purpose than article 13, but in situations where the data has not been obtained from the data subject	

15	The controller has the obligation to tell the data subject if, and to what extent, he processes personal data related to him	In cloud computing schemes involving multiple parties, such as some of SafeCloud use cases, it might be difficult for the controller to be able to provide the required information
16	The controller has the duty to rectify inaccurate personal data	Anti-tampering techniques as those developed by SafeCloud might not allow to erase the data in question but to store the rectification as new copy
17	The controller has the duty to erase personal data under certain circumstances	Anti-tampering techniques do not allow for a total and definitive deletion of the data. However, eventual deletion after a certain time has elapsed, and techniques to block the access to the data so that processing is no longer possible, might be feasible
18	This article defines in which situations the controller must cease to process the data without erasing it	The controller using SafeCloud must be able to ensure that both him or the processor ceased to process the data
19	Besides the obligations of articles 16 to 18, the controller must also communicate the rectification, erasure or restriction to whom he disclosed the data in question	
20	The controller has the obligation to transfer a copy of the data he holds that is readable for another controller	
21	The controller shall no longer process personal data when the data subject objects to the processing, when the legitimating ground is not a mission of public interests, or the private interest of the controller	
22	Provides a particular framework for decisions based solely on automated systems or profiling	
23	Provides a general framework for restrictions of data subject's right in certain particular domains	Domains such as public or national security or defense are regulated by Member States. As a result, the controller might have to face further obligations from national laws
24	Establishes a general responsibility for the controller to implement organizational and technical measures in order to ensure and demonstrate compliance with the GDPR	This article is fundamental for the functioning of the GDPR. The controller has the responsibility to protect personal data: By using technical measures, such as the technologies developed by SafeCloud; By organizing the processing of personal data and choosing partners that ensure compliance with the regulation
25	Imposes a general duty for the controller to implement measures encouraging privacy by design and privacy by default	SafeCloud's technology clearly follows this purpose, enhancing security and confidentiality in the cloud is one of the major aims of the consortium
26	Determines how joint controllers must organize themselves in order to avoid holes in the protection	In cloud computing schemes involving multiple parties, it might happen that some parties act as joint controllers

27	Obliges controllers and processors who are not established in the EU, but offer goods and services or profile EU Citizen to appoint a representative.	
28	Determines the obligations of parties which are qualified as personal data processor	Most of SafeCloud use cases involve a processor who will have to follow the rules provided by this article
29	Provides a general duty for the processor only to process data under the instruction of the controller	
30	Obliges the controller to record its activities	
31	Obliges the controller to cooperate with supervisory authorities of article 51 and following	
32	Imposes an obligation for the controller and the processor to implement technical and organizational measures to ensure data security	SafeCloud technology provides efficient technical measures to ensure data security and confidentiality
33-34	Obliges the controller to notify both supervisory authorities and data subjects of data breach	
35-36	Defines when and how data protection impact assessment must be carried out and obliges the controller to consult the supervisory authority when the data protection impact assessment results in a high risk	By processing sensitive data in the cloud with a technology that surpasses the state of the art, such impact assessment is mandatory for Maxdata use cases
37-39	Defines situations in which a data protection officer must be appointed, and what his tasks are	
40-43	Encourages the elaboration and the application of codes of conduct in order to promote the proper application of the regulation	
44-50	Provides a general interdiction to transfer personal data to third countries, unless the GDPR conditions are met	Secure communication middleware allows to easily control the transit and the location of the data
51-67	Obliges member states to appoint independent public supervisory authorities responsible for the monitoring of the regulation. Defines how they execute their tasks, who can seat in, what are their competences, tasks and powers, and how they work together	
68-76	Institutes a European Data Protection Board, which has for task to monitor and ensure the consistent application of the regulation and make reports regarding data protection.	
77-81	These articles define who can lodge a complaint with supervisory authorities,	

	and who has a right to effective judicial remedies related to this decision, or a potential violation of the regulation from the controller or the processor	
82	This article provides that any person who suffered damage resulting from the infringement of the regulation have the right to receive compensation from the controller or the processor	
83-84	This articles determine how and according to which criteria administrative fines can be imposed by supervisory authorities	
85-91	These articles leave Member States room in order to organise their legislation in relation to freedom of information, public documents, employment or scientific, statistical or historical purpose take in account both freedoms	
92-99	These articles organize the entry into force of the directive, and its relations with the already existing legal framework	

Table 1: Impact of the GDPR on the SafeCloud platform

4 Issue I: The concept of data

This section addresses the material scope of the GDPR and in particular the notion of personal data. Indeed, among various categories of data, the GDPR is only applicable to the processing of personal data. A controller who processes non-personal data, for example, through the design of the technology he uses, or the service he intends to propose, has no responsibility under the GDPR. Especially, anonymization techniques may allow to qualify the data as non-personal according to Article 4 § 1 and Recital 26 of the GDPR.

4.1 Material scope of the GDPR

According to article 2, the *"regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system".*

Although the definition of personal data is, in the GDPR, a little bit broader than the previous definition from the Directive 95/46/EC, now clearly including identification numbers, location data and online identifiers, the fundamental criteria previously laid down remain the same[1].

4.1.1 Processing …

Article 4 § 2 defines processing as: *"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"*.

4.1.2 … of personal data …

Article 4 § 1 defines personal data as "*any information relating to an identified or identifiable natural person".* According to Article 2, the regulation applies to the processing of personal data wholly or partly by automated means.
The Article 29 Working Party drafted an opinion in order to define this notion. Four criteria have to be fulfilled in order for data to be personal:

- **Any information:** no matter the nature of the information, whether subjective or objective, or the content of the information, whether strictly private or less personal[2]. It is also to be noted that the protection of personal data is, according to the European Court of Human Rights, an independent fundamental right, broader than the mere notion of private sphere protected by the right to privacy[3]. The format of the data is technologically neutral, and is designed to encompass any further development[4];

[1] BOARDMAN R./MULLOCK J./MOLE A., *Bird&Bird guide to the General Data Protection Regulation*, London, 2016, p. 6

[2] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion N° 4/2007 on the concept of personal data*, adopted on 20 June 2007, p. 6

[3] Article 8 ECHR, WALTER J.-P., *le droit à l'oubli, la perspective européenne,* in : GIANORA T., (édit) l*e droit à l'oubli : du mythe à la réalité*, CEDIDAC, Lausanne, 2015, p.12

[4] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion N° 4/2007*, p. 8

- **Relating to:** the information has to be in relation to the data subject. This block encompasses direct relations, such as a subject's personal data on a medical record, but also looser relations which indirectly refers to the data subject, for example when data does not concern an individual but can be tied to an individual based on other data[5];

- **An identified or identifiable person:** The data must be linked to an individual that can be sorted out of the group. Identifiability depends on the group and the data in possession of the controller. The person can be directly identified by name, or indirectly identified, when data and combination of different criteria allow to narrow the group to which the subject belongs[6]. This notion has been specified in the GDPR, encompassing location data, online identifiers and genetic, mental or economic data which can make a person identifiable[7]. As a result, three types of factors lead to identification:

    - **A direct reference.**

    - **A reference through an identifier**

    - **A reference through special personal characteristic[8]**;

- **A natural person:** the subject must be a natural person in order to be protected, no matter the country in which this person resides, or his nationality. Legal persons are not concerned by the GDPR. However, some data relating primarily to legal persons may indirectly apply to natural persons, for example the data of a company's employees[9].

4.1.3 … by automated means

The main reason why processing personal data is relevant is that the development of ITCs allows for an even easier and more widespread access to personal data in the electronic form[10]. According to the DPD, Recital 27 states that although the provision must remain technically neutral, manual treatment, unless structured in order to offer an easy identification, shall remain out of the scope of the directive. Recital 15 of the GDPR maintains this distinction[11].

4.2 Personal data: a relative perspective

Once the data in question is qualified as personal, the processing of that data falls within the scope of the GDPR which follows in this situation the reasoning of the previous DPD, proposing a dualistic approach: either a data is personal, or it is not. However, identifiability depends on the efforts and means at disposal of the controller to link the data to the natural person, and it is thus not simple to assess what type of behavior falls out of the scope of the GDPR[12].

[5] Article 29 Data protection Working Party, *Opinion N° 4/2007*, p. 9

[6] Article 29 Data protection Working Party, *Opinion N° 4/2007*, p. 13

[7] Article 4 para. 1 GDPR

[8] Spindler G./Schmechel P. *Personal Data and Encryption in the European General Data Protection Regulation*, in : Dreier T./Metzger A/Spindler G, JIPITEC – *Journal of Intellectual Property, Information Technology and E-Commerce Law*, vol. 7, p. 3

[9] Article 29 Data protection Working Party, *Opinion N° 4/2007*, p. 23

[10] Article 29 Data protection Working Party, *Opinion N° 4/2007*, p. 5

[11] Recital 27, Directive 95/46/CE, recital 15, GDPR

[12] Spindler/Schmechel, p. 4

The article 29 Working Party also seems to adopt a relative approach when assessing the identifiability of the data. Even if the opinion in question was issued for the DPD, the wording of its recital has not changed on this point in the GDPR, stating that all the means likely reasonable to be used should be taken into account in order to assess identifiability. This seems to refer to a relative approach[13].

Recital 26 of GDPR specifies that in order for a natural person to be identifiable, *"account should be taken of all the measures reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person, directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purpose[14]".* According to this paragraph, anonymization is relative. In order to fall out of the scope of the new regulation, a controller using the state of the art technology must not be able to identify the data subject without having to use unreasonable means in order to do so[15].

Moreover, all factors such as costs, the intended purpose, the structure of the process, the advantages expected by the controller, the personal interests at stake as well as breaches of confidentiality duties and technical failures shall be taken into account when assessing identifiability[16].

However, this relative prospective is counterbalanced in some aspects. At first, the same recital also takes into accounts the measures and efforts of third parties, which could be anybody with any type of equipment[17.]

According to Article 4 § 5 of the GDPR, "*pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".*

This definition is new to the GDPR, and may complicate the definition of the clear extents of anonymous data. Indeed, Recital 28 states that pseudonymisation shall be seen as a way to reduce the risks of the data subjects, but not as a way to step out of the scope of the GDPR. Under an absolute approach, encrypted data, which meets the elements of pseudonymisation will never be considered as anonymous[18].

The GDPR, sadly does not bring a clear answer to a question that is already crucial for the application of the DPD principles.

[13] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion N° 4/2007,* p. 15

[14] Recital 26, GDPR

[15] DE TERWANGNE C., *La réforme de la Convention 108 du Conseil de l'Europe,* In CASTETS-RENARD (édit), *Quelle protection des données personnelles en Europ*e ? Larcier, Bruxelles, 2015, p. 84

[16] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion N° 4/2007*, p. 15

[17] SPINDLER/SCHMECHEL p. 3

[18] Recital 28, GDPR, SPINDLER/SCHMECHEL p. 15

4.2.1 Anonymous encrypted data according to the relative view

Having recourse to the cloud in order to store or process data has many advantages. However, its greatest flaw is that the user leaves the control of the security and resilience of the data he stores to the cloud provider. Encryption of the data stored is an efficient mean in order to keep control over privacy and security of the data. Moreover, encryption is one of the main measures a controller can resort to in order to comply with his data protection duties or even to avoid such duties[19].

Unfortunately, the GDPR does not provide a definition of encrypted data, and only uses such notion as compliance requirements, or a mean to enhance security. As a result, even encrypted data must be assessed on the same basis as clear data, depending on the identifiability of the data subject[20]. The question that must be answered is thus: can the data, as encrypted in the situation in question, be linked to a natural person? Among usual means of encrypting data, the length of the key, as well as its management and the evolution of the state of the art have to be taken into account in order to assess the level of identifiability.

4.3 Schematic view of the material scope of the GDPR

Three types of data can be stored on a cloud provider service with regards to the general data protection regulation:

- Data that does not relate to an identified or identifiable person. Such data falls out of the scope of the regulation, and no special question of compliance in relation to the GDPR appears. According to a relative approach, encrypted data may enter this category;

- The data is qualified as personal, but the data controller is a natural person that processes it in the course of a purely personal or household activity according to Article 2 § 2 let. c. Such processing also falls outside the scope of the GDPR. According to an absolute approach, encrypted data falls within this category;

- The data is qualified as personal, and the controller does not meet the requirements of the purely personal activity, and in that case, he must fully comply with the GDPR.

4.4 Legal and technical recommendations in relation to use cases

As only personal data falls within the scope of the GDPR, the best way to mitigate legal risks in relation to fines and liability is for the cloud provider himself not to deal with personal data. However, the notion of processing is very broad and encompasses for example the encryption process of data. As a result, from the mere storage provider prospective, the best way to get rid of the obligations provided by the general data protection regulation, either for its own liability or in order for the data controller to be able to comply using the cloud provider services, is to store only encrypted data.

Nevertheless, the mere encryption of the data does not definitely take it out of the scope of the GDPR. Account shall be taken of the factual situation, and advantages balanced with both technical or organizational risks, in order to clearly assess the identifiability of the

[19] SPINDLER/SCHMECHEL p. 169
[20] SPINDLER/SCHMECHEL p. 170

data. For example, if the encryption key is stored together with the data, the host can trivially identify data records by decrypting the records with the key.

4.4.1 Cloud&Heat CloudBlockStorage deployment

It first must be noted that data stored on Cloud&Heat services may not always be considered as personal data. Data can be non-personal as such, but account must be taken of those that are also indirectly related to an individual. It must also be noted that the notion of personal data now clearly encompasses identification numbers or location data.

In cases where the client wants to use personal data and does not encrypt it, Cloud&Heat's data processing will fall within the scope of the GDPR. In cases where the data in question is encrypted, an absolute view about the notion would imply that, as the client owns the data and can collude with Cloud&Heat, the data remains personal, thus also triggering the application of the GDPR. On the other hand, with a relative approach, Cloud&Heat would fall out of the scope of the GDPR in cases where it does not dispose of technical means to easily decrypt the data.

4.4.2 Cloud&Heat SafeCloudBox deployment

In this situation, an intermediary element, the SafeCloudBox, appears between the client and the storage. It processes the data on a trusted cloud, or on the client's premises, and encrypts the data before sending it to the cloud.

In this situation the storage provider only processes encrypted data and is unable to read the data in question, unless colluding with the data controller or client. As a result, the storage provider does not fall within the scope of the GDPR according to a relative perspective.

4.4.3 Maxdata SaaS Deployment

The Maxdata healthcare platform is based on an eHealth web application owned by Maxdata. Its objective is to provide management and control capabilities over medical, or medically related data to healthcare organizations such as hospitals, clinics, laboratories and primary care units of different sizes.

In the SaaS deployment, designed for small and medium-scale business organizations and undertakings, all components will be deployed on a third party cloud provider. Data processing will be deployed on a trusted cloud provider, but will be stored using a secure file system and secure SQL solution on untrusted cloud providers, rendering the last cloud provider unable to read the data in question.

In this situation, the GDPR will be applicable for both the user and the trusted cloud provider, and thus compliance is necessary, especially for such particular data as medical data.

On the other hand, as the second cloud provider will never see the raw data, and will only transmit and store data that he cannot link to any identifiable person, the GDPR will not be applicable, provided that the further legal development will adopt a relative approach with encrypted data.

4.4.4 Maxdata Hybrid Deployment

This use case is designed for organizations that still want to benefit from the cloud's advantages, but do not trust cloud providers. The processing will be done on the client's premises, but will still be stored on untrusted cloud providers. Again, the SafeCloud SQL engine and the SafeCloud file system will be used to ensure security and privacy.

Here, the intermediary cloud provider disappears. As a result, the client is responsible for the collection and processing of the data in question, thus, the GDPR will apply to him/her. However, the GDPR will not be applicable to the cloud provider who will only store encrypted data.

Nevertheless, it is to be noted that the obligation of the controller to ensure privacy and security also encompasses the technical and organizational means of any of his partners. As a result, the controller must choose a cloud provider that guarantees compliance with the GDPR[21].

4.4.5 Maxdata Analytics deployment

Groups of healthcare organizations that want to share analytics on their combined data without having to disclose their own data can use Maxdata's analytics deployment.

The processing is still done on each client's side and stored on untrusted clouds, but here, each organization's Secure SQL Engine will participate in a secure multi-party communication protocol.

Private data is also secret-shared, and shares are stored in a set of untrusted public clouds. Each share is necessary to reconstruct the data and perform processing on it. However, only the result is transmitted to the client who asks for analytics while the shares remain secret.

In this case, the application of the GDPR will depend on the situation. The division of the data into shares cannot be considered, under a relative prospective as personal data, as the purpose of secure multiparty computation is to distribute shares so that no party is able to reconstruct the data without the other shares. As a result, the GDPR would be only applicable to the cloud client who collected the data of a certain patient. The analytic processing of the personal data does not allow the other cloud clients who participate to identify the data subject, and thus they must fall out of the scope of the GDPR

The activities of the cloud providers should remain out of the scope of the GDPR, as long as the data remains non-personal through technical and organizational measures, such as for example providers chosen for their inability to collude, or contractual guarantees not to collude.

[21] For further developments in this issue, see Chapter 5

5 Issue II: Responsibility for Data

The whole system of compliance of the GDPR is organized around the data controller. The entity who determines the purpose and the means of the processing of personal data has to comply with the obligations of the GDPR, and may face some fines in cases where he fails. This is especially true in cloud computing schemes, where the whole process of collecting and processing personal data is shared among numerous entities. One party collects the data and needs the processing, but leaves another undertaking perform the task. It is thus of paramount importance to know each party's status, in order to clearly establish its obligations.

5.1 Data controller as the cornerstone of data protection efficiency

The data controller qualification for an entity plays an almost as important role for data protection as the qualification of personal data. Indeed, the qualification of controller *"determines who shall be responsible for compliance with data protection rules, how data subjects can exercise their rights, which is the applicable national law and how effective Data Protection Authorities can operate"*[22].

Due to the increasing number of parties in the environment of data processing, the assessment of controllership can become complicated. Cloud environments might involve different parties that play different roles in the processing, and the controller might delegate some of his prerogatives. For example, it is the controller's duty to determine how the process will take place technically. By contracting with a cloud provider and outsourcing a part of the process, it sometimes has to agree on pre-written terms and conditions. However, the notion is technologically neutral, thus independent of the evolution of the technological context[23].

5.2 Elements of the definition

According to Article 4 § 7, *"'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data".* This definition does not differ from the previous one under the DPD.

5.2.1 A natural, legal person or any other body…

The definition is broad, and is designed to ensure the effective application of the GDPR. The range goes from natural to legal persons, but also other public bodies. Legal bodies are privileged over natural persons when the processing activity takes place within its realm of activities and risks[24].

5.2.2 Who determines the purpose and means of the processing…

The ability to determine the purposes and means of the processing is an independent concept that can stem from different situations.

According to Article 29, *"Being a controller is primarily the consequence of the factual circumstance that an entity has chosen to process personal data for its own purposes.*[25]*".* In

[22] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion N° 1/2010 on the concepts of "controller and "processor", adopted on 16 February 2010, p. 3*

[23] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion N° 1/2010,* p. 4

[24] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion N° 1/2010,* p. *15*

[25] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion N° 1/2010,* p. 10

order to determine the controller, we must determine who initiated the processing and why such processing is taking place[26].

5.2.3 … Alone or jointly with others

In case of situations in which multiple parties are involved in the act of processing personal data, the qualification of each party is important. Indeed, a single processing operation purpose and means can be determined by multiple parties. By stating that the controller can act alone, or jointly, the legislator considered that in some situations, the burden of responsibility should be borne by each party who acts as a controller, and the identification of a controller did not qualify every other party as a processor[27].

5.3 The particular case of joint controllers

Parties have a great latitude when they organize themselves to process personal data. Different controllers might be involved in the processing operation, simultaneously, or at different stages of the operation.
As a result, even if one of the parties clearly determines the purposes and the means of the processing, for example the hospital who decides to store medical data on the cloud, a form of joint control over the data remains possible in situations where the cloud service provider takes part in the determination of the purposes and means jointly with the hospital, or at a later stage of the processing[28].

5.4 The status of the processor

According to the GDPR, the processor is any *"natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"[29].*

This status applies to who processes personal data, but does not take part in the determination of the purposes and means of the processing.

Two conditions induce the qualification of processor:

- The processor must be a distinct entity from the controller;
- The processor must process personal data on the controller's behalf. The crucial element here is to determine for who's interest the data is processed, and who controls the processing[30].

It must also be noted that the territorial scope of the GDPR has been extended to processors established outside the EU when their processing activity is related to the offering of goods or services, or to the monitoring of data subjects in the Union[31].

This is, depending on the circumstances, the default status of a cloud service provider. Indeed, in principle, the cloud client determines the purpose and the means of the processing activities. The use of cloud services can be seen as an externalised tool, and the cloud provider's processing activities are usually made on the controller's interest[32].

[26] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion N° 1/2010,* p. 10
[27] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion N° 1/2010,* p. 17
[28] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion N° 1/2010,* p. 18
[29] Article 4 para. 8 GDPR
[30] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion N° 1/2010,* p. 25
[31] Article 3 GDPR
[32] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion N°05/2012 on Cloud computing,* adopted on 1st July 2012, p. 7

However, the client loses a certain amount of control over the processing. It is difficult for the controller to have a clear view on how the data is stored, on which infrastructure and according to which security conditions. As a result, the cloud provider might have an important influence on how the processing takes place, thus can be also considered as a joint controller[33]. Moreover, the cloud provider might also process personal data for his own purpose[34].

5.5 The relation between the controller and the processor

According to the UK ICO[35], *"the controller says how and why personal data is processed and the processor acts on the controller's behalf"[36].*

Data responsibility, in schemes involving multiple parties, is of paramount importance.The client of Cloud&Heat infrastructure, or of Maxdata software can be considered as a controller under the GDPR, as he determines the purposes and means of the processing of the personal data. According to Article 24, the controller shall implement appropriate technical and organizational measures to ensure and be able to demonstrate that processing is performed in accordance with the regulation.

As a result, the controller must ensure that data has been processed lawfully, fairly, and transparently. He must have a legitimate purpose for processing such data, and make sure he follows principles such as data minimization, accuracy, integrity and confidentiality.

The Article 29 Working Party, in opinion 05/2012 [37] states that *"businesses and administrations wishing to use cloud computing should conduct, as a first step, a comprehensive and thorough risk analysis. All cloud providers offering services in the EEA should provide the cloud client with all the information necessary to rightly assess the pros and cons of adopting such a service. Security, transparency and legal certainty for the clients should be key drivers behind the offer of cloud computing services[38]".*

Indeed, and despite the question whether or not the cloud service provider shall be considered as a controller or a processor, the controller, to meet his responsibilities must choose a service that guarantees compliance with the GDPR[39]. He must assess the risks and advantages of having recourse to a specific cloud service[40]. In other words, the question the controller must ask himself is: am I able to fulfil my duties according to the GDPR when I use such specific cloud service?

On this question, we currently are working on the particular legal aspects and specificities of different cloud offerings, such as Infrastructure-as-a-Service, Platform-as-a-Service or Software-as-a-Service.
Two main points are of particular importance in this situation:

[33] INFORMATION COMMISSIONER'S OFFICE, Guidance n° 20140506, *Data controllers and data processors: what the difference is and what the governance implications are,* para 22 21

[34] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion N°05/,* p. 8

[35] The ICO is the UK's independent body set up to uphold information rights, and in particular to cover the compliance with the UK's data protection act, designed to implement the directive 95/46/EC

[36] INFORMATION COMMISSIONER'S OFFICE, Guidance n° 20140506, *Data controllers and data processors: what the difference is and what the governance implications are,* p.

[37] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 5/2012 on Cloud Computing, adopted on the 1 July 2012*

[38] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 5/2012,* p. 2

[39] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 5/2012,* p. 2

[40] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 5/2012,* p. 4

- By using cloud computing services, the controller might not be able to take only organizational or technical measures in order to ensure the principles and duties in relation to data;
- By outsourcing a part of the processing, the controller might not obtain enough information from the cloud service provider, thus he might not be able to take appropriate measures to counter threats and risks according to its own obligations[41].

However, according to Article 28 GDPR, it is the controller's duty to *"use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."* In other words, organizational questions shall not interfere with the protection of the data subject's rights.

Thus, compliance with the GDPR from the Cloud provider prospective is also of paramount importance, as a controller who chooses a non-compliant provider is liable in relation to any violation of the data protection regulation, and thus will look for a processor that guarantees this compliance.

5.6 Legal and technical recommendations in relation to use cases

5.6.1 In general

The contractual way is not only a good way to clarify the situation between two parties, it is also mandatory according to Article 28 GDPR between a controller and a processor. Such contract must, according to the Article 29 Working Party, contain the following elements

- What type of instructions will the processor follow?
- What are the risks, and what countermeasures will be used by the processor;
- The subject and timeframe of the cooperation, and most importantly what will happen at the end of the cooperation, in relation to the erasure of the data;
- The obligation for the processor not to disclose the data he deals with;
- The obligation for the processor to support the controller in cases where a data subject exercises a right;
- The obligation to notify the controller in case of breach of data;
- Where the data is physically stored;
- A way for the controller to monitor the actions of the cloud provider, specifically any modification of its services, and a procedure of audit;
- A general obligation for the processor to comply with the principles of data protection[42].

A contract containing such clauses protects the controller from potential violations on the processor side. A processor thus must be able to respect those obligations in order to be able to propose a GDPR compliant behavior even though the obligations do not directly apply to him.

[41] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 5/2012,* p. 6
[42] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 5/2012,* p. 14

5.6.2 Cloud&Heat CloudBlockStorage deployment

In this situation, Cloud&Heat will be considered as a processor in cases where the client decides to process personal data. According to Article 28, the controller shall only use processors who provide sufficient guarantees to implement appropriate technical and organisational measures in order to ensure data subject's right.

5.6.3 Cloud&Heat SafeCloudBox deployment

In this situation, the client who collects personal data is considered as a controller. He also controls where the processing component is deployed: under the control of the same legal person, and in this case there is no processor, or on a trusted cloud. The cloud provider shall in this situation be considered as a processor, unless he uses the data for its own purpose.

The situation of the public cloud remains out of the scope of the GDPR. However, the client will still have to fulfil his duties.

5.6.4 Maxdata SaaS Deployment

Each of Maxdata's clients, such as laboratories or small and medium healthcare organizations, shall be considered as data controllers under Article 4 § 7 GDPR. As a result, they are the primary recipients of the duty of compliance.

The cloud provider, on which the processing component is deployed, shall be considered as a data processor in cases where it only processes data on behalf of the controller. Two elements are important: the data must be processed for the client's interest, and under his control. If the cloud provider uses the data for its own purposes, or collects information itself, he will become a joint controller.

In this deployment, Maxdata will act as an intermediary. The client will acquire the service from Maxdata whose role is to act as a mediator and be responsible for the security of the complete solution, who will be in a contractual relation with the cloud providers. In such an intermediary situation, Maxdata shall be considered also as a processor, provided the data is processed for the client's interest and under his control.

The untrusted cloud provider who stores the data shall qualify neither as a controller nor as a processor, as it does not process personal data.

However, compliance with the GDPR must not be neglected for the trusted cloud provider because of its processor status. Indeed, it is the responsibility of the controller to guarantee compliance both in cases where he processes himself, or delegates the task. As a result, the controller must obtain both technical (e.g., ones provided by SafeCloud technology) and juridical guarantees.

Thus, we recommend, both for the client and the cloud provider's sake to contractually clearly define their roles both legally and technically. The controller must make sure that he remains able to comply with the GDPR, and the cloud provider must be certain that he is considered as a processor.

5.6.5 Maxdata's hybrid deployment

In this situation, the trusted cloud part is deployed on premises, thus the client and the trusted cloud are the same legal person with direct legal duties to the data subject.

The untrusted public cloud provider here remains a third party.

5.6.6 Maxdata's analytics deployment

In this situation, each client is considered according to the GDPR as a controller for the data it obtains and stores.

The question remains to know whether or not, for processing of data through aggregated queries, each client acts as a joint controller, or is only able to process non-personal data. This qualification depends on what type of data can be queried by each party. If the data in question can relate to a personal body, thus each client will be considered as a controller.

As a result, we recommend for the parties to contractually define in which depth queries by other clients can be answered in order to stay out of the qualification of joint controller and the duties related.

The cloud providers, as long as technical and organisational measures prevent them to collude remain out of the scope of the GDPR, and are considered only as third party.

6 Issue III: Legal duties related to the data subject's rights

According to the GDPR, data subjects have a range of rights. Furthermore, it is the duty of the controller to be able to let data subjects exercise their rights. Among those rights, the right to rectification and erasure, quite new, might enter into conflict with security requirements.

6.1 Lawfulness of the processing

According to article 6 GDPR, data shall only be processed on a lawful ground, which means:

- When the data subject has given consent for a specific purpose;
- When the processing is necessary for the performance of a contractual task
- When the controller has to fulfil a legal obligation
- In order to protect the vital interest of another natural person;
- In order to perform a task for the public interest, or in the exercise of official authority
- When the processing is necessary for the purpose of the controller's legitimate interests, when this interest is not overridden by the data subject's fundamental rights[43].

The approach towards consent has been improved, and it must now be given for a specific form of processing according to article 6 § 1 let. a and 9 § 2 let. a.

Any controller must, according to Article 24 of the GDPR, be able to demonstrate the lawfulness of the processing.

6.2 Transparency, information and access

Article 12 imposes on the controller the obligation to provide transparent information to the data subject in order to allow him to coherently exercise his rights. This obligation starts from the collection of the data, and lasts as long as the data exists.

Any controller must be able to give the information required in a concise, transparent, intelligible and easily accessible way[44].

Moreover, the data subject has, according to Article 15 of the GDPR, the right to obtain from the controller confirmation whether or not personal data concerning him is being processed.

6.3 Rectification and erasure

According to Article 17 of the GDPR, the data subject has the right to obtain from the controller the erasure of personal data in certain circumstances:

- When the data is no longer necessary for the purpose for which they were stored;
- When the data subject withdraws his consent;
- When the data subject objects the processing;
- When the data has been unlawfully processed;
- When erasure is necessary for the compliance with a legal obligation.

[43] Article 6 GDPR

[44] Article 12 GDPR

A controller who uses SafeCloud has access to very powerful storage techniques. As a result, and if blocks are entangled in order to offer strong anti-tampering and reliable long term storage, its mere purpose is to avoid total erasure.
In such a situation, deleting all the blocks related to a personal data is nearly impossible and would require to destroy the whole set of entangled data.
However, the notion of erasure in relation to the GDPR is not quite clear and might differ with a technically precise notion of erasure. The legislature, at recital65 requires the data to be erased and no longer processed.
As a result, blocking the access to the data so that it can no longer be processed can be enough, although it has not been physically destroyed. According to the European Network of Legal Experts[45], three remedies can be taken into account in order to comply with the right of erasure:

- The mere erasure of the data, which is the easiest to foresee
- The limitation of the processing, according to which, the access to the data is limited;
- The delisting of the data, as decided by the ECJ, which is nevertheless far from a total erasure of the data[46].

We must also note that the two first solutions also follow the purpose of abstention to further disseminate the data contained in Article 17 of the GDPR.
From the prospective of the ECJ case Google vs. Costeja Gonzales, it seems that what is at stake is the access to the data, and not the data itself. However, the decision took place before the adoption of the GDPR.
The Finnish data protection authority stated in a guideline that as the GDPR did not set the requirements for the technical implementation of the removal, a strict limitation of the access to the data is enough even if the data in question still exists physically. Moreover, encrypting the data with a strong algorithm and then destroying the key or overwriting the data is an option[47].

The United Kingdom has, since 1998, the notion of deletion in its DPA[48]. Article 14 allows courts to order the controller to rectify, block, erase or destroy personal data. As a result, the ICO issued a guidance on the meaning of "deletion", that was not defined in the Act. The ICO also recognizes that due to the development of electronic storage, a literal interpretation of the word was not clear[49], and put an emphasis on the fact that the controller shall be *"absolutely clear with individuals about what they mean by deletion and what actually happens to personal data once they have deleted it[50]".*

The ICO also considers the data as deleted when the information is put beyond use. The data is not formally deleted but the data controller must:

- *Not be capable of using the personal data;*
- *Not give any other organization access to the personal data;*
- *Surround the personal data with appropriate technical and organizational security;*
- *Commit to permanent deletion of the information when it becomes possible[51].*

[45] M. CLEMENT-FONTAINE/ R. AMARO in *: Données de santé,* in : MARTIAL-BRAZ N., *La proposition de règlement européen relatif aux données à caractère personnel : propositions du réseau Trans Europe Experts,* Société de législation comparée, Paris, 2014p. 426
[46] INFORMATION COMMISSIONER'S OFFICE, *Overview of the General Data Protection Regulation (GDPR),* p. 3
[47] J. TOMPPA, *GDPR and Right to Erasure*, October 10 2016 (http://dobefore.net/?p=30).
[48] Data protection Act 1998
[49] INFORMATION COMMISSIONER'S OFFICE, Guidance n°20140226, *Deleting personal data,* p. 3
[50] INFORMATION COMMISSIONER'S OFFICE, Guidance n°20140226, *Deleting personal data*, p. 3
[51] INFORMATION COMMISSIONER'S OFFICE, Guidance n°20140226, *Deleting personal data*, p. 5

We must nevertheless note that this guidance has been issued for the English Data Protection Act, and not the GDPR. However, as the DPA, the directive 95/46/EC and the GDPR follow the same purposes, it would be valuable to take inspiration from it.

6.4 Restriction of processing

The right to restriction of processing of Article 18 GDPR requires the controller to provide a way to block the processing for a certain period of time.

The restriction of processing obliges the controller only to store the data, and not to process it further, unless the data subject gives its consent or the processing is necessary for the protection of the legal rights of another person [52.]

6.5 Portability

Article 20 provides the right for the data subject to obtain from the controller the transmission of his personal data to another controller or to the data subject himself in a structured, commonly used and machine readable form[53].

6.6 Legal and technical recommendations in relation to use cases

From the legal prospective, one thing is certain. A data controller (or a processor when working for a controller) must ensure that, in certain situations, the access to a certain set of personal data can be blocked.

On the other hand, what is uncertain is if the requirement of Article 17 GDPR necessitates that the data must be physically destroyed.

In order to comply with the regulation, it should at least be recommended to introduce a technical procedure, enabling a total restriction to the access, such as for example a new encryption followed by the erasure of the key.

On the legal side, the possibility and the process required to erase the data must be taken into account. The processor should not agree to physically erase the data he processes in situations where it is technically impossible. The controller needs, in order to be able to fulfil his obligations, for example, at the end of the collaboration or when a data subject requires it, to be sure that his processor has the ability to erase the data.

A controller or a processor who uses SafeCloud's Secure Data Archive technology is not able to physically destroy the data, due to the entanglement techniques that protect the data against tampering.

A mitigation scheme would be not to provide an immediate erasure, but to provide a periodical process that allows data subject who asked for deletion to see their its data disappear after a certain amount of time.

This question is really interesting from a legal perspective as the legislator requires the controller to promote both the right to self-determination of the data subject and also to guarantee the safety of the data in question. For example, Article 32 let. c GDPR provides that controllers must be able to restore and ensure the availability of the data. As

[52] BOARDMAN/MULLOCK/MOLE, p. 29
[53] BOARDMAN/MULLOCK/MOLE, p. 24

proposed by SafeCloud, entanglement helps to comply with this duty but seems also to be in conflict with the right to self-determination.

6.6.1 Maxdata SaaS Deployment and Cloud&Heat CloudBlockStorage deployment

The processing component is deployed on a trusted cloud. As a result, the controller must ensure that the technical and organisational measures taken allow him to fulfil his legal duties.

The controller must thus inform the data subject especially on the fact that the data will be processed by a trusted cloud provider and stored on an untrusted one.

The controller must also be able to inform the client of eventual issues, and thus must be informed by the processor in case of problems. The processor must also be able to bring information such as the location or the technical process he intends to use.

Secure Block Storage and Secure File system technologies allow for the erasure of the data. It is however necessary for the controller to clearly define, in his contractual relation with the processor the obligation to erase or to stop the processing on the demand of the controller, and also the procedure that should be used in order to ensure and to prove the erasure.

6.6.2 Cloud&Heat SafeCloudBox and Maxdata's Hybrid deployment

In both these deployments, the controller keeps an important influence on the processing of the data. As a result, the controller's duties are mainly internal to the controller.

As this deployment uses Secure Block Storage and Secure File System technologies, the erasure of the data is not problematic in itself, but a process allowing the keeping of the data out of processing, as well as for its mere erasure, shall be foreseen in advance, and its modalities shall be transmitted to the client.

6.6.3 Maxdata's analytic deployment

In this situation, the legal duties of controllers who use the analytics deployment will depend on the qualification of such data.

7 Issue IV: Data security in relation to medical data

This part focuses on the use cases of Maxdata. Here, the situation is clear: not only personal data will be processed, but sensitive categories of data will be collected and stored. The GDPR put special categories of data under a different framework in order to offer better protection conditions to the data subject.

7.1 Specific categories of data

Article 4 § defines data concerning health as *"personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".*

Such category of data is covered by the general interdiction of Article 9 § 1. In order to be able to process such data, Paragraph 2 provides a list of exceptions. In particular, let. a requires the explicit consent of the data subject, and let. i requires a public interest in the area of public health.

The notion of consent is defined in Article 2 § 11 as *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*.

However, in relation to special categories of data such as medical data, the consent must be explicit, and this notion is not defined in the regulation.

According to the Article 29 Working Party, "*explicit consent encompasses all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing*[54]*".*

Article 7 of the GDPR provides that the data subject can withdraw his consent at any moment. The consent must be freely given. Especially, the consent must not be a conditional to the performance of another part of the contract.

The data controller must be able to prove the data subject's consent according to article 24 § 1. As such, depending on the situation, stronger evidences will be necessary.

7.2 Specific duty in relation to sensitive data

In order to obtain the explicit consent of the data subject in relation to the processing of medical data, but also to prove the lawfulness of the processing, a clear contractual clause is necessary.

In order to mitigate the risks, the data subject must give his consent through a clear affirmative action, for example by signing a special contract in relation to data processing, or by opting in in, for example by ticking a checkbox in a wider contract. The consent must be freely given, specific and informed[55]. It must also clearly depict for what it is given.

Article 9 letters I and J provides exceptions for the processing of personal data in relation to public healthcare or scientific research as legitimating grounds for the processing. Article 89 however provides that mitigation techniques are still necessary in order to process them.

7.3 Security of processing

Article 32 *requires the controller to take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk*

[54] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 4/2007,* p. 25

[55] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 15/2011 on the definition of consent, adopted on 13 July,* p. 8

of varying likelihood and severity for the rights and freedoms of natural persons, in order to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate.
Such obligation depends on the risks related to the processing of the data. As medical data is considered by the regulation as very important, and as storing it in the cloud is new, the system must provide an adequate security. Appropriate measures in this situation will need to be very strong in order to meet this requirement.

7.4 Legal and technical recommendations in relation to use cases

Once again, the controller is responsible to prove the lawfulness and the security of the processing.

7.4.1 Maxdata's deployment

It is the client's duty to ask for the data subject's consent, and to prove it in case of problem. As he processes special categories of data, a specific consent for the specified purpose of storing and using the data is necessary. We recommend the controller to agree in a written form with the data subject on the processing of his personal data. The agreement must clearly depict the purposes and the limitations of such processing and leave the data subject the possibility to disagree.

On a processor prospective, we can note that even if the general liability of the controller obliges the processor to propose a sufficiently strong framework for special categories of data, his own status and obligations do not change depending on the qualification of the personal data

Concerning the analytical deployment, and if the aggregated queries allows for the processing of personal data, a specific consent should not be necessary, as public interest in the area of public health is a legitimate ground provided specific measures to safeguard the subject's rights are taken. The use of secure multi-party computation and secret sharing can be considered as such measures.

8 Ongoing work and outlook for the next deliverable

8.1 Further development of GDPR issues

The oncoming GDPR is wide and introduces various changes for already existing concepts, but also introduces new ones, especially in terms of organization, such as disclosure of breaches of data, or the encouragement of privacy by design and privacy by default. As this deliverable does not exhaustively treat the GDPR related concerns of SafeCloud, our ultimate goal is to conduct a complete privacy impact assessment for each configuration provided by the use cases in order to systematically identify, assess and reduce the privacy risks at stake in the project, thus ensure a full compliance with the GDPR.

8.1.1 Localisation of the data and rules applicable in relation to the security of the communications

SafeCloud introduces new and innovative ways to secure and monitor communications across the architecture. Three solutions are used. First, vulnerability tolerant channels solutions ensure that the failure of any mechanism does not cause a security failure in the whole channel. Then, protected channels introduce multiple methods to reduce the risks of fake certificates or port scans. Third, route-aware channels solutions provide an efficient way to monitor the paths of communication and detect route hijacking[56]. As SafeCloud pushed the state of the art further and offers strong safeguards we foresee to put a special emphasis on compliance in relation to the transfer of personal data across Europe or even outside of the EU.

8.1.1.1 The framework for the processing of data outside of the EU

Chapter 5 of the GDPR discusses the transfer of personal data to third countries.

In relation to the SafeCloud project, untrusted cloud provider can have various policies in relation to the storage of the data they hold. It is thus of paramount importance to clearly assess in which configuration the use cases might involve a transfer of personal data, and how the architecture and organizational measures allow it.

8.1.1.2 The particular case of data in transit

SafeCloud introduces new ways to monitor and control the transit of the data across the system and ensure its confidentiality. We will assess how such technology allows to enhance and guarantee the right and principles established by the GDPR.

8.2 Legal questions related to other branches of law

Data protection is not the only aspect of law affected by the tremendous development of ICTs. For example, during the nineties, the development of internet and of peer-to-peer networks challenged copyright law, facilitating to the extreme the reproduction and sharing of works under copyright. Nowadays, numerous aspects of our lives have been impacted by such technologies, and this revolution is not expected to stop, as both the European Union[57] and Switzerland[58] are trying to develop and expand their digital economy.

[56] Deliverable 5.2, p. 9

[57] European Council, Digital single market for Europe (http://www.consilium.europa.eu/en/policies/digital-single-market-strategy/)

[58] Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC, *Stratégie du Conseil fédéral pour une société de l'information en suisse,* 1ère édition, 2012, p. 5

As technology, and sociological and economical uses of the web change rapidly, both legislatures are now changing or conceiving new rules in order to put a legal framework around those practices[59]. The development of internet has led to the creation of the numerous intermediaries such as content providers, hosts, access or storage providers[60]. The same trend can be seen in relation to personal data processing, and similarities in terms of status or liability could be useful to draw soft law codes of conduct and practices.

One of the particularities of cyberspace law is its hybrid aspect. In parallel to the legal framework enacted by the States which is compulsory, such as, in relation to personal data protection, the Directive 95/46/EC or the new GDPR, there exists a whole set of different soft rules, such as codes of conduct that internet service providers can willingly choose to follow in order to fill the gaps of the legal framework.[61].

The actors of the cyberspace turned to soft-law to fulfil their needs, because they faced a lack of legal certainty due to the difficulty for conventional law to implement a clear framework on internet practices, but were in need of an alternative set of rules[62].

There is a great diversity of soft law: it goes from terms and conditions whose acceptance (often tacit) is required to conclude a contract, to private declarations, or even to guides or recommendations drafted by administrative bodies[63].As contractual agreements are also required by controllers in order to comply with article 24 GDPR, it would be interesting to compare how other branches deal with such questions.

Self-regulation cannot be considered as “law” as it lacks the political legitimacy, and often even the mere quality of being general and abstract. Nevertheless, it can have an important normative effect as it stems from the general acceptance of the participants of the community. Self-regulation is not imposed on participants whose will is to comply[64].

Although it is subsidiary to “hard” law, self-regulation is a framework created by actors of the cyberspace to fill the gaps of the legislation. As such, it can reflect the needs in terms of regulation of society in particular situations. Often redacted by practitioners they inspire both legal doctrine and also jurisprudence[65].

Such practical importance can help to determine the state-of-the-art both in terms of technology and in terms of legal obligations. Besides compliance with the GDPR, the project could lead to the comparison of the legal and contractual framework related to personal data protection with other branches of law that have also been strongly influenced by the development of ICTs, such as copyright law. A comparison of the solutions and problems faced could be very profitable to both domains.

[59] Département fédéral de l’environnement, des transports, de l’énergie et de la communication DETEC, *Stratégie du Conseil fédéral pour une société de l’information en suisse,* 1ère édition, 2012, p. 5

[60] Département fédéral de l’environnement, des transports, de l’énergie et de la communication DETEC, *Stratégie du Conseil fédéral pour une société de l’information en suisse,* 1ère édition, 2012, p. 5

COTTIER B., *Le droit "suisse" du cyberespace,* in : ZSR/RDS, *Rechtsfragen im digitalen Zeitalter = Questions juridiques à l'ère du numérique*, Helbing Lichtenhahn, Basel, 2015, p. 228

[62] WEBER R. H., *Realizing a New Global Cyberspace Framework, Normative Foundations and Guiding Principles*, Schulthess, Zurich Basel Geneva, 2014, p. 26

[63] COTTIER, p. 229

[64] WEBER, p. 27

[65] COTTIER, p. 229

9 Bibliography

Article 29 Data protection Working Party, *Opinion N° 1/2010 on the concepts of "controller and "processor", adopted on 16 February 2010*

Article 29 Data protection Working Party, *Opinion N° 04/2007 on the concept of personal data*, adopted on 20 June 2007

Article 29 Data Protection Working Party, *Opinion N°05/2012 on Cloud computing,* adopted on 1st July 2012

Article 29 Data protection Working Party, *Opinion 15/2011 on the definition of consent, adopted on 13 July*

Boardman R./Mullock J./Mole A., *Bird&Bird guide to the General Data Protection Regulation*, London, 2016

Clement-Fontaine M./Amaro R. in *: Données de santé,* in : Martial-Braz N., *La proposition de règlement européen relatif aux données à caractère personnel : propositions du réseau Trans Europe Experts,* Société de législation comparée, Paris, 2014

Cottier B., *Le droit "suisse" du cyberespace,* in : ZSR/RDS, *Rechtsfragen im digitalen Zeitalter = Questions juridiques à l'ère du numérique*, Helbing Lichtenhahn, Basel, 2015

Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC, *Stratégie du Conseil fédéral pour une société de l'information en suisse,* 1ère édition, 2012

De Terwangne C., *La réforme de la Convention 108 du Conseil de l'Europe,* In Castets-Renard (édit), *Quelle protection des données personnelles en Europ*e ? Larcier, Brussels, 2015

Gasser U., *Perspectives on the Future of Digital Privacy*, in: ZSR/RDS, *Rechtsfragen im digitalen Zeitalter = Questions juridiques à l'ère du numérique*, Helbing Lichtenhahn, Basel

Information Commissioner's Office, Guidance n° 20140506, *Data controllers and data processors: what the difference is and what the governance implications are*

Information Commissioner's Office, Guidance n°20140226, *Deleting personal data*

Information Commissioner's Office, *Overview of the General Data Protection Regulation (GDPR),* 13 October 2016

Salvadé V., *droit d'auteur et technologies de l'information et de la communication,* Schulthess, Geneva, 2015

Spindler G./Schmechel P. *Personal Data and Encryption in the European General Data Protection Regulation,* in : Dreier T./Metzger A/Spindler G, JIPITEC – *Journal of Intellectual Property, Information Technology and E-Commerce Law*, vol. 7

J. Tomppa, *GDPR and Right to Erasure*, 10 October 2016

WALTER J.-P., *le droit à l'oubli, la perspective européenne,* in : GIANORA T., (édit) l*e droit à l'oubli : du mythe à la réalité*, CEDIDAC, Lausanne, 2015

WEBER R. H., *Realizing a New Global Cyberspace Framework, Normative Foundations and Guiding Principles*, Schulthess, Zurich Basel Geneva, 2014