Project Acronym:	**OPTIMIS**
Project Title:	**Optimised Infrastructure Services**
Project Number:	**257115**
Instrument:	**Integrated Project**
Thematic Priority:	**ICT-2009.1.2 – Internet of Services, Software and Virtualisation**

D7.2.1.1 – Cloud Legal Guidelines

Activity 7: *Business and Legal*

WP 7.2: *Legal Issues*

Due Date:		M6
Submission Date:		30/11/2010
Start Date of Project:		01/06/2010
Duration of Project:		36 months
Organisation Responsible for the Report:		Leibniz Universität Hannover
Version:		1.0
Status		Final
Author(s):	Benno Barnitzke	LUH
	Marcelo Corrales	LUH
	Andrew Donoghue	451G
	Prof. Nikolaus Forgó	LUH
	Andy Lawrence	451G
Reviewer(s)	Daniel Field	ATOS
	Csilla Zsigri	451G

Project co-funded by the European Commission within the Seventh Framework Programme		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission)	
RE	Restricted to a group specified by the consortium (including the Commission)	
CO	Confidential, only for members of the consortium (including the Commission)	

Version History

Version	Date	Comments, Changes, Status	Authors, contributors, reviewers
0.1	06/10/2010	Input from the 451group concerning Non-Legislated Data Centre Energy Initiatives	Andy Lawrence, Andrew Donoghue (451G)
0.2	08/10/2010	First draft of the Deliverable ready for internal review	Benno Barnitzke, Marcelo Corrales, Nikolaus Forgó (LUH)
0.3	31/10/2010	Second draft of the Deliverable ready for external review	Benno Barnitzke, Marcelo Corrales, (LUH) Andrew Donoghue (451G) , Nikolaus Forgó, (LUH)Andy Lawrence(451G)
0.4	18/11/2010	Final version of the Deliverable; included grey boxes for improved readability; ready for review by the European Commission	Benno Barnitzke, Marcelo Corrales, (LUH) Andrew Donoghue (451G) , Nikolaus Forgó, (LUH)Andy Lawrence(451G)
0.5	19/11/2010	Revision of the deliverable	Daniel Field (ATOS), Csilla Zsigri (451G)
1	29/11/2010	Overall format revision, TOC, header, references, etc	Malena Donato (ATOS)

Table of Contents

Index of Figures

Index of Tables

Glossary of Acronyms

Acronym	Definition
AAUs	Assigned Amount Units
BCS	British Computer Society
BHB	British Horserace Board
BREEAM	Building Research Establishment Environmental Assessment Method
CCA	Climate Change Agreement
CDM	Clean Development Mechanism
CER	Certified Emission Reduction
CO2	Carbon Oxide
CoC	Code of Conduct
CRC	Carbon Reduction Commitment
D	Deliverable
DCIE	Datacentre Infrastructure Efficiency
DEFRA	Department for Environment, Food and Rural Affairs
DRS	Document Review Sheet
EC	European Commission
ECJ	European Court of Justice
EPC	European Patent Convention
EPEAT	Electronic Product Environmental Assessment Tool
ErP	Energy related Products
EU	European Union
EU ETS	European Union Greenhouse Gas Emission Trading System
EuP	Energy using Products
Fit4Green	Federated IT for a sustainable environmental impact
GAMES	Green Active Management of Energy IT Service Centres
GeSI	Global e-Sustainability Initiative
GHG	Greenhouse Gas
ICT	Information and Communication Technology
IDE	Integrated Development Environment
INFOSOC Directive	Information Society Directive
IP	Infrastructure Provider
IPRs	Intellectual Property Rights
ISO	International Organisation for Standardisation
IT	Information Technology
JBCE	Japanese Business Council Europe
JI	Joint Implementation
LEED	Leadership in Energy & Environmental Design
NAP	National Allocation Plan

OPTIMIS	Optimised Infrastructure Services
OECD	Organisation for Economic Co-operation and Development
PAS	Publicly Available Standard
PDUs	Power Distribution Units
PM	Project Manager
PO	Project Officer
PUE	Power Usage Effectiveness
RECs	Renewable Energy Certificates
ROCs	Renewable Obligation Certificates
SDO	Service Deployment Optimiser
SLA	Service Level Agreement
SP	Service Provider
SP	Service Provider
SPEC	Standard Performance Evaluation Corporation
TRIPS	Agreement on trade-related aspects of intellectual property rights
UNFCCC	United Nations Framework Convention on Climate Change
UPS	Uninterruptible Power Supply
US EPA	United States Environmental Protection Agency
VM(s)	Virtual Machine(s)
WBCSD	World Business Council for Sustainable Development
WCT	WIPO Copyright Treaty
WIPO	World Intellectual Property Organisation
WIR	World Resource Institute
WP	Work Package
WTO	World Trade Organisation

1 Abstract

Our aim is on the one hand to ensure that no legal barriers are going to hinder the way of accomplishing the OPTIMIS project goals. On the other hand this paper gives guidance about legal issues of cloud computing as such.

In this Report, we focus on legal requirements relevant to OPTIMIS in order to achieve compliance of the project with European legislation and efface legal uncertainty. Without doubt, cloud computing raises particularly complex legal issues which can potentially put the overall goal of OPTIMIS at risk. However, this risk can be successfully mitigated if OPTIMIS is aware of these issues and implements compliant technical solutions.

We analyse the fields of law relevant to OPTIMIS, namely Data Protection and Data Security, Intellectual Property and Green Legislation and specify the legal requirements for the project. We follow a high level approach by assessing the legal problems at European level in order to ensure compliance across the various jurisdictions of the Member States.

As regards data protection, we find that the national law applicable depends on the location of the data centres and statutory seats of the cloud providers. Also, the role of data controllers in OPTIMIS is not fixed, but depends on the specific cloud scenario at stake.

There are many intellectual property issues concerning ownership and rights in information and services placed in the Cloud. In some cases it is easy to decide who owns the data but in some others it is difficult to separate between the rights of the owners and those of the service providers. We attempted to raise and answer some of these questions.

Concerning green legislation there are many legal and non-legal issues to take into consideration and compliance with these legal requirements together with de facto standards, metrics and industry initiatives is mandatory.

In conclusion, OPTIMIS should distinguish the stakeholders and clearly assign the level of influence on the processing of data in the Cloud. Clarifying intellectual property rights between all the stakeholders is very important for the outcome of the project and further exploitation of the end product. Compliance with Green legislation is mandatory not only for environmental reasons but rather for the socio-economic implications relevant for the project.

Keywords: Data Protection Directive 95/46/EC, data flow, applicable law, establishment, virtual machine, data centre, data controller, essential elements of the means, joint controllership, normative approach, intellectual property rights, copyrights, patents, trade secrets, database right, green legislation, data centre energy initiatives, carbon emissions (CO2).

2 Executive Summary

This Report, Cloud Legal Guidelines, deals with the intrinsic legal issues of cloud computing, in particular those issues specific to OPTIMIS. Its aim is to ensure that no legal barriers are going to hinder the way of accomplishing the OPTIMIS project goals.

The main problems of cloud computing occur in three main fields of law:

- Data Protection Law
- Intellectual Property Law
- Green Legislation

This is mainly the result of cloud computing characteristics, where data is provisioned dynamically which brings along a loss of control for personal data processed in the cloud (data protection law). Also, it is important to know which intellectual property assets are protected in OPTIMIS (intellectual property law). Finally, cloud computing involves the use of data centres with a considerable amount of energy consumption (green legislation).

Accordingly, this Report is subdivided into three main sections. We assess these fields of law from a high-level perspective by scrutinising the corresponding European legislation. This approach simplifies compliance within particular Member States as the national laws of the Member States are harmonised by this legislation. Where necessary, we provide advice on how to comply with particular provisions of a Directive or a Regulation.

Data Protection Law

Before assessing the legal issues related to OPTIMIS, it is important to understand the fundamental legal concepts laid down in the EU Data Protection Directive 95/46/EC. In order to provide a deeper understanding of these basic concepts and facilitate compliance with data protection regulations for OPTIMIS, we give an overview of the EU Data Protection Directive 95/46/EC and its guiding principles on the protection of personal data. It aims at the **protection of fundamental rights** and freedoms and "in particular" the "right to privacy with respect to the processing of personal data". The Directive defines personal data as "any information relating to an identified or identifiable natural person". Processing personal data is only legitimate where a data subject has given his unambiguous **consent** or by **legal allowance**. The **data controller** is the natural or legal person, who processes data and also **determines the purposes and means** of such processing. This may be contrasted with the data **processor**, who merely processes data **on behalf of the controller**.

Directive 2002/58/EC concerning the processing of personal data and the privacy in the electronic communications sector is applicable as well because cloud computing is considered a publicly available electronic communications service. Additionally, the Data Retention Directive 2006/24/EC is closely connected with this subject as it requires electronic communications services to retain specific categories of traffic data. Since this Directive adopts the definition of 'publicly available communications services' it is also applicable to cloud service providers.

Next, we analyse the data processing practices within OPTIMIS. This is carried out at a rather abstract level, as OPTIMIS only provides the toolkit and specification which support the con-

struction of multiple coexisting architectures to make up a cloud service ecosystem. We identify possible data flows and stakeholders in the different scenarios and use cases.

After that, we determine the national data protection law applicable. Here it is decisive where the establishments processing personal data are located. While Virtual Machines cannot be regarded as establishments, the location of the cloud computing data centres determine the national law applicable as well as the statutory seats of each SP and IP respectively of the service consumer.

Finally, we identify data controllers responsible for compliance with the Data Protection Directive within OPTIMIS according to the different scenarios: Federated Cloud Architecture, Multi-cloud Architecture (all OPTIMIS enabled), Multi-cloud Architecture (some OPTIMIS enabled), Hybrid Cloud Architecture.

- In the **Federated Cloud Scenario as defined in the Architecture Design Document 1.2.1.1**[1], the service consumer acts as a data controller since he takes the decision to start the initial data flow with regard to a specific purpose. Conversely, the SP does not have the authority to 'determine' the objectives of the processing as this has been already done by the service consumer. By contrast, albeit the initial IP selected by the SP does not determine the purposes, his influence on determining the means of the processing is considerably high as he exercises sole and full control over the federation and must be regarded as a data controller.
- The service consumer is again regarded as a data controller in the **multi-cloud scenario (all OPTIMIS enabled)**. As opposed to the federated cloud scenario, the SP has a significantly high influence because of the fact that he determines essential elements of the data processing. Thus, he can be deemed a data controller in this scenario. Conversely, IPs are unaware of each other which indicates a certain lack of control over the data processing.
- As in the multi-cloud scenario (all OPTIMIS enabled), the service consumer and SP are deemed data controllers in the **multi-cloud scenario (some OPTIMIS enabled)**, while this is not the case for IPs.
- While private cloud providers initiate a data flow and determine purposes and means of the processing, public IPs appear as their instrument to process personal data in the **hybrid cloud scenario**. Consequently, private cloud providers are considered data controllers, while public IPs cannot guarantee the rights conferred on data subjects. Hence, they are denied the status of a data controller.

Based on these findings, we can draw several conclusions:

The location of the Virtual Machines processing the data does not determine the national data protection law applicable. Rather, the statutory seat and the location of data centres are decisive

[1] OPTIMIS D1,2,1,1 Architecture Design Document, p. 15 et seq.

Ascertaining data controllers in OPTIMIS is challenging due to the normative approach of the definition of a data controller[2] which does not offer fixed conditions to qualify as a data controller. Thus, determining data controllers within OPTIMIS is an individual case decision and depends on the selected role in the different scenarios.

Therefore, OPTIMIS must clearly

- distinguish between different stakeholders
- define to what extent stakeholders determine the purposes and means of the data processing

Intellectual Property Law

Before assessing the intellectual property issues within OPTIMIS it is important to understand the key concepts of these rights and the scope of protection for such rights. It is also important to get a picture of the international and European framework. Therefore, this first analysis is based on finding out which of these rights might be relevant for the project. OPTIMIS relies on a very complex infrastructure and therefore needs to establish a relationship among a large number of stakeholders. Each of these stakeholders has different interests and therefore there are many questions concerning ownership and rights in information and services which need to be clarified. Most of the times this is straightforward but other times the complex infrastructure makes it very difficult. These are important issues for users so they can rely on the services provided in the Cloud. For this reason, we have provided for such a framework and we have answered the most important questions from a high level perspective indicating which directives and provisions need to be taken into account. At the end of this section we arrive to the conclusion that copyright protection of computer programs is certainly possible as long as there is a certain degree of originality in the creation of the computer program. The same is true for the adaptations of existing protected computer programs provided there is the necessary level of creativity involved. As far as the patentability of computer software concerns, this remains as a latent possibility if such program meets certain requirements such as a new technical contribution in the current state of the art while running the computer program.

Special attention is paid to the database right (also known as the "*sui generis*" right). Within Cloud computing, storage capabilities i.e. databases play an important role where the database right can represent a very important legal and economical tool to recoup the investment. The *sui generis* right in a Cloud computing environment is very difficult to achieve but not impossible. This situation needs to be analysed in a case by case basis as it is arguable whether Cloud computing databases fall under the scope of the Database Directive. One could argue that such collection of data does not constitute a substantial investment in the obtaining of the contents of that database since the data will be collected automatically by the OPTIMIS risk assessment components. Clarifying these rights will therefore provide the owner of the databases the necessary legal protection for any future exploitation.

[22] The definition of 'data controller' is provided in Art. 2 lit. d) Directive 95/46/EC. For more details how to construe this provision see Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf

Green Legislation

Eco-efficiency is increasingly becoming of paramount importance for the success of businesses. The increase of energy prices, the shortage of energy power and the high consumption of electricity of companies which provide IT services is costing them a great deal of money. In addition, they are under social, business and stakeholder pressure to reduce carbon emissions which is strongly associated with energy use. They may also, under present or future legislation, or in customer procurement documents, have to report IT related energy use and carbon emissions. There are a number of legal provisions starting from international treaties such as the Kyoto Protocol to domestic green legislation of EU Member States which need to be taken into consideration. A good example to analyse this situation is the recent UK legislation in regards to its Carbon Reduction Commitment (CRC) which could be spread all over Europe. There are also different non-legally binding documents which suggest a change in the legislation adding strict measures to different stakeholders in a Cloud computing ecosystem. Therefore, we provide the international and European framework relevant to OPTIMIS together with a comprehensive list of de facto standards e.g. PUE (Power Usage Effectiveness), GHG (Greenhouse Gas) Protocol, LEED (Leadership in Energy and Environmental Design), BREEAM (Building Research Establishment Environmental Assessment Method), etc. which even though they may not have a heavy impact on the legislation, they still might influence the legislation over the forthcoming years. Nevertheless, these standards, metrics and industry initiatives could and should be adopted in Cloud computing and in particular in OPTIMIS as we suggest along the green legislation part.

3 Introduction

As the OPTIMIS project is a trailblazer with regard to a holistic cloud computing approach, it is paramount to take into account legal rules for the architecture design as a whole. To cope with these risks, we will give legal guidance to ensure that no legal barriers are going to hinder the way of the OPTIMIS project goals. Cloud computing involves a variety of legal problems, ranging from Data Protection and Data Security over Intellectual Property to Green Legislation. Despite being a relatively new phenomenon, cloud computing does not exclusively raise new legal questions. It also entails questions which are already known, but have not yet been discussed or even resolved in the context of cloud computing. Assessing these issues is a challenge as there is still almost no legal guidance from authorities (for instance Data Protection authorities) due to the novelty of the cloud model, not to mention the absence of court decisions.

The Report is structured in three parts. The first part deals with Data Protection and Data Security issues. The second part addresses the most relevant intellectual property rights which need to be taken into account during the course of the project and the third part deals with green legislation.

In the section about data protection (section 4.3), we mainly deal with identifying the various stakeholders and data flows, determine the national law applicable and scrutinise the data controllers within the different scenarios (Federated Cloud, Multi-Cloud (all OPTIMIS), Multi-Cloud (some OPTIMIS) and Hybrid Cloud Architecture).

In the section about intellectual property (section 4.4), we provide an overview of the international and European framework in the realm of intellectual property rights. Our main focus is to make an assessment of the main intellectual property issues which need special attention for the software development process. Special attention is made to copyright and database protection which is answered in the light of the European directives and the most relevant European Court of Justice decisions.

In the section about green legislation (section 4.5), we analyse the main international treaties and agreements which influences the current European and Member States' green legislation. We provide an overview of different legally binding documents as well as other so called "soft law" such as resolutions, recommendations and code of conducts relevant to take into account during the course of the project. We also provide a comprehensive description of the de facto standards, metrics and industry initiatives which in most cases do not have any direct legal weight. However, this may change in the coming decade as legislation spreads.

For purposes of improved readability and understanding the sometimes complex legal questions, we inserted grey textboxes into the Report to enable the reader to quickly get the essential information needed. The grey boxes contain the main results from the sections above concerning a specific legal problem. They are mainly addressed at consortium and project management members. The reader should derive the legal requirements for OPTIMIS from these boxes. The requirements are indicated by a heading "What OPTIMIS needs to do". Finally, we show the result of being compliant. Where applicable, we also take into account what non-compliance would result in. However, for a detailed overview and for a deeper understanding of the issues, we suggest to read the whole report.

This is the first release of D7.2.1.1 Cloud Legal Guidelines. It will be updated on a six-monthly basis with input on previously unexamined issues or topics.

4 Legal requirements

4.1 Characteristics of Cloud Computing and consequential legal implications

The reason why cloud computing involves the three aforementioned fields of law (data protection, intellectual property, green legislation) is mainly to do with its typical features. Usually, cloud computing has the following characteristics[3] which trigger consequential legal questions:

- the infrastructure used to store and process a customer's data is shared with other customers (multi-tenancy)
- the supplier's servers are located in several jurisdictions
- data is transferred from one location to another depending on where resources are available
- the cloud service provider decides the location of the data, the service standards and the security standards instead of the customer
- no dedicated, but dynamically provisioned IT resources

➔ **Data Protection Law**

- software, data and databases can easily and in an uncontrolled way be reproduced on Virtual Machines (VMs) running in the cloud
- easy access of users to information anywhere in the world due to "location-less" services

➔ **Intellectual Property Law**

- data centres providing the cloud computing infrastructure have high energy consumption

➔ **Green Legislation**

The benefits of cloud computing characteristics for both businesses and individuals are clear[4], but it is necessary that data protection and data security are embedded within the entire life-

[3] See OPTIMIS D1.2.1.1 Architecture Design Document for detailed explanation of the OPTIMIS Architecture; see also Cloud Computing: The Key Issues and Solutions, available at http://www.ffw.com/publications/all/articles/cloud-computing.aspx.

[4] See Opinion of 18 March 2010 of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, No. 12, available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf.

cycle of the cloud computing architecture from the early design stage to deployment, operation and ultimate disposal. This is usually referred to as "privacy by design"[5].

The data protection issues have mainly to do with the question whether moving data into the cloud is compliant to national data protection law. Another major concern is that cloud computing is a relatively complex data processing structure and involves many different stakeholders in different jurisdictions.

Regarding intellectual property concerns, the major concern lies in establishing ownership and rights in information and services which are place anywhere in the Cloud. These are important issues to clarify between all the stakeholders.

As far as green legislation is concerned,, compliance with legal and other requirements is also mandatory not only for environmental reasons but for cost-efficiency.

4.2 Data Protection within the European Union

With the advent of global, large-scale networks and the facility to transfer data within seconds, data protection legislation has to cope with new challenges concerning global distribution of data and the protection of the data subjects' fundamental right to privacy. Increases in processing power as well as in storage capacity and Internet bandwidth allow more information to be collected at low cost, making it considerably easier to process and transmit personal data[6]. Besides, globalized networks such as the Internet and technologies making use of it (i.e. cloud computing) entail massive data flows within as well as outside the European Union.

While the IT industries are working at the cutting edge of computer technology, important parts of data protection legislation in the European Union date from the year 1995[7]. Thus, seen from a technological perspective, this legislation seems light years behind schedule. Certainly, emerging innovative technologies give rise to new legal questions to which current data protection legislation might not have yet found answers, but since the Data Protection Directive has been created in a technology-neutral way[8], even new developments can be handled by the Directive.

Before assessing the legal issues related to OPTIMIS, it is important to understand the fundamental legal concepts laid down in the EU Data Protection Directive 95/46/EC. In order to provide a deeper understanding of these basic concepts and facilitate compliance with data protection regulations for OPTIMIS, we give an overview of the EU Data Protection Directive

[5] See Opinion of 18 March 2010 of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, No. 12, available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf.

[6] See Brown, Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, Working Paper No. 1: The Challenges to European Data Protection Laws and Principles, Oxford 2010, p. 2, available at: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_1_en.pdf; Recital 4 Directive 95/46/EC.

[7] With regard to the genesis of Directive 95/46/EC see Simitis, From The Market to the Polis: The EU Directive on the Protection of Personal Data, 80 Iowa L. Rev. 445 (1995), p. 445 et seqq.

[8] See for example the Definition in Art. 2 lit. b) DPD, where it is of no importance whether or not data is being processed by automatic means. Furthermore, the definition does not distinguish between specific operations falling into the scope of the DPD. Rather, "any operation or set of operations which is performed upon personal data" is comprised by the wording.

95/46/EC and its guiding principles on the protection of personal data. After addressing the aim and scope of the Directive, we briefly deal with the national law applicable and criteria for making data processing legitimate. Furthermore, we explain the concept of a data controller and its interaction with the concept of a data processor. Additionally, we describe the duties of the data controller and the corresponding rights of the data subject in a few words. A description of transfers of personal data within the EU and to third party countries concludes this section.

4.2.1 Art. 8 Charter of Fundamental Rights of the European Union

On 7 December 2000, at the European Council meeting in Nice, the Charter of Fundamental Rights was signed and "solemnly proclaimed" by the European Commission, Parliament and Council. It is a written catalogue of fundamental rights in primary Community law. Though not legally binding at the time of adoption[9], the Charter is now incorporated in primary European Community law pursuant to Art. 6 of the Treaty on European Union by entry into force of the Treaty of Lisbon on 1 December 2009.

Established within Title II ("Freedoms") of the Charter, Art. 8 bears the heading "Protection of personal data". According to this article, everyone has the right to the protection of personal data. The right includes that data must be processed fairly for specified purposes and on the basis of either the consent of the person concerned or another legitimate basis laid down by law. In addition, the person concerned has the right of access to the collected data and to rectify incorrect data. An independent authority shall control compliance with the aforementioned rules. The insertion of such a right into primary European Law expresses a growing social concern to protect individual privacy against new technologies[10]. Respecting this right by incorporating it into EU primary law does not only mean the European Union recognises that the use of novel technologies can pose threats to the privacy of individuals, but that it needs to be protected in a more profound way. Thus, the protection of personal data has been granted fundamental right status.

Since the European Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data shall, protects the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, one has to look at all its provisions in the light of the Charter of Fundamental Rights which in the first place establishes such a right. While Art. 8 of the Charter outlines the rules governing lawful processing of personal data, the Data Protection Directive renders more precisely the conditions which have to be met in order to process personal data legitimately. Consequently, data protection within the OPTIMIS project is not mere, onerous compliance with the Data Protection Directive, but in fact entails the protection of fundamental rights of any person whose data is being processed in the cloud.

[9] See Calliess, in: Ehlers, European Fundamental Rights and Freedoms, Berlin 2007, § 20 margin no.34 et seqq.

[10] Bercusson, European Labour Law and the EU Charter of Fundamental Rights, 1st Edition, Baden-Baden 2006.

4.2.2 Art. 16 Treaty on the Functioning of the European Union

Art. 16 Treaty on the Functioning of the European Union (TFEU) has been inserted into Title II of the TFEU which reads "Provisions Having General Application". According to this article, "everyone has the right to the protection of personal data concerning them." Obviously, the wording of Art. 16 sub. (1) TFEU is identical to Art. 8 sub. (1) Charter of Fundamental Rights. It covers all areas of EU law and is designed to be the cornerstone of data protection within the EU. As follows from the text of Title II of the TFEU, Art. 16 applies to all processing in the private and public sector[11].

4.2.3 The Concept of Data Protection According to Directive 95/46/EC

The legal framework for the processing of personal data is regulated in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as "Data Protection Directive").

4.2.3.1 Genesis

The European Parliament dealt with the protection of personal data remarkably early. In March 1975, it demanded a regulation for processing of personal data in order to protect the fundamental rights of individuals in the intensifying European data flows[12]. It was not until 1990 that the commission responded and offered a first proposal for a Directive. After several amendments, the final version of the Directive came into force on 24.10.1995.

4.2.3.2 Aim and scope of the Directive, Artt. 1 and 3 Data Protection Directive

According to Art. 1 of the Directive it is clear that one of the main aims is the **protection of fundamental rights** and freedoms and "in particular" the "right to privacy with respect to the processing of personal data"[13]. Recital 10 of the Directive explicitly emphasises this aspect and refers to Art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, which protects the right of everyone to respect for his private life[14]. In addition, the Directive shall ensure the "**free flow of personal data between Member States**". Member States may therefore no longer inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals[15]. It is obvious that the first aim of the Directive is at certain conflict with the second objective. While the first one points to the protection of fundamental rights, the second stresses economical interests relating to personal data. Both objectives have to be balanced to such an extent that the free flow of data is realised by applying the data protection provisions[16].

The Directive deals with the processing of personal data. Personal data is defined in Art. 2 lit. d) Data Protection Directive as "**any information relating to an identified or identifiable natu-**

[11] Hijmans/Scirocco, Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty Be Expected to Help?, 46 CML Rev. 2009, p. 1485, 1515.

[12] Kühling/Seidel/Sivridis, Datenschutzrecht, Frankfurt am Main 2008, p. 47.

[13] Korff, EC Study on Implementation of Data Protection Directive, Cambridge 2002, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf.

[14] Convention for the Protection of Human Rights and Fundamental Freedoms of Rome, 11/4/1950.

[15] See Recital 10 Data Protection Directive.

[16] See Dammann/Simitis, EG-Datenschutzrichtlinie, Baden-Baden 1997, Einleitung margin no. 9.

ral person". The term does not comprise data of legal persons, as only natural persons are covered by the Directive[17]. Although the Directive adopted a broad concept of personal data, the scope of the data protection rules should not be overstretched. However, at the same time, unduly restricting the interpretation of the concept of personal data should also be avoided[18]. To determine whether a person is identifiable, account should be taken of all the means likely and reasonably to be used by either the controller or by any other person to identify the said person[19]. The definition of "personal data" is as general as possible so as to include all information concerning an identifiable individual[20].

As opposed to anonymous data, personal data are any information relating to persons who can be identified with reasonable effort[21] by perceiving this information. In contrast, anonymous data are data where the data subject can only be identified with an unreasonable amount of costs, capacities and time. However, the Data Protection Directive does not comprise a definition of this "depersonalised data". Still, the provision shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable[22]. Whether or not a natural person is identifiable is highly debated in cases like Google Street View, where some argue that facades constitute personal data[23]. In any event, if a person can be identified by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (i.e. telephone number, social security number, passport number, banking account number, age, occupation, place of residence etc.), the Directive's data protection rules apply.

The Data Protection Directive applies to the **processing** of personal data. According to Art. 2 lit. b) Data Protection Directive, processing shall mean **any operation** or set of operations which is **performed upon personal data**. This definition is likewise an extensive one as it covers everything from the collection to the erasure of data, including retrieval, storage, use, disclosure, dissemination and destruction etc. of personal data[24]. The Directive protects all personal data regardless of the form in which they are available. It includes information stored in a computer memory by means of binary code as well as information contained in an electronic document such as an e-mail[25]. This is a consequence of covering processing of personal data "by automatic means" pursuant to Art. 3 Data Protection Directive. Addressee of the Data Protection Directive is the **"controller".** This is the body which **determines the purposes and means of**

[17] Nevertheless, pursuant to Recital 24, this does not prevent Member States from implementing rules concerning the protection of legal persons as well. Austria has made use of this possibility, see, § 4 No. 3 Datenschutzgesetz 2000 (BGBl. I Nr. 165/1999, amended by BGBl. I Nr. 133/2009).

[18] Art. 29 Working Party, WP 136, Opinion 4/2007 on the concept of personal data, p. 4, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

[19] See Recital 26 Data Protection Directive.

[20] COM (92) 422 final, p. 8; Art. 29 Working Party, WP 136, Opinion 4/2007 on the concept of personal data, p. 4, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

[21] Recital 26 Data Protection Directive.

[22] Art. 29 Working Party, WP 136, Opinion 4/2007 on the concept of personal data, p. 4, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

[23] See Forgó/Krügel, MMR 2010, 17 et seqq. and Forgó, MMR 2010, 217 for further information.

[24] COM (92) 422 final, p. 9.

[25] Art. 29 Working Party, WP 136, Opinion 4/2007 on the concept of personal data, p. 4, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

the processing of personal data (Art. 2 lit.d) Data Protection Directive) and can either be a natural or a legal person. The controller is ultimately responsible for the choices governing the design and operation of the processing carried out, rather than anyone who carries out processing in accordance with the controller's instructions[26].

According to Art. 3 sub. (2), the Data Protection Directive does not apply in certain cases. If the data processing is performed by a natural person in the course of a purely personal or household activity, the data protection provisions are not applicable[27], Art. 3 sub (2) first indent. The same applies to an activity which falls outside the scope of European Union law, Art. 3 sub. (2) second indent[28].

4.2.3.3 National law applicable, Art. 4 Data Protection Directive

Art. 4 Data Protection Directive provides the legal basis for the determination of the national law which is applicable to processing. The law applicable according to Art. 4 sub. 1 lit. a) Data Protection Directive is defined by the reference to the place of establishment of the data controller[29]. If a controller is not established within the European Union but makes use of equipment situated on the territory of a Member State, then the law of this Member State is applicable. It will be one of the challenges within OPTIMIS to determine what constitutes an establishment.

4.2.3.4 Criteria for making data processing legitimate, Artt. 6 and 7 Data Protection Directive

The Data Protection Directive foresees in Sections I and II criteria for legitimate processing of personal data. While Art. 6 deals with basic principles concerning lawful processing of personal data, Art. 7 Data Protection Directive substantiates these principles and provides for an exhaustive list of the various circumstances in which processing may be carried out.

According to Art. 6 lit. a) Data Protection Directive, personal data must always be processed **fairly and lawfully**, meaning that the concealed collection of personal data without the knowledge of the data subject is excluded[30]. Art. 6 lit. b) Data Protection Directive determines that personal data may only be processed according to **specified purposes**. The latter must be explicit and legitimate and has to be determined at the time of collection of data[31]. Additionally, the processing of personal data must be **adequate, relevant and not excessive** in relation to the previously specified purposes (Art. 6 lit. c) Data Protection Directive). Art. 6 lit. e) Data Protection Directive ensures that personal data is **kept for no longer than is necessary** for the purposes the data were initially collected.

---

[26] COM (92) 422 final, p. 9.

[27] See also Recital 12 clause 2 Data Protection Directive.

[28] Note: the actual wording of Art. 3 sub. (2) second indent speaks of "an activity which falls outside the scope of Community law". However, with entry into force of the Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community of 13th December 2007 on the 1st December 2009, the terminology of the wording would have to be adapted to "an activity which falls outside the scope of European Union law". See for further details Hijmans/Scirocco, supra note 11, p. 1485, 1515 et seqq.; *Zerdick*, "Folgerungen aus der Vergemeinschaftung der Justiz- und Innenpolitik für den Datenschutz", available at: http://www.datenschutz.hessen.de/download.php?download_ID=187.

[29] COM (92) 422 final, p. 13.

[30] See COM (92) 422 final, p. 15.

[31] Recital 28 clause 2 and 3 Data Protection Directive.

Art. 7 Data Protection Directive sets out the specific rules under which processing is allowed. It is the central provision for the legitimacy of processing personal data. Generally speaking, there are two possibilities for making data processing legitimate: either by the data subject's unambiguous **consent** or by **legal allowance**. The data subject's consent is defined in Art. 2 lit. h) Data Protection Directive as any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. This is a rather strict definition and requires that the data subject is clearly informed in advance of what he is consenting to[32]. Subsequently, consent must be **informed consent**, meaning that the controller has to make available the necessary information to the data subject in order to ensure the consent is "freely given" and results in the data subject's "informed indication of his wishes". Consent may either be given oral or in writing[33]. In electronic environments, consent may also be given in electronic form[34]. In case there is no consent, processing may still be legitimate because of a legal allowance according to Art. 7 Sec. b) to f) Data Protection Directive. Legal allowance always requires the processing to be "necessary" to achieve legitimacy. Where, for example, a contract could reasonably be performed in some other way without the need for processing, such processing is not necessary[35]. Consequently, if there are less severe measures and personal data is not required for certain activities, personal data may not be processed. Art. 7 b) Data Protection Directive allows processing of personal data if it is necessary for the contract to which the data subject is party. Art. 7 lit. d) Data Protection Directive considers legal obligations to which the controller is subject. Processing is therefore necessary if the controller has to comply with an obligation imposed by national or Community law[36]. Art. 7 lit. f) Data Protection Directive establishes a rule of balance of interests between the data subject and the controller or third parties to which the data are disclosed, taking into account the fact that there may be legitimate interests at stake other than those of the controller and of the data subject[37].

4.2.3.5 The concept of data controller and its interaction with the concept of data processor, Artt. 16 and 17 Data Protection Directive

The classification of an actor as a controller or a processor can sometimes be exceedingly difficult. Unfortunately, the Data Protection Directive does not give much guidance in determining when a body can be considered a data controller or a data processor[38]. Essentially, a **data controller** is the natural or legal person which **determines the purposes and means** of the processing of personal data (Art. 2 lit. d) Data Protection Directive), while a **processor** is any natural or legal person which processes personal data **on behalf of the controller** (Art. 2 lit. d) and e) Data Protection Directive). Thus, instead of processing personal data within its organisation, a data controller may employ another natural or legal person with processing. However, the

[32] *Kuner*, European Data Protection Law – Corporate Compliance and Regulation, 2nd Edition, New York 2007, margin no. 2.14.

[33] See COM (92) 422 final, p. 11.

[34] *Ehmann/Helfrich*, EG- Datenschutzrichtlinie, Kurzkommentar, Köln 1999 Art. 7 marg. no. 9.

[35] See *Carey*, Data Protection – A Practical Guide to UK and EU Law, New York 2009, p. 68.

[36] COM (92) 422 final, p. 17.

[37] COM (92) 422 final, p. 17.

[38] Apparently, the same applies to national data protection laws as well, see *Kuner, supra note 32,* margin no. 2.21.

data controller remains responsible while the processor performs the processing of personal data[39]. In other words, a processor is essentially an agent of the controller[40].

Despite the definitions given in the Directive, it is complex to examine whether or not a particular entity "determines the purposes and means of the processing of personal data" since these terms have not been defined in the Directive at all. However, it is vital to distinguish between the role of a controller and a data processor as it has important consequences in certain areas:

- The controller is the body which shall be responsible for compliance with data protection law. Most of the provisions laid down in the Data Protection Directive must be met by him (see for example Art. 6 sub. (2), Art. 7, Art. 10, Art. 11, Art. 12 Data Protection Directive)[41]. Even if it is not clearly expressed, all provisions setting conditions for lawful processing are addressed to the controller, as it is the controller who has to comply with the general principles laid down in Art. 6 sub (1) Data Protection Directive.
- Data controllers rather than data processors are liable for data protection violations, Art. 23 Data Protection Directive.
- Data processors are supposed to process data according to the mandate and the instructions given by the controller, Art. 16 Data Protection Directive.

In a nutshell, the concepts of controller and processor are first and foremost about allocating responsibility[42]. Accordingly, the role of a controller determines the entity to which the data subject can turn to in order to exercise his rights.

The Art. 29 Working Party has emphasised two basic conditions for qualifying as a processor according to the definition in Art. 2 lit. e) Data Protection Directive. The first condition is that the processor be a **separate legal entity** with respect to the controller. The second condition is that he processes the data **on behalf of the controller**. Acting on behalf means serving someone else's interest. In the context of data protection law, processing on behalf of the controller requires the processor to implement the instructions given by the controller with regard to the purpose and the essential elements of the means of processing[43]. The Art. 29 Working Party also emphasises that it depends on the **concrete activities in a specific context** whether an

[39] However, this does not prevent Member states from implementing in its national data protection law provisions which foresee additional liability of a processor in certain cases, see Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 28, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[40] Korff, Comparative Study on Different Approaches to New Privacy Challenges, Particular in the Light of Technological Developments, Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments, London 2010, p. 61, available at: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf.

[41] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 4, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf; *Kuner, supra note 32,* margin no. 2.20.

[42] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 4, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf; see also Recital 25 Data Protection Directive.

[43] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 25, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

entity acts as a processor[44]. If the processing entity plays a relevant role in determining the purposes or the essential means of processing, it is a controller rather than a processor. The same applies if the processor exceeds the scope of his assigned duties and acquires a role in which he determines the purposes and means of the processing of personal data.

In order to distinguish data controllers from data processors it is helpful to establish reliable criteria on which grounds the two can be discerned. The Data Protection Directive contains two provisions which are specifically addressed to the processor and which define his obligations with regard to the processing of personal data. These provisions help in distinguishing between entities acting as a data controller and those acting as a data processor. According to **Art. 16 Data Protection Directive**, any person acting under the authority of the controller, including the processor, who has access to personal data must not process them except on instructions from the controller. **Art. 17 Data Protection Directive** requires a contract or a binding legal act regulating the relations between data controller and data processor. The contract shall be in writing for the purposes of keeping proof. The minimum content which has to be contained in the contract must stipulate that the processor shall only act on instructions from the controller and implement appropriate technical and organisational measures to protect personal data. The contract should include a detailed enough description of the mandate of the processor[45]. We can therefore summarise the following criteria determining whether an entity acts as a data controller or a data processor:

- A data processor acts **under the authority of a data controller**[46]. Therefore, a processor is always a subordinate entity in relation to the controller and has to process personal data consistent with the instructions given by the controller. It depends on the **level of prior instructions** given by the data controller which determines the level of independence of the processing entity and the scope of action left to him[47]. The more restrictive the instructions given by a data controller, the more likely it is that the processing entity acts on behalf of the data controller and therefore qualifies as a data processor.
- **Monitoring** by the data controller of the execution of the data processing performed by another entity also indicates contract data processing. Constant supervision by the controller to ensure compliance with instructions and terms of the data processing contract shows that the controller is in full and sole control of the processing operations[48].
- The **image**, respectively the **appearance** of the data processing entity and the related expectations of the data subjects on the basis of this image/appearance may also de-

[44] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 25, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[45] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 26, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[46] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 25, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf; see COM (1992) 422 final, p. 34.

[47] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 28, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[48] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 28, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

termine the roles of a data processor or a data controller[49]. If the separate natural or legal person processing the personal data presents itself using the name of another natural or legal person when collecting personal data from the data subject, this indicates contract data processing.

- The **expertise** of the involved parties may also entail the qualification as data controller or data processor. In some cases, the professional expertise of a service provider could therefore lead to a qualification as a data controller.
- Additionally, the **means** put in place to reach the purposes may determine the relevant roles. The entity which determines the means is usually considered the data controller, see Art. 2 lit. d) Data Protection Directive.
- A written **contract**[50] between the service provider and the entity for which it processes the data could also suggest that the service provider be a processor. Nevertheless, the mere fact of a written contract between the parties does not automatically mean the existence of a controller-processor relationship. Although a contract may help in understanding the relationship between the parties involved, it is neither constitutive nor decisive[51].
- As **new means** of processing entail specific privacy risks, this may lead to favouring the qualification as a data controller rather than data processor[52].
- The controller still needs to exercise full and sole control at any time while the data processing takes place. While it is not necessary that the controller controls and agrees on all the details of the means, it would still be necessary that he is at least **informed about the main elements of the processing structure**[53]. If the exertion of control by the data controller cannot be ensured due to technical or other reasons, the processing entity may itself be considered a data controller.

As a legal consequence, a data processor is part of the data controller when processing personal data. The **data processor** is **legally privileged**: Any disclosure of personal data to the data controller by the processor is not considered a transmission and therefore does not require legal allowance or the data subject's consent. Since the processor acts "on behalf of the controller" it is as if the controller were itself processing the data. As opposed to third parties, processors transferring data to and receiving data from controllers are in principle no new controllers[54]. Rather they are **part of the data controller**, while Artt. 7 and 8 Data Protection

[49] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 28, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[50] Or a contract in another equivalent form, see Art. 17 sub (4) Data Protection Directive.

[51] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 26 et seq., available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf

[52] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 29, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[53] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 27 et seq., available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf

[54] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 31, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

Directive are not applicable for the data flow between controller and his processor(s)[55]. Thus, the Data Protection Directive treats a processor as if it were identical to the controller and data flow between them does not require additional legal basis. However, it is still the **controller** being **responsible** for the whole data processing as the Data Protection Directive imposes all obligations on the data controller, see Art. 6 sub (2) Data Protection Directive. The processor must not process the data except on the instructions from the controller and is therefore **bound to** these **instructions**[56]. If the processor exceeds its mandate, he might himself be considered a data controller, and the transfer or reception of data to or from the data controller would be rendered unlawful.

4.2.3.6 Third parties, Art. 2 lit. f) Data Protection Directive

Third parties are defined as "any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data". While the term "third party" refers to any subject which is not part of an agreement or an entity in civil law, it has – to some extent – a different meaning in the context of the Data Protection Directive. A third party is any subject who has **no specific legitimacy or authorisation** to process personal data as it is **not involved in the controller-to-data-subject relationship**[57].

Legal consequence of a subject being a third party is that data flows to third parties require either legal allowance or consent. Hence, third parties are usually new data controllers if personal data is being revealed or disclosed to them.

Companies possessing legal personality are considered to be "third parties" even if they should belong to the same group. This is due to the fact that the Data Protection Directive does **not provide for** a "**group privilege**", where a group of companies would be considered as one and the same controller[58]. Therefore, disclosure of personal data to companies within a group ("intra-group transfers"[59]) requires legal basis according to Artt. 7 and 8 Data Protection Directive.

4.2.3.7 Obligations of the data controller and rights of the data subject

The obligations in the Data Protection Directive are imposed on the data controller. He has to ensure the compliance with the provisions laid down in the Directive. Apart from the principles of legitimate processing of data laid down in Artt. 6 and 7 Data Protection Directive, the data controller has several more specific obligations:

- The data controller has to provide a data subject from whom data relating to himself are collected with specific information, Art. 10 Data Protection Directive.
- This applies as well where the data have not been obtained from the data subject, Art. 11 Data Protection Directive.

[55] Kotschy, in: Büllesbach/Poullet/Prins, Concise European IT Law, New York 2006, Directive 95/46/EC, Art. 2 note 6 et seq.

[56] However, the processor might still have room for manoueuvre.

[57] See Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 31, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[58] Kotschy, in: Büllesbach/Poullet/Prins, supra note 55, Art. 2 note 7, who falsely calls it "company privilege"; Kuner, supra note 32, margin no. 2.101.

[59] Helbing, How the New EU Rules on Data Export Affect Companies in and Outside the EU, http://www.thomashelbing.com/en/how-new-eu-rules-data-export-affect-companies-and-outside-eu.

- The controller must implement appropriate technical and organisational measures according to Art. 17 sub. (1) Data Protection Directive to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access etc.
- The data controller has to notify the supervision authority before carrying out automatic data processing, Art. 18 Data Protection Directive.
- The controller has to provide for prior checks by the supervisory authority, according to Art. 20 Data Protection Directive.
- The controller can be held liable for any damage suffered resulting from unlawful data processing, Art. 23 Data Protection Directive.

Conversely, the data subject can exercise the rights deriving from the Data Protection Directive provisions:

- The data subject can give his unambiguous consent for making data processing lawful[60].
- The data subject has a right of access to data and may obtain from the controller especially confirmation as to whether or not data relating to him are being processed, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed, Art. 12 Data Protection Directive.
- The data subject has a right to object to the processing in certain cases, Art. 14 Data Protection Directive.

These obligations of the data controller ensure that data will be processed in a way which protects the fundamental rights of the data subject.

4.2.3.8 Transfer of personal data within the EU and to third countries, Art. 25 Data Protection Directive

International data transfers are subject to certain restrictions. As a general rule, international transfer of data is only allowed within the EU, whereas data transfers outside the EU are subject to certain restrictions to be observed by the data controller.

4.2.3.8.1 Transfer of personal data within the EU, Art. 1 sub. (2) Data Protection Directive

According to Art. 1 sub. (2) Data Protection Directive, Member States shall neither restrict nor prohibit the free flow of personal data between Member States. Here, the principle of **free flow of data within the EU**, respectively the European Economic Area (EEA), is realised. This means that a Member State may not impose legal restrictions on data transfers to another Member State for reasons of the level of data protection in such Member State[61]. Since the Directive provides for the same protection in every Member State, the level of protection is equivalent throughout the European Union[62]. This way the Data Protection Directive estab-

[60] Note, however, that missing consent can be compensated by legal allowance from the Data Protection Directive.

[61] Kuner, supra note 32, margin no. 2.68.

[62] COM (1992) 422 final, p. 9.

lishes the internal market according to Art. 26 of the Treaty on the Functioning of the European Union (ex-Art. 14 Treat Establishing the European Community, TEU)[63].

However, since Art. 6 Data Protection Directive requires personal data be processed fairly and lawfully and Art. 7 Data Protection Directive states that either consent or legal allowance for processing is needed, transfer of data within the EU (respectively the EEC) is not generally permitted. As long as the requirements for transfers within the EU implemented by the Member States are non-discriminatory, such restrictions are covered by the Data Protection Directive[64]. Art. 1 sub. (2) Data Protection Directive only ensures that Member States cannot prohibit transfer of personal data within the EU (EEC) on grounds of an inadequate level of protection[65].

4.2.3.8.2 Transfer of personal data to third countries, Artt. 25 and 26 Data Protection Directive

International transfers of personal data outside the EU (and the EEC) are governed by Chapter IV Data Protection Directive. Art. 25 Data Protection Directive establishes the principle that transfer of personal data may only take place if the third country ensures an **adequate level of protection**. At the time of the preparation of these Guidelines, the Commission has so far recognised

- Switzerland
- Canada
- Argentina
- Guernsey
- Isle of Man
- the US Department of Commerce's Safe harbor Privacy Principles, and
- the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection

as providing adequate protection[66]. A transfer of personal data to other countries and any data transferred to the US outside the scope of either Safe Harbor Principles or Passenger Name Record Agreement is basically prohibited, see Art. 25 sub. (1) Data Protection Directive.

[63] See Heil, in: Büllesbach/Poullet/Prins, supra note 55, Art. 1 note 3.

[64] Kuner, supra note 32, margin no. 2.69.

[65] Kuner, supra note 32, margin no. 2.69 and margin no. 4.03; Heil, in: Büllesbach/Poullet/Prins, supra note 55, Art. 1 note 3.

[66] http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm; Kuner, supra note 32, margin no. 4.48 et seq.; the Art. 29 Working Party has recently published WP 177, Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp177_en.pdf, where it finds that the Eastern Republic of Uruguay ensures an adequate level of protection within the meaning of Art. 25 Data Protection Directive. It is not unlikely that the European Commission follows this opinion.

4.2.3.8.3 Legal grounds for data transfer in third countries without an adequate level of protection

Although transfer of personal data to third countries is not allowed if the country in question does not ensure an adequate level of protection, this does not mean there is no possibility to disclose personal data to third countries. Several instruments enable controllers to transfer personal data to third countries despite that they do not ensure an adequate level of protection.

- **Data Subjects's consent**

  The Data Subject's **unambiguous consent** renders a transfer of personal data lawful. This requires a freely given, specific, clear and unambiguous indication of the data subject's wishes, which excludes implied consent[67].

- **"Safe Harbor" Principles (US only)**

  The United States of America is not considered to be a third country with an adequate level of protection. Nevertheless, organisations may take part in the US "Safe Harbor" programme[68]. The "Safe harbor" principles are privacy principles issued by the US Department of Commerce which are considered to provide an adequate level of protection by virtue of a decision of the European Commission pursuant to Art. 25 sub (6) Data Protection Directive[69]. Under the "safe harbor", US companies can voluntarily adhere to a set of data protection principles which have been deemed by the Commission to provide adequate protection with regard to transfers of data out of the EU.

  It enables organisations to sign up for safe harbor and thereby demonstrate their **compliance with** the provisions of the **EU Data Protection Directive by performing a self-certification procedure**. Transfer of personal data to a controller within the US, which would otherwise be illegitimate, is allowed if the controller joins the Safe Harbor list[70].

- **EU Standard Contractual Clauses**

  According to Art. 26 sub. (2) Data Protection Directive, adequate safeguards put in place by the recipient may authorise a transfer or a set of transfers of personal data to a third country. Such "safeguards may in particular result from appropriate contractual clauses." Furthermore, Art. 26 sub. (4) Data Protection Directive provides that the

---

[67] Art. 29 Working Party, WP 114, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, p. 10, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf.

[68] http://www.export.gov/safeharbor/.

[69] 2000/520/EC, Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25.8.2000, pp. 7 et seqq, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:EN:PDF; see also Data protection: Commission adopts decisions recognising adequacy of regimes in US, Switzerland and Hungary, IP/00/85, available at http://europa.eu/rapid/pressReleasesAction.do?reference=IP/00/865&format=HTML&aged=1&language=EN&guiLanguage=en; further information: Klug, RDV 2000, 212 et seqq.

[70] Conolly, The US Safe Harbor – Fact or Fiction?, p. 4, available at: http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf; Kuner, supra note 32, margin no. 4.59; on the level of protection provided by the Safe Harbor principles see Art. 29 Working party, Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp32en.pdf.

European Commission may decide "in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2". To this end, the Commission has set up a **standardised set of clauses** which can be used as a legal basis for transfer from each Member State (Standard Contractual Clauses[71]). If a controller located within the EU or EEC enters into a contract which includes the EU Standard Contractual Clauses, the controller located outside the EU or EEC is considered to **provide an adequate level of protection**[72].

- **Binding Corporate Rules (BCR)**

  Another possibility to ensure an adequate level of protection is to implement Binding Corporate Rules (BCR). BCRs are a set of **rules adopted within a particular company** or corporate group that provide legally-binding protections for data processing within the company or group. BCRs can be legally binding on members of a corporate group through a variety of legal devices, and may provide a legal basis for data transfers to other countries or regions[73]. All companies belonging to the group are considered to ensure an adequate level of data protection[74].

4.2.3.9 The Art. 29 Data Protection Working Party, Artt. 29 and 30 Data Protection Directive

Artt. 29 and 30 Data Protection Directive set up a Working Party on the Protection of Individuals with regard to the Processing of Personal Data (hereinafter referred to as 'Working Party') in order to achieve several objectives. It is an **independent advisory board of the European Commission** on questions relating to data protection. The Working Party shall

- examine any question with regard to national measures adopted under the Data Protection Directive in order to contribute to the uniform application of such measures
- provide expert opinion to the Commission on the level of protection within the Community
- advise the Commission on any proposed amendments of the Data Protection Directive
- give opinions on codes of conduct drawn up at Community level.

The Working Party may also – on its own initiative – make recommendations on all matters relating to the protection of personal data. It is composed of

- a representative of each Member State
- a representative of the European Data Protection Supervisor[75] and

[71] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF.

[72] Helbing, supra note 59.

[73] Kuner, Using Binding Corporate Rules for International Data Transfers: The ICC Report, Electronic Banking Law And Commerce Report, Vol. 9 No. 8 2005, p. 3, available at: http://www.hunton.com/files/tbl_s47Details%5CFileUpload265%5C1060%5Ckuner_ICC-report.pdf.

[74] Helbing, supra note 59.

[75] Currently, Peter Hustinx has been appointed European Data Protection Supervisor, whose task it is to ensure the fundamental right to protection of personal data is respected by EU institutions and bodies, see http://ec.europa.eu/justice/policies/privacy/eusupervisor/index_en.htm for details.

- a representative of the Commission.

Since the opinions and recommendations provided by the Working Party are well recognised among Data Protection Authorities as well as in data protection literature, we will occasionally refer to them in this Report. Usually, any material provided by the Working Party is also published on the Internet. In order to enable the reader to retrieve further information, we will provide the relevant URLs within this Report where possible.

4.2.3.10 Summary

Ensuring Data Protection in OPTIMIS also involves creating awareness for all parties involved. To explain fundamental legal concepts of data protection, we included a brief description of the Data Protection Directive.

The legal framework for data protection legislation within the EU is mainly determined by Directive 95/46/EC. It has two main purposes:

- It ensures the free flow of data within Europe. This prevents Member States from blocking data flows within the EU on grounds of data protection.
- It achieves a consistent level of data protection within all EU Member States. This means every Member State has more or less the same level of protection for personal data.

The natural or legal person or body responsible to comply with the obligations in the Data Protection Directive while processing personal data is called the 'data controller'. The person whose personal data is being processed and who could be affected by data protection violations is called the 'data subject'. 'Personal data' includes all information concerning an identifiable individual. Processing personal data is not limited to processing in a mere technical sense. Instead, it comprises any operation performed upon personal data (i.e. collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction).

The Data Protection Directive established six main principles, of which the following three are the most important:

The Directive establishes a principle of prohibition of processing personal data unless there is either consent of the data subject or one of the enumerated exceptions where it is allowed to process data.

Personal data may only be processed for the purposes to which the data subject has consented to or which would be reasonably obvious to the data subject. The data subject must be provided with information concerning the purposes of the processing and the identity of the data controller.

Transfer of personal data within the EU is allowed if all conditions for processing of personal data (consent or exception in the Data Protection Directive) are met. Transfer of personal data to countries outside the EU is principally prohibited. However, there are some exceptions to this rule. For some countries, the European Commission has decided that they provide an adequate level of protection. These countries are treated as if they were EU Member

States. Transfer of personal data to countries which do not provide an adequate level of protection can be justified on the following grounds:

- the data subject has given his consent
- transfers to the US happen according to the Safe Harbour Agreement, according to which US enterprises, companies or organisations demonstrate their compliance with the EU Data Protection Directive
- the parties have agreed to use the EU Standard Contractual Clauses which provide an adequate level of data protection between the parties using them
- a company or corporate group have adopted Binding Corporate Rules, so that all companies belonging to the group are considered to ensure an adequate level of data protection.

4.2.4 Directive 2002/58/EC on Privacy and Electronic Communications and EU Directive 2009/136/EC amending Directive 2002/22/EC, Directive 2002/58/EC and Regulation (EC) No 2006/2004

Directive 2002/58/EC[76] (hereinafter referred to as "ePrivacy Directive") basically deals with the right to privacy and confidentiality with respect to the processing of personal data in the electronic communication sector. The provisions of the Directive particularise and complement Directive 95/46/EC and have recently been amended by Directive 2009/136/EC[77]. Communication in the meaning of Directive 2002/58/EC is any information exchanged or conveyed between parties by means of a publicly available electronic communication service. What constitutes an electronic communications service has unfortunately not been defined by the Directive on Privacy and Electronic Communications. Instead, the Regulatory Framework Directive[78] provides the following definition:

"'electronic communications service' means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, […] but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services".

Notably, the Directive on Privacy and Electronic Communications only covers the electronic communication services that do not focus on the content, but on the communication of information (i.e. providing access to the Internet, mobile and telephone connections)[79]. It has not

[76] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications), OJ L 201, 31.07.2002, pp. 37 – 47.

[77] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009, pp. 11-36; the consolidated version of Directive 2002/58/EC is available in the leaflet "Regulatory framework for electronic communications in the European Union" by the European Commission, http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

[78] Directive 2002/21/EC of the European Parliament and of the Council Of 7 March 2002 on a Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive) OJ L 108, 24.04.2002, p. 33.

[79] Kuner, supra note 32, margin no. 3.54.

yet been clarified whether the provision of hardware infrastructure services as in the use of cloud computing can be deemed an 'electronic communications service'. One could argue that cloud infrastructure providers provide a service which consists mainly in the conveyance of signals on the Internet, since with cloud computing data is dynamically provisioned within the entire cloud and therefore will be constantly transmitted to other data centres. However, the wording of the aforementioned definition deserves a closer look here. Directive 2002/58/EC covers services which consist 'wholly or mainly in the conveyance of signals on electronic communications networks'. It is clear that cloud computing cannot be considered a telecommunications service, as it is not a service which consists 'wholly […] in the conveyance of signals', but it may be a service which consists 'mainly in the conveyance of signals'. Conveyance is the process of taking something from one place to another[80]. Common examples of electronic communication services include providing access to the internet, transmission of information through electronic networks, voice telephony services, electronic mail conveyance, mobile and telephone connection etc.[81] Cloud Computing is as such not comparable to these examples, but it takes data from one place to another in order to optimise the use of hardware infrastructures. It is thus not unreasonable to regard OPTIMIS as a service conveying data from one data centre to another. 'Signals' are a series of electrical waves that carry content to a recipient. In OPTIMIS, these signals are conveyed between different cloud providers in order to optimise the use of the hardware infrastructure.

Furthermore, an examination of the genesis of the ePrivacy Directive might clarify its scope. Directive 2002/58/EC replaces Directive 97/66/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. The latter applied to the "processing of personal data in connection with the provision of publicly available telecommunications services in public telecommunications networks". The ePrivacy Directive has broadened this scope: it applies to the "processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks". The term 'telecommunication' has been replaced by 'electronic communications' which shows that the European legislator intended to cover all different types of transmission services for electronic communications rather than mere telecommunications services[82]. Recital 4 ePrivacy Directive supports that view by saying that the ePrivacy Directive shall provide an equal level of protection 'regardless of the technologies used'. Consequently, cloud computing would be comprised by the scope of the ePrivacy Directive.

However, this Directive excludes services providing content or exercising editorial control over content transmitted using electronic communications networks. If a service mainly consists in offering information, the Directive on Privacy and Electronic Communication does not apply[83]. This is also emphasised by Recital 5 Regulatory Framework Directive which stresses that it is "necessary to separate the regulation of transmission from the regulation of content." Since

[80] Oxford Advanced Learner's Dictionary, Oxford 2010, available at: http://www.oxfordadvancedlearnersdictionary.com/dictionary/conveyance.

[81] Kuner, supra note 32, margin no. 3.54; Rosier, in: Büllesbach/Poullet/Prins, supra note 55, Directive 2002/58/EC, Art. 2 note 1 lit. b).

[82] COM (2000) 385 final, p. 2.

[83] Kuner, supra note 32, margin no. 3.54 et seq.

OPTIMIS does not offer content, but rather provides means to efficiently distribute information within a cloud, it is not excluded by the ePrivacy Directive.

Nevertheless, there is an exception with regard to private clouds. Pursuant to Art. 3 sub (1) ePrivacy Directive, the electronic communications services concerned are only those publicly available. Private clouds are internal networks, accessible only for the organisation operating them. The ePrivacy Directive does therefore not apply to them. However, if a private cloud makes use of a public cloud by deploying VMs and sending personal data to a public cloud provider, the ePrivacy Directive would apply again[84].

We will analyse the consequences deriving from the applicability of the ePrivacy Directive in the following Reports.

4.2.5 Directive 2006/24/EC of the European Parliament and of the Council on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC

One the most controversial[85] legal instruments within the field of data protection is Directive 2006/24/EC on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks (hereinafter referred to as Data Retention Directive). The legislative procedure was the shortest in the history of the EU[86] and has to be regarded in the context of the bombing attacks in Madrid in March 2004[87]. Pursuant to Art. 1 sub (1), the Data Retention Directive applies to the Providers of publicly available electronic communications services with respect to traffic data which are generated or processed by them. The definition of the term 'electronic communications services' is identical to the one provided in Directive 2002/21/EC, as Art. 2 sub (1) Data Retention Directive provides that the definitions of Directive 95/46/EC, Directive 2002/21/EC and Directive 2002/58/EC apply.

The purpose of the Data Retention Directive is to retain certain categories of data in publicly available electronic communication services in order to investigate, detect and prosecute serious crimes in the Member States. It applies to traffic and location data of both legal entities and natural persons, but not to the content of electronic communications, including information consulted using an electronic communications network.

[84] Art. 29 Working Party, WP 37, Privacy on the Internet – An integrated EU Approach to On-line Data Protection, p. 23, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37en.pdf.

[85] The Register, 'Data Retention Directive Receives Rubber Stamp', available at: http://www.theregister.co.uk/2006/02/24/data_retention_directive_ratified/; see also Spiegel Online, 'German High Court Limits Phone and E-Mail Data Storage', available at: http://www.spiegel.de/international/germany/0,1518,681251,00.html.

[86] Liebwald, MR-Int. 2006, 49.

[87] Kosta/Dumortier, MR-Int. 2007, 130.

The Data Retention Directive foresees a two-tier model:

- **Obligation to retain data**

  According to Art. 3 Data Retention Directive, each provider of publicly available electronic communications services has to retain specific categories of data such as the data necessary to

  - trace and identify the source of a communication,
  - identify the destination of a communication
  - identify the date, time and duration of a communication
  - identify the type of communication
  - identify user's communication equipment or what purports to be their equipment
  - identify the location of mobile communication equipment.

  This list is ostentatiously extensive[88]. The retention of data includes data generated or processed and logged by providers of publicly available electronic communications services. This also contains Internet traffic data[89].

- **Access to data**

  Art. 4 Data Retention Directive stipulates that data retained be only provided to the competent national authorities in specific cases and in accordance with national law. Furthermore, the retained data must be stored in a way that it can be transmitted upon request to the competent authorities without undue delay (Art. 8 Data Retention Directive).

It is up to the Member States to decide on the retention period for the specified data, but according to Art. 6 Data Retention Directive, the storage period must not be less than six month and not exceed two years from the date of communication.

Data protection law also applies to the retained data. Art. 7 Data Retention Directive provides a minimum standard in so far as the retained data must be of the same quality and subject to the same security and protection as that data on the network. It is of uttermost importance to protect and secure the retained data appropriately, as there is a high risk that the aggregated traffic data could be misused by different interest groups[90]. For this reason, European Data Protection Supervisor (EDPS) Peter Hustinx demands more safeguards and criticizes that a mere reference to the existing legal framework on data protection (Directive 95/46/EC and Directive 2002/58/EC) is not sufficient[91]. In case traffic or location data will be stored in OPTI-

[88] Liebwald, MR-Int. 2006, 49, 50.

[89] Liebwald, MR-Int. 2006, 49, 50.

[90] Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005) 438 final), 2005 OJ C 298, 29.11.2005, pp. 3 et seqq, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2005:298:0001:0012:EN:PDF; Liebwald, MR-Int. 2006, 49, 52.

[91] Opinion of the European Data Protection Supervisor, ibid.

MIS, these data have to be highly secured by adequate safety measures (i.e. limited access, exclusion of any further use, guarantee the security of data, guarantee data subject's rights)[92].

There is also an obvious contrast between the ePrivacy Directive and the Data Retention Directive[93]. While Art. 6 ePrivacy Directive provides that traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication, the Data Retention Directive stipulates their retention for a definite period of time. Art. 15 sub (1) ePrivacy Directive provides that Member States may restrict the right to confidentiality of the communications "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system". Hence, the Data Retention Directive is the instrument to impose these restrictions in the Member States since its transposal is mandatory.

The Data Retention Directive raises some issues with regard to cloud computing. Especially as smaller operators frequently use outsourcing to carry out traffic data retention activities[94]. The use of cloud computing in order to perform data retention could lead to a situation where operators are considered data controllers who collect traffic data according to Art. 3 Data Retention Directive, but may not be able to accurately monitor data processing operations, particularly with data retained outside the domestic borders of the operator. The Art. 29 Working Party proposes a federated solution, whereby one of the federated cloud providers or a delegated third party, designs and implements the traffic data retention system, manages the authentication phases and partitions the memory allocated to each provider[95].

Whenever retained traffic data is transferred to other countries, this transfer must meet the conditions in the Data Protection Directive 95/46/EC. Therefore, if data retention is carried out in cloud computing environments where data is stored and provisioned dynamically, some issues will be identical to those surrounding the Data Protection Directive.

A more detailed analysis of the Data Retention Directive will be provided in one of the next Reports.

[92] Opinion of the European Data Protection Supervisor, supra note 90, pp. 5 et seq.

[93] Opinion of the European Data Protection Supervisor, supra note 90, 2005 OJ C 298, 29.11.2005, p. 3.

[94] Art. 29 Working Party, WP 172, Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive, p. 17, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf; see also Information Security Breaches & The Law, 'Article 29 Data Protection Working Party reports on implementation of Data Retention Directive', available at:

http://blog.securitybreaches.com/2010/07/19/art_29_data_protection_working_party_reports_on_implementation_of_data_retention_directive/.

[95] Art. 29 Working Party, WP 172, Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive, p. 17, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf.

4.3 Data Protection within OPTIMIS

In this section we consider privacy concerns specific to the OPTIMIS project by analysing its different cloud computing scenarios and provide an overall assessment of privacy risks inherent in OPTIMIS cloud computing.

First of all, it must be pointed out that simple compliance of OPTIMIS with the regulations of the Data Protection Directive does not prevent the necessity of Infrastructure and Service Providers to comply with local data protection law of the Member States[96]. Nevertheless, adhering to the Data Protection Directive is the first important step to compliance and will most likely result in local compliance as well. The reason for this is that the Data Protection Directive is intended to ensure that the level of protection with regard to data processing is equivalent in all Member States[97]. Pursuant to Recital 10 Data Protection Directive, the approximation of laws must not result in any lessening of the protection but must, on the contrary, seek to ensure a high level of protection in the Community. Therefore, the ECJ decided in the well known "Lindqvist" case, that the harmonisation is not limited to minimal harmonisation but amounts to **harmonisation** which is **generally complete**[98]. Albeit there is a certain margin of manoeuvre in some of the provisions of the Data Protection Directive, national law-making has to be in accordance with the objective of maintaining a balance between the free movement of personal data and the protection of private life.[99]

This Report will focus on the following issues: initially, we will analyse the **data flows and stakeholders** in OPTIMIS. After that, we will examine which **national data protection law** will be **applicable**. Next, we will identify the relevant **data controllers** within the OPTIMIS cloud infrastructure according to the four different scenarios presented in the Description of Work (Annex I).

There are more issues to be addressed here. It is questionable whether controller-processor relationships can be lawfully established in a cloud computing environment on account of a possible lack of control of the data controller over the data processors[100]. Moreover, questions arise from the transfer of personal data to third countries. Finally, legal requirements for data security have to be taken into account in OPTIMIS. We will scrutinise these issues in the following releases in more detail.

At this stage, it is more important to identify the data controllers within OPTIMIS. The reason for this is that all legal requirements of the Data Protection Directive are imposed upon the data controller. Consequently, we will first determine the stakeholder responsible for complying with legal requirements.

---

[96] Kuner, supra note 32, margin no. 5.03; this high level compliance approach is reasonable to ensure that the OPTIMIS project has an overview of what compliance activities are taking place in the various local jurisdictions, Kuner, supra note 32, margin no. 5.07.

[97] Recital 8 and 9 Data Protection Directive.

[98] ECJ, Judgment of 6 November 2003, case C-101/01 margin no. 95 et seqq, OJ C 7, 10.01.2004, p. 3 et seq - *Lindqvist*.

[99] ECJ, ibid.,margin no. 97.

[100] See Section 4.3.5.

4.3.1 Analysis of Data Processing Operations within OPTIMIS Scenarios and Use Cases

It is impossible to determine what compliance steps need to be taken in OPTIMIS unless one first knows the main elements of the processing activities, especially which stakeholders are involved, what personal data is being processed, what the purposes of processing are and whether personal data are being transferred outside the EU. Hence, the first step is to analyse the data processing practices within OPTIMIS scenarios and use cases[101]. This will be carried out at a rather abstract level, as OPTIMIS only provides the toolkit and specification which supports the construction of multiple coexisting architectures to create a cloud service ecosystem. Therefore, we will analyse the data processing practices according to the different scenarios as proposed in Annex I – "Description of Work", p. 14 et seqq.

4.3.1.1 Possible data flows according to the service lifecycle and scenarios

The OPTIMIS toolkit foresees a three-phase service lifecycle: *construction of the service*, *deployment of the service* and *operation of the service*. The service lifecycle is initiated each time a service developer implements a service and writes a service manifest. In all of the three phases, the transfer of personal data could be involved.

In the **service construction phase**, the SP builds, implements, assembles or orchestrates the service and prepares it for placement and execution on the IP. The activities performed include preparation of the VM images, configuration of parameters as well as specification of dependencies among the different components forming the service[102]. Furthermore, the service manifest describing the functional and non-functional parameters is specified and configured. This information includes location and cost constraints, capacity and elasticity requirements etc.[103] These tasks are performed with the help of OPTIMIS Programming Model using the Integrated Development Environment (IDE).

In case personal data are already processed during the construction phase, a data flow from end user to SP would be established. Typically, SPs make services accessible to the service users (subscribers, consumers, end users)[104], but it is also possible that they are cloud service providers themselves who use the capacities of IPs[105]. Therefore, data flows between subscribers and service providers could be established and personal data be transferred to the SP .

In the **service deployment phase**, the service is placed on an IP for operation by the SP[106]. Here as well it is unclear whether personal data are transferred to the SP for purposes of setting up the services. It cannot be ruled out that in deployment phase personal data are being transferred to the SP. In this case, three data flows must be distinguished:

---

[101] See Kuner, supra note 32, margin no. 5.10.

[102] Annex I, p. 12.

[103] OPTIMIS D1.2.1.1 Architecture Design Document, p. 8.

[104] Vaquero et al., A Break in the Clouds: Towards a Cloud Definition, available at: http://www.systems.ethz.ch/education/past-courses/fs09/NIS/reading/cloud-definition.pdf.

[105] While it is possible that SPs and IPs may be part of the same organization (see Annex I, p. 12), it is assumed here that the stakeholders are separated legal entities.

[106] Annex I, p. 12.

- In order to deploy the service on an existing infrastructure of an IP, the end user transfers personal data to the SP.
- The SP discloses personal data to the IP in order to deploy the service.
- The IP retrieves personal data and, to cope with peak loads, temporarily transfers it to another IP.

The **service operation** phase covers a set of operations relevant to the management of the service performed by the SP, (i.e. monitoring , corrective actions etc.) as well as run-time optimisation by the IP (i.e. moving Virtual Machines onto another data centre or even to another subcontracted Cloud Provider).

4.3.1.1.1 Actors involved

OPTIMIS involves a number of actors. Identifying the actors is important for the allocation of responsibility. Thus, we will briefly present the stakeholders in OPTIMIS cloud computing here.

- **Service provider**: The organisation providing the final cloud service via a service interface for customers
- **Infrastructure provider** is the internal or external organisation providing resources to confront the capacity demand for correct delivery of the encapsulated service.
- **Service consumer/subscriber/end user**: The organisation accessing the cloud services (i.e. a company). This service may be accessed through a user-friendly interface.

4.3.1.1.2 Federated cloud architecture, Scenario 1

In the federated cloud scenario, several Infrastructure Providers (IPs) use the OPTIMIS toolkit to establish a cooperation in which any IP can rent capacity from the others and also allow these to use its capacity. While the SP is unaware of this federation, the IP is fully responsible for the establishment of the federation and for subcontracting[107]. Although the SP is unaware of the federation set up by an IP, the SP can still pose constraints to the IP with regard to legal issues, i.e. restricted data movement across country borders.

Stakeholders in this scenario are subscribers or end users consuming the services, the service provider offering the cloud services and the underlying infrastructure provided by IPs building a federated cloud. Personal data will be moved from the subscriber to the SP who offers the services. The SP will then deploy the services on the infrastructure of an IP using the OPTIMIS deployment optimiser. Consequently, data flows will be established from end users to a SP, and from the SP to an IP. Eventually, the IP will build a federation with other IPs. This means that one or more data flows will also be established from the initial IP to (an)other IP(s) in case the initial infrastructure does not provide for enough capacity.

4.3.1.1.3 Multi-cloud architecture (all OPTIMIS), Scenario 2

As opposed to the federated cloud architecture, the SP is responsible for the service operation in the multi-cloud scenario (all OPTIMIS). He negotiates with and monitors each IP during service operation. Since IPs are managed independently by the SP, personal data will be transferred from the SP to one or several IPs. As a consequence, the different IPs used by the SP will be separated from and hence unaware of each other. Likewise, there will be no data flows

[107] Annex I, p. 14.

between the IPs. Rather, the SP will migrate services from one IP to another IP if the latter does not fulfil the agreed objectives. Personal data will therefore only be moved or transferred by the SP if services need to be migrated.

4.3.1.1.4 Multi-cloud architecture (some OPTIMIS), Scenario 3

This scenario does not differ very much from the previous one from a legal point of view. In a multi-cloud architecture in which only some IPs adopt the OPTIMIS toolkit it is still the SP who is provisioning the services on different IPs. Again there will be no data flows between IPs as it is the SP who contacts the possible IPs and monitors the service operation. Similarly to scenario 2, personal data will only be transferred by the SP to several IPs which are unaware of each other.

4.3.1.1.5 Hybrid-cloud architecture, Scenario 4

In the hybrid cloud scenario, any organisation operating a private cloud is able to externalise resources to public IPs. When the cloud optimiser component triggers that more capacity is needed, some virtual machines are deployed to public clouds. Personal data will therefore possibly be transferred from the private cloud to a public IP.

4.3.1.2 Data flows within OPTIMIS use cases

OPTIMIS will present three different use cases in which the results of the project will be applicable[108]. It is therefore important to look at these use cases and identify possible data flows for further data protection compliance analysis.

4.3.1.2.1 Cloud Programming Model, Use Case 1

As a programming model describes the fundamental attributes of a programming language, the first use case will not include any data flows to be analysed.

4.3.1.2.2 Cloud bursting, Use Case 2

Cloud bursting in OPTIMIS takes advantage of the OPTIMIS toolkit as a means to provide nearly immediate redirection of requests to an external cloud in the event that corporate resources are depleted. When a request is received, the global load balancer decides which data centre (corporate or cloud) should handle the request based on its understanding of capacity[109]. Several actors have to be distinguished in order to determine the data flows.

The first actor is the service consumer, defined as the organisation or person which is accessing the cloud service. The second stakeholder is the cloud service provider running the business application and processing the service consumer's data, defined as the organisation providing the final cloud service. In order to use the cloud service, the service consumer will externalise his business applications into the cloud, which typically goes in hand with the transfer of personal data. Therefore, a data flow is being established between service consumer and service provider. As the aim of cloud bursting is to use external resources when the cloud provider's corporate data centre has reached capacity, a third actor is involved in this use case. This is the cloud provider acting as an external organisation and providing resources to confront capacity demands of the first actor. Consequently, one more data flow is established

[108] OPTIMIS Architecture Design Document D1.2.1.1, pp. 9 et seqq.

[109] See Cloud Balancing, Cloud Bursting and Intercloud, available at: http://devcentral.f5.com/weblogs/macvittie/archive/2009/07/09/cloud-balancing-cloud-bursting-and-intercloud.aspx.

between the cloud service provider which provides the service interface to the customer and the external organisation which provides additional resources to the first cloud provider in order to handle peak loads.

4.3.1.2.3 Cloud brokerage, Use Case 3

Use case 3 focuses on the means to perform cloud brokerage. Cloud brokerage enables users to use different services from multiple cloud providers. With a multiplicity of cloud providers, each with their own set of services, pricing model etc. it would be quite cumbersome for end users to evaluate and access each service. Instead, a cloud broker creates a layer of abstraction between end user and several cloud providers by providing a single interface through which the service consumer can manage multiple clouds. This enables the end user to simply deal with the interface of the cloud broker[110]. Depending on which services a cloud broker offers, he also provides (federated) identity and access management, as well as audit capabilities and a metering of connections.

Within the cloud brokerage use case, there are three different scenario setups which make up this use case.

- **Enterprise use of multiple cloud providers**

  In the first and most simple scenario, an enterprise makes use of different services provided by various cloud providers to perform internal (business) processes. The enterprise orchestrates the different services all by itself. The actors involved are the enterprise acting as a service customer and the numerous cloud providers providing the services. The number of cloud providers performing the services depends on the complexity of the business processes to be fulfilled.

  Personal data will be transferred to several different cloud providers where all of them fulfil different tasks. Thus, data flows are being established between the enterprise and the various cloud providers rendering the services. As these cloud providers might use the advantages of cloud bursting enabled by OPTIMIS, it is also noteworthy that personal data could also be transferred to IPs when cloud providers use resources from an external cloud provider in order to confront capacity demand. Consequently, data flows are established between cloud providers providing the final cloud services and the cloud provider which is used to handle peak loads.

- **Cloud provider to broker multiple providers to provide a SLA-based tiered pricing model**

  The second scenario foresees that a cloud broker selects the best match according to the requirements of the enterprise wishing to use cloud computing. For these purposes the enterprise approaches a cloud broker with a given set of functional requirements (i.e. pricing, energy consumption, SLA parameter, compliance etc.) to which the cloud broker must comply when choosing the right cloud provider.

[110] See O'Neill, How Cloud Service Brokers Enable the Cloud Marketplace, available at: http://www.soatothecloud.com/2010/02/how-cloud-service-brokers-enable-cloud.html; see also Kupferman, The Low Down on Cloud Brokers, available at: http://www.regexprn.com/2009/08/low-down-on-cloud-brokers.html.

Cloud brokers can either simply be brokers or, at a more complex stage, additionally provide identity management, access management and audit capabilities. In the first case a broker will help IT managers to find the right cloud offering, deploy their business application into the cloud and manage it properly[111]. Stakeholders involved in this scenario are the enterprise using the cloud services, the cloud broker procuring the service providers and the cloud service providers providing the final cloud services. If the cloud broker retrieves or receives personal data from the enterprise for purposes of brokering or deploying cloud services, data flows from enterprise to the cloud broker would be established. As the cloud broker would transfer personal data into the cloud of the brokered cloud provider, another data flow would be established between the cloud broker and the cloud provider selected by the broker.

In the second case where the cloud broker is also responsible for federated identity and access management (IAM), he needs to collect personal data in order to identify the users and provide their access to the brokered cloud services. Besides, when deploying the services, personal data will be transferred from cloud broker to the correspondent cloud providers. Last but not least, the cloud provider selected as the best match by the cloud broker might also take advantage of cloud bursting and externalise resources to public IPs. Here, the first data flow can be determined between the enterprise and the cloud broker, while the second is being established between cloud broker and cloud service provider. If the latter uses cloud bursting, than a third data flow is established between cloud service provider and the external organisation providing additional resources.

- **Cloud aggregation ecosystem (CAE)**

  In the most complex scenario IT and business functions will be treated as interconnected cloud services. This scenario differs from the previous one in that the cloud broker also takes care of the network level, while the second scenario is managed on the Virtual Machine level. With CAE, a Service Oriented Infrastructure will be built on the cloud. It is therefore possible to build new services by combining or fusing different cloud services to a new offering. The cloud broker will ensure the integration, movement and security of the data between the users and cloud providers[112]. Again, there are at least three stakeholders involved: service consumer, cloud broker and the cloud providers performing the final services. Accordingly, data flows will be established between these actors.

4.3.1.3 Summary

Compliance in OPTIMIS will only succeed if the data processing operations within the various scenarios are carefully being examined. As will be shown later in the Report, the factual circumstances are often decisive in data protection compliance (see section 4.3.4). The first necessary step is to therefore create an inventory of the data processing practices of the project.

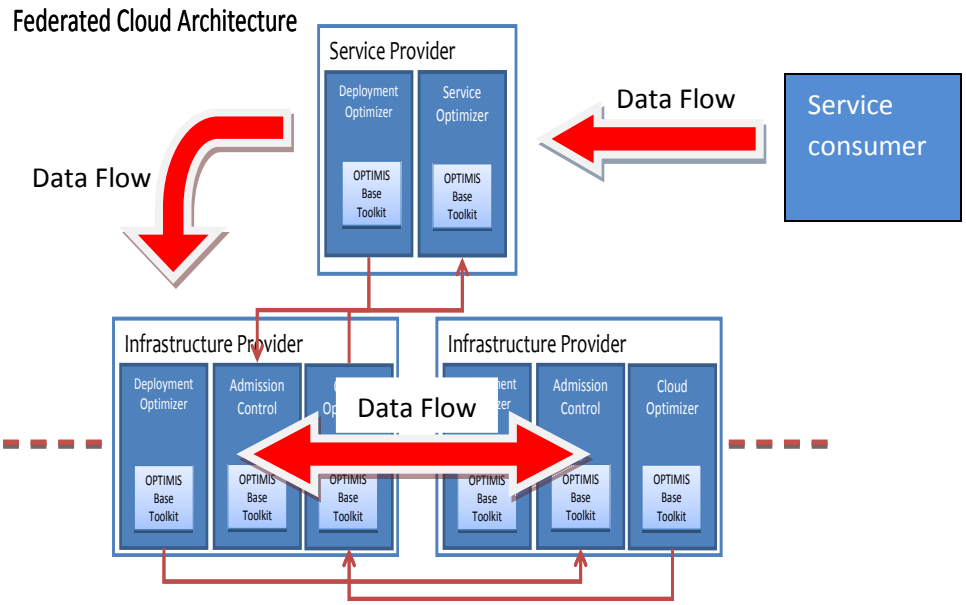
[111] See Rubin, Dynamic Cloud Fitting – The Future in Automated Cloud Management, available at: http://www.cloudswitch.com/blog/category/Cloud%20Service%20Brokers.

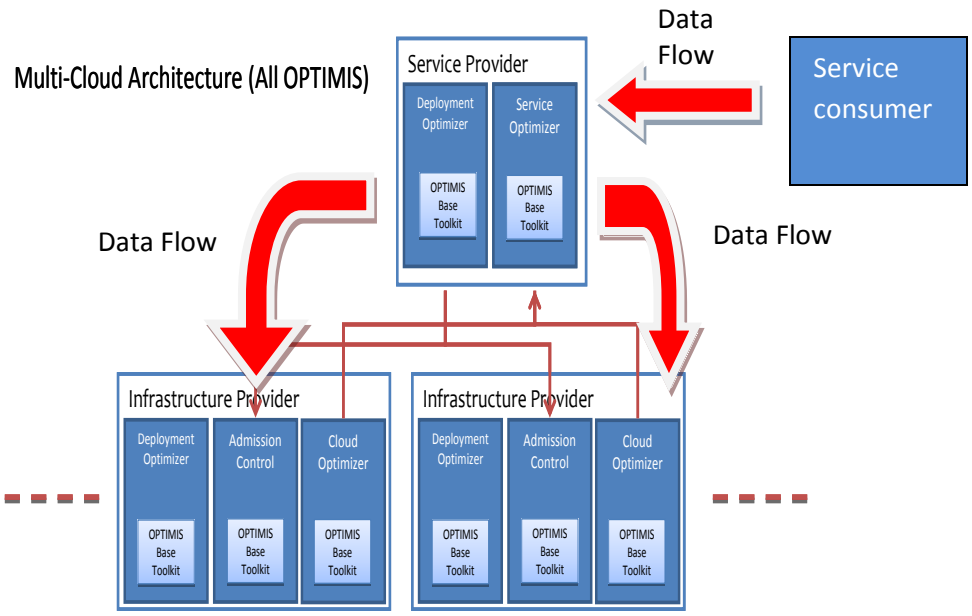
[112] Burt, Gartner Predicts Rise of Cloud Integration Services, http://www.eweekeurope.co.uk/news/news-security/gartner-predicts-rise-of-cloud-integration-services-1350.

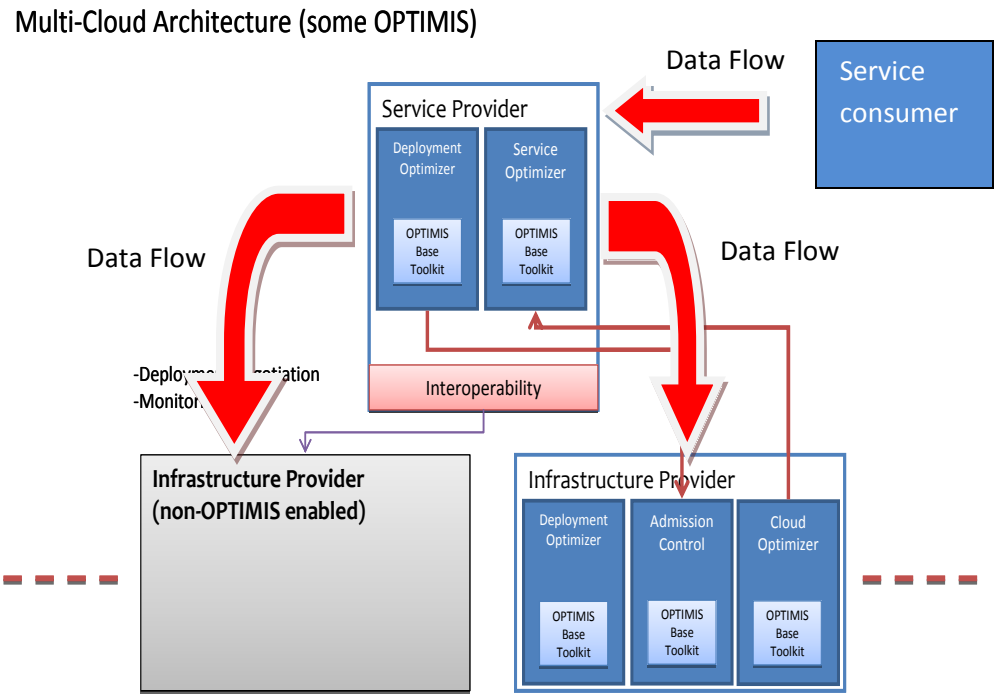
It would be impossible to determine which compliance steps are required to be taken, unless it is clear which stakeholders are involved and where personal data are being transferred to. To this end, our first step was to analyse where possible data flows might occur, which will then later be subject to our legal analysis.

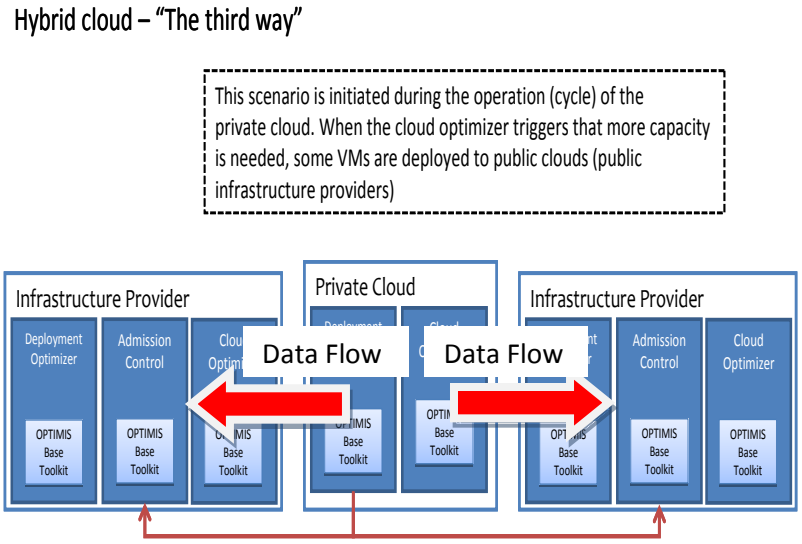
At first, we identified the actors involved in data processing in OPTIMIS. After that, we looked at possible data flows between these actors in the service lifecycle and the various scenarios envisioned by OPTIMIS. For all scenarios, it is assumed that the service consumer has previously transferred personal data to the SP who will then create, deploy and operate the services. Instead of summarising the data flows again, we will provide a graphical overview on the scenario:

4.3.1.4 *Graphical overview over data flows within OPTIMIS*




Multi-Cloud Architecture (All OPTIMIS)
Service Provider
Deployment Optimizer
Service Optimizer
OPTIMIS Base Toolkit
Data Flow
Service consumer
Data Flow
Data Flow
Infrastructure Provider
Deployment Optimizer
Admission Control
Cloud Optimizer
Infrastructure Provider


Multi-Cloud Architecture (some OPTIMIS)
Data Flow
Service consumer
Service Provider
Deployment Optimizer
Service Optimizer
OPTIMIS Base Toolkit
Data Flow
Data Flow
Interoperability
Infrastructure Provider (non-OPTIMIS enabled)
Infrastructure Provider
Deployment Optimizer
Admission Control
Cloud Optimizer



4.3.2 Personal data in OPTIMIS

Cloud OPTIMIS provides for optimised hardware infrastructure services on the basis of VMs[113]. These VMs are not earmarked to serve particular purposes, but frequently used in a business context by enterprises in order to process customer and employee data in customer relationship or human resources management applications. The operation of such applications typically involves processing of personal data. Therefore, it has to be scrutinised whether encryption of this data will render the Data Protection Directive inapplicable because of processing potentially anonymous data. Providing a deep analysis of this issue is very complex as the concept of personal data is itself highly debated. Therefore, this topic needs further research and we will address this question following Reports.

4.3.3 National Data Protection Law Applicable, Art. 4 Data Protection Directive

In this section, we assess the applicable law according to Art. 4 Data Protection Directive. Since OPTIMIS refers to an optimised use of distributed infrastructures and resources which require that data will be moved geographically, it is clear that this involves different jurisdictions and data transfers to other countries. The location of personal data will be moved continuously during service operation, rendering the location of personal data highly volatile. For that reason, one of the challenges in OPTIMIS is to determine which national data protection law applies. As the law ultimately requires durable connections with a Member States, the OPTIMIS concept finds itself in a certain field of tension with the determination of applicable law. The question which national law applies is important, as in case of a dispute this will be decided by either a national court or a national data protection authority at the very beginning of the case. If a cloud provider falls into the jurisdiction of a Member State's national data protection act, he must comply with these specific provisions. Failure to do so might result in fines as well as civil liability or even criminal prosecution.

[113] OPTIMIS Architecture Design Document D1.2.1.1, p. 7.

According to Art. 4 sub (1) Data Protection Directive, the establishment of the controller processing the data determines the national law applicable. Hence, for reasons of compliance it is imperative to know what constitutes an establishment in the meaning of this provision and where these establishments are located. Cloud Providers and Service Providers within the OPTIMIS project therefore have to be aware of the location of establishments involved in the processing in order to know which national data protection laws they have to comply with.

Art. 4 Data Protection Directive seems to be easily applicable at first glance. Only at a second glance it becomes clear that determining which national law applies is extraordinarily complex. At the same time, determining the applicable law is of central importance as one of the main impediments in compliance is not knowing which law is applicable[114].

4.3.3.1 Establishment of a controller in a Member State, Art. 4 sub. (1) lit. a) Data Protection Directive

According to Art. 4 sub. 1 lit. a) Data Protection Directive, each Member State shall apply the national provisions to the processing of personal data where the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State. Hence, the national law applicable is determined by a data controller's establishment[115]. The Data Protection Directive establishes a strict "country of origin principle" for controllers processing personal data[116]. This means if a data controller is established in a certain Member State, but is processing data in another Member State, he only has to comply with the national data protection law in the Member State in which he is established. Nevertheless, it is not clear what constitutes an establishment with regard to the OPTIMIS cloud computing concept.

4.3.3.1.1 Virtual Machines (VMs) as establishments

One could argue that virtual machines created for the delivery of services constitute establishments in the meaning of Art. 4 sub. (1) lit. a) Data Protection Directive. Virtual machines are created during the deployment phase in the service lifecycle[117]. A virtual machine is a software implementation of a machine that executes programs similar to a physical machine[118]. A system virtual machine provides a complete, persistent system environment that supports an operating system along with its many user processes. It provides the guest operating system with access to virtual hardware resources, including processor, memory, network devices etc.[119] To put it simple, a virtual machine is a virtual computer which has the same features as a physical server. Since virtual machines are hosted in physical data centres and thus have a real location, a virtual machine could be considered an establishment in a Member State which governs the national law applicable.

---

[114] Kuner, supra note 32, margin no. 3.01.

[115] This section will not discuss who the actual data controller is within OPTIMIS. Rather, it primarily deals with the determination of the applicable law. The analysis of the data controller within OPTIMIS will be discussed in the following section 4.3.4.

[116] Terstegge, in: Büllesbach/Poullet/Prins, supra note 55, Art. 4 note 1.

[117] Annex I, p. 12.

[118] Virtual machine, available at: http://en.wikipedia.org/wiki/Virtual_machine.

[119] Smith/Nair, The Architecture of Virtual Machines, 2005 Computer (IEEE Computer Society), Vol. 38 Issue 5, p.32, 34.

However, there are major doubts concerning this view with regard to factual and legal aspects. One the main advantages of VMs is that they are provisioned dynamically within the OPTIMIS cloud. This does not only result in high volatility of VMs but also of the personal data being processed by the VMs. If an IP does not adhere to the performance SLA, the VM will automatically be moved to another IP with data centres providing sufficient compute power to guarantee the SLA. Furthermore, the service provider may in the course of monitoring the service execution move the VM to another IP when the former IP exceeds power consumption limits in SLAs in order to minimize power consumption and save costs for the service consumer. VMs can also easily be erased or shut down. Moreover, the provisioning of VMs is rather random with regard to location as the service deployment optimiser automatically performs evaluation and, based on this evaluation, decides which IP the VM is placed on. Therefore, VMs cannot be regarded as establishments.

4.3.3.1.2 Cloud computing data centre as establishments

It is debatable whether cloud computing data centres of IPs can be considered establishments in the meaning of Art. 4 sub. (1) lit. a) Data Protection Directive. To decide this question, further analysis of the requirements to qualify for an establishment is needed.

It is settled by case law of the European Court of Justice (ECJ) that the concept of establishment within the meaning Art. 49 of the Treaty on the Functioning of the European Union (ex-Art. 43) involves the actual pursuit of an economic activity through a fixed establishment in another Member State for an indefinite period[120]. Likewise, Recital 37 of Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market sets out that the place at which a provider is established should be determined in accordance with the case law of the ECJ. Accordingly, Art. 4 Nr. 5 Directive 2006/123/EC defines "establishment" as the actual pursuit of an economic activity by the provider for an indefinite period and through a stable infrastructure from where the business of providing services is actually carried out. Nonetheless, it has yet to be proven that this construction of the term ‘establishment’ can be applied to establishments in the meaning of Art. 4 Data Protection Directive. Recital 19 Data Protection Directive specifies that an establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements. This clarification reflects all the elements laid down in the case law of the ECJ as well as in Directive 2006/123/EC. Hence, there seems to be no substantial difference between the definition given in Recital 19 and the ECJ judgments respectively the Directive on services in the internal market. For the construction of the term “establishment” we can therefore revert to the definition given by the ECJ and the according definition in Directive 2006/123/EC[121]. Consequently, all reasons support the view that there are four core elements to be fulfilled for an establishment:

- (economic) activity
- actual pursuit / effective and real exercise of this activity

[120] See ECJ, Judgment of the Court of 25 July 1991 – Case C-221/89 margin no. 20 - *Factortame*; ECJ, Judgment of the Court of 30 November 1995 – Case C-55/94 margin no. 25 – *Gebhard*; ECJ, Judgment of the Court of 08. September 2010 – Case C-409/06 margin no. 46.

[121] Terstegge, in: Büllesbach/Poullet/Prins, supra note 55, Art. 4 note 1.

- fixed establishment / stable arrangement
- for an indefinite period

This definition is a rather broad one and therefore includes many types of business activities, not only permanent ones, but also activities that indicate a durable connection with the Member State[122]. Still, it has to be assessed whether cloud computing data centres fall under these requirements.

Without doubt, operating cloud computing data centres is an economic activity as IPs – as well as SPs – charge a fixed amount according to the utilisation of their infrastructure. It is questionable, though, whether operating data centres is an actual pursuit of an activity. Some argue that an effective and real exercise of an activity requires (human) management within the establishment and eventually the exercise of human activities, while mere technical bases are not covered by the term[123]. Typically, data centres are facilities used to house computer systems and associated components, such as telecommunications and storage systems[124]. With highly automated OPTIMIS components, data centres require little to no human intervention during service operation. This might lead to the conclusion that data centres cannot be considered establishments in the meaning of Art. 4 sub. (1) lit. a) Data Protection Directive. However, several arguments can be adduced against this view. Recital 19 Data Protection Directive shows that the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect. Rather, any establishment – regardless of its legal form – is comprised by the term. Typically, data centres do not have legal personality since they merely provide the technical means by which a cloud provider offers services to customers. But as simple branches are covered by the Data Protection Directive, data centres would fall into the scope of Art. 4 sub. (1) lit. a) Data Protection Directive. Furthermore, human activity is not completely absent in data centres. While it is clear that simple servers do not constitute establishments, the operation of large data centres is not comparable to a single server and unimaginable without human intervention. In case of failure of components, human activity is required to replace malfunctioning components or reboot physical servers after system crashes. Additionally, data centres are constantly supervised by (human) system administrators. Although some of this data centre administration work can be done remotely, it directly affects the operation of the data centre. For instance, the reconfiguration of a specific physical server in a data centre affects the way in which the servers behaves in the future. Thus, albeit administered remotely, human activity takes place in data centres.

Even if one argues that a data centre is highly automated which requires no human activity at all, an actual pursuit of an economic activity does not necessarily require human activity according to the definition of an establishment provided by the ECJ. In the decision *Factortame*,

[122] See Kuner, supra note 32, margin no. 2.51.

[123] This is – with regard to servers – argued by Engel, Reichweite und Umsetzung des Datenschutzes gemäß der Richtlinie 95/46/EG für aus der Europäischen Union in Drittländer exportierte Daten am Beispiel der USA, Doctoral Thesis, Berlin 2005, p. 35, available at:

http://www.diss.fu-berlin.de/diss/servlets/MCRFileNodeServlet/FUDISS_derivate_000000001587/2_3.pdf and Dammann, RDV 2002, 70, 74.

[124] Data centre, available at http://en.wikipedia.org/wiki/Data_center.

the ECJ decided that the instrument for pursuing an economic activity which involves a fixed establishment in the Member State concerned, cannot be dissociated from the exercise of the freedom of establishment[125]. For a cloud provider, data centres are the instruments to pursue his economic activity (providing infrastructure or software services) on a stable and continuous basis. Thus, the decisive element of an establishment is not the exercise of human activity, but rather the stable and continuous basis. This is also reflected in Recital 19 Data Protection Directive, where human activity is not explicitly required. Rather, any actual pursuit of an economic activity is covered which also includes processing inside cloud computing data centres. This is reasonable, as today data are mainly processed with the help of information technology. Data centres are stable arrangements. To build them, specific requirements must be met. For instance, major aspects of choosing data centre locations concern energy availability, energy consumption costs, climate and link to the Internet[126]. There are not many locations in a country where all factors can be met. Once a location is found and the data centre is built, it will be operated for many years. It is thus also built up for an indefinite period.

All in all, cloud computing data centres of SPs and IPs can be considered establishments within the meaning of Art. 4 sub. 1 lit. a) Data Protection Directive. The legal consequence is that data centres built and operated by the OPTIMIS partners have to comply with the national provisions of the Member State in which they are located.

4.3.3.1.3 Statutory seat of SPs and IPS as establishments

Establishments require an actual pursuit of an economic activity through a fixed establishment in another Member State for an indefinite period. SPs and IPs manage their data centres and their entire business activities from the statutory seat. Since it is not decisive where the data flows, but rather where the establishment is situated, the statutory seat also determines the national law applicable. Thus, the statutory seats constitute an establishment as well. Art. 4 sub. (1) lit. a) second clause provides that when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable. Therefore, if SPs or IPs have their statutory seat and their data centres in different countries, each of these establishments will have to comply with different national laws.

4.3.3.1.4 Statutory seat of service consumers/subscribers as establishments

Furthermore, also service consumers/subscribers have to determine which national law is applicable. Again, the establishment of the controller is decisive. A company which decides to make use of cloud services will therefore have to comply with the national law of the Member State on whose territory it has established the statutory seat.

[125] ECJ, Judgment of the Court of 25 July 1991 – Case C-221/89 margin no. 22 – *Factortame*; in this case, this instrument was a vessel.

[126] For further details see Stackhouse, Location Factors for Data centres, available at: http://www.areadevelopment.com/siteSelection/august09/data-centers-electricity-climate-space008.shtml?Page=1; Trujillo, Naturkatastrophen, gesetzliche Regelungen und Steuern bewerten – Die Standortwahl von Rechenzentren wird international, available at:

http://www.searchdatacenter.de/themenbereiche/physikalisches-umfeld/allgemein/articles/100922/.

4.3.3.2 Summary

In section 4.3.3, we identified which national data protection law is applicable. The decisive factor is the "establishment" of a cloud provider. The national law applicable depends on where the establishments processing personal data are located. It is not easy to determine what constitutes an "establishment" since the Data Protection Directive does not give much guidance on this matter. One might argue that VMs can be considered establishment. Any VM remotely started by an IP or SP would then have to comply with the data protection law of the Member State in which the VM was started. However, we concluded that VMs cannot be regarded as establishments because their existence is too volatile and can change quickly within OPTIMIS. Instead, the location of the cloud computing data centres determines the national law applicable, as well as the respective statutory seats of each SP and IP and of the service consumer.

4.3.3.3 What OPTIMIS needs to do

In the case of OPTIMIS, establishments are

- the data centres of the OPTIMIS stakeholders
- the statutory seat of the different stakeholders involved; more precisely, these are the statutory seats of SPs, IPs and service consumers.

In the first place, it follows from the foregoing analysis that it is necessary to list the data centres operating OPTIMIS to process personal data, in order to determine the national data protection law applicable for each stakeholder involved. Thus, each IP or SP operating a data centre using OPTIMIS is required to disclose the location (Member State is sufficient) in order to determine which national data protection law of a Member State is applicable. The Member State in which the data centre is located then determines the national data protection law applicable.

Furthermore, since also the statutory seats of SPs, IPs and service consumers determine the national data protection law applicable, it is necessary to list the statutory seats of these involved stakeholders.

Example:

Enterprise E with a statutory seat in UK decides to use OPTIMIS enabled cloud computing and moves personal data to SP S with a statutory seat in Spain. S operates his business by running VMs on the data centre of Infrastructure Provider I in Germany.

Since E has an establishment (statutory seat) in the UK, it has to comply with UK data protection law. S has to be compliant with Spanish data protection law, while I has to comply with the German data protection act.

4.3.3.4 Result

As a result, every stakeholder in OPTIMIS will know which national data protection law he will have to comply with.

4.3.4 Data Controllers within OPTIMIS – Responsibility for Data Protection Compliance

Clouds are met with the threat of loss of responsibilities. The involvement of many different actors like Service and Infrastructure Providers in OPTIMIS leads to situations where the data subject does not have a responsible entity to refer to for exercising the rights deriving from the Data Protection Directive. Put simply, the main problem is to **define who is who and who does what**[127]. Therefore, it is imperative to identify the stakeholders responsible for any operation or set of operations performed upon personal data. Consequently, in this section, we identify data controllers responsible for the compliance with the Data Protection Directive within OPTIMIS. We will distinguish between the four OPTIMIS scenarios[128] as the specific architectures might lead to different results.

Note, however, that the determination of data controllers in this section is only a preliminary assessment. Since we will also discuss contract data processing within OPTIMIS later on, we might come to a conclusion that contract data processing is not legitimate within OPTIMIS cloud computing concept. This may lead to the result that a stakeholder found not to be a data controller here would neither be considered data controller nor data processor. Obviously, this cannot be the final outcome of the analysis. The concept of controller is first and foremost to allocate responsibility. This is also reflected in the German and French translation of the Data Protection Directive: while the term used for the controller in the German version is "für die Verarbeitung Verantwortlicher", the French version talks of the "responsable du traitement"[129]. It is therefore a key challenge to ensure that the responsibility for data processing is clearly defined within the cloud scenarios provided by OPTIMIS[130]. Where the complexity of processing operations leads to a loss of responsibilities, only a qualification as data controller ensures that stakeholders are compliant and the data subject's right to privacy is guaranteed. Thus, the following remarks shall be without prejudice to the legitimacy of contract data processing. Rather, the analysis of contract data processing will add to the findings in this section.

4.3.4.1 Federated cloud architecture

In the federated cloud architecture, a SP offers and delivers services to a service consumer using cloud infrastructure resources of an IP. In this scenario, the SP is unaware of federations arranged by IPs. While the SP can pose certain constraints to the IP regarding performance or legal issues, the IP is fully responsible for choosing cooperation partners and subcontracting.

4.3.4.1.1 Service consumer / subscriber

Being a data controller can simply be the result of taking the decision to process personal data for a specific purpose and by specific means. Thus, any entity making this decision can be con-

[127] Poullet et. al., Discussion paper – Cloud computing and its implications on data protection, Namur 2010, available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_yvespoullet1b.pdf

[128] Annex I p. 14 et seq.

[129] Both terms can be translated "person responsible for the processing".

[130] European Data Protection Supervisor Peter Hustinx refers to this problem as one out of five main challenges with cloud computing. See Hustinx, "Data Protection and Cloud Computing under EU law", speech delivered by Peter Hustinx at the Third European Cyber Security Awareness Day, 13th April 2010, Brussels, p. 2 et seqq. available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-04-13_Speech_Cloud_Computing_EN.pdf; see also Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 4 and 7, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

sidered data controller[131]. If a company decides to process personal data by making use of OPTIMIS cloud computing and for this reason moves data into the cloud, the entity initiates a data flow (to a SP or to an IP). The processing usually happens in the pursuit of certain objectives and therefore for a specific reason or purpose. By selecting cloud computing, the company also determines the technical and organisational means of processing. The decision taken by the company includes both the purposes and means of the processing. In this case, the service consumer (subscriber) clearly determines the purpose of data processing. Thus, the first stakeholder acting as a data controller is the service consumer or subscriber[132].

4.3.4.1.2 Service providers

It is much more complex to determine the role of SPs and IPs within federated cloud architectures. The decision of whether SPs and IPs can be considered data controllers also determines whether contract data processing between the different stakeholders is still possible. Once an actor is considered to be data controller, processing on behalf of another data controller is excluded. Rather, as a data controller a stakeholder is fully responsible for compliance with the Data Protection Directive.

In order to assess the role of SPs and IPs, we will closely follow the definition given in Art. 2 lit. d) Data Protection Directive. According to this provision, controller shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. From this definition, we can derive several conditions (or "building blocks" according to the Art. 29 Working Party[133]) which have to be met in order to qualify for a data controller:

- authority of the data processing entity to "determine"
- Subject of the determination authority: "purposes and means of the processing"
- Involvement of one or multiple stakeholders: "alone or jointly with others"
- Personal scope: "natural or legal person […] or any other body"

Whether service providers are considered data controllers according to the conditions above will be examined now.

- **Authority of the SP to "determine"**

  Although the word "determine" does not constitute the first element in the definition, it is helpful to start the examination with this building block[134]. Since the decision-making authority over the purposes and means is a key feature of data controllers, "determine" should be the preliminary element to be assessed[135].

[131] Kotschy, in: Büllesbach/Poullet/Prins, supra note 55, Art. 2 note 5.

[132] See Schultze-Melling, IT-Compliance – Challenges in a Globalized World, CRi 2008, 142, 143.

[133] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 7, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[134] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 8, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[135] Hawellek, MMR-Aktuell 2010, 300069.

The word "determine" suggests that an entity must have the authority or control to decide on the processing of data. Consequently, Art. 2 lit. d) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (Convention 108) defines the controller of the file as the body who is "competent […] to decide"[136]. Similarly, the Explanatory Memorandum comments on the definition in Art. 2 lit. d) Data Protection Directive that the controller "decides the 'objective' of the processing". The controller decides on the purposes and the operations which shall be applied to personal data[137]. The word "controller" already implies that the processing entity has the power of control over particular circumstances of data processing. Consequently, the power to decide on the circumstances of data processing indicates that an entity can be regarded as a data controller. Where it is doubtful whether an entity is a data controller, a possible approach could be to examine why the processing is taking place and who initiated it[138].

Still, this does not answer when a processing entity effectively has such power. For this reason, further criteria are needed to assess whether a processing entity actually "determines" the objective of data processing. The first Commission proposal referred to Convention 108 which stipulates in Art. 2 lit. d) that a data controller is the "body who is competent according to the national law to decide". The final adopted text only refers to the body "which determines". Hence, the genesis of the data controller definition shows that it is possible to be a data controller regardless of a specific power to control data conferred by law[139]. Accordingly, the concept of data controller is a functional concept and thus based on factual rather than formal analysis[140]. This means that responsibility of a controller is attributed on the basis of factual circumstances[141].

Moreover, the concept of controller has two aims: Firstly, it intends to allocate responsibility. This means that the role of the controller is to determine who shall be responsible for compliance with data protection rules[142]. Secondly, it shall ensure predictability with regard to control[143]. For the processing entity, it must be foreseeable whether the processing operation or set of such operations will result in the responsibility as a data controller.

[136] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 8, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[137] See Art. 2 lit. d) Convention 108.

[138] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 8, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[139] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 8, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[140] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 9, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[141] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 11, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[142] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 4, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[143] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 9, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

With regard to OPTIMIS, SPs do not have the authority to assign or decide on the objectives of data processing. Rather, the processing is initiated by the subscriber of the services offered by the SP. The decision to "move to the cloud" stems from the entity which chooses to make use of cloud computing. Usually, this is the decision of service consumer. Although the data have been transferred to the SP, the objective of the processing has been decided by the controller. Unless otherwise agreed, amending the objectives of data processing typically is not envisioned by the entity using a cloud service.

From a service consumer point of view, SPs merely provide externalised business software applications with all the advantages that cloud computing additionally offers. The service provider deploys and operates the business process as a service according to the needs of the customer. While operating the services, the SP shall not have any power to decide on the objectives of the processing. From the point of view of a SP, the data collected is not meant to be used for his own purposes. Rather, the SP receives the data in support of the service consumer (subscriber). The SP offers a service by adhering to the purposes defined by the subscriber. Thus, for SPs the objective of processing stays an external objective. SPs do not receive the data for the purpose of further processing, but for providing the services such as business processes (i.e. customer relationship management, human resource management). Instead of pursuing his own purposes with the data transmitted, the SP adheres to the purposes predetermined by the service consumer/subscriber. A decision by the SP to use the data for other objectives than providing a software service would result in a change of purpose for which data subject's consent would be necessary. Consequently, the factual analysis points towards the service consumer/subscriber as the data controller, while SPs do not seem to determine the processing operations.

- **Subject of the determination authority: "purposes and means of the processing"**

  Nevertheless, one might come to a different conclusion when regarding the 'substantial part'[144] of the definition in Art. 2 lit. d) Data Protection Directive. Data controllers are required to determine the "purposes and means of the processing". The word "purpose" refers to "an anticipated outcome that is intended or that guides your planned actions"[145]. With regard to data protection, the purpose is the reason for the data processing. "Means" refers to "how a result is obtained or an end is achieved"[146]. In relation to data protection, the means are actions, objects or systems by which data processing results are achieved. In short, "means" implies "how" data are processed, while "purpose" involves "why" data are processed. Account must be taken of the fact that this element is to be read together with the first element: the data processing entity "determines the purposes and means of the processing". The purposes and means therefore give guidance on the level of influence which the data processing entity

[144] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 12, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[145] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 13, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[146] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 13, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

must have over the activities[147]. For analysing the role of a data controller, it is decisive to which level of detail the entity must determine the purposes and means – the "why" and "how" of the data processing[148].

One might argue that an entity which determines the means already has a high level of influence on the whole data processing: in the service deployment phase, the Service Deployment optimiser in the SP performs a service deployment optimisation procedure based on careful evaluation of IPs, including negotiation of terms of use. The main objective for service deployment is to select the most suitable IP for hosting a service. Therefore, as SPs select infrastructures of IPs according to SLA requirements, SPs could be considered data controllers for the mere fact of determining the means of data processing. While the service consumer/subscriber has little or no influence on this decision, it is the SP which determines the means by selecting the most appropriate IPs. Hence, SPs could be regarded as data controllers.

However, this construction of the term "means" only takes into account technical aspects. But its meaning has to be construed in a broader sense. "Means" do not only refer to technical ways of processing data, but also include the question of "how" data are processed, therefore also comprising organisational ways of processing data. This incorporates decisions about the kind of data being processed, entities having access to data, storage period of data etc.[149]. Arguably, depending on the services offered, SPs can also have influence on organisational ways of processing: for instance, if a SP offers customer relationship management (CRM) software, he could determine which kind of data he will process in his SaaS offer when designing the services. He will also determine who may access the services by providing identity management and, based on the OPTIMIS deployment optimisers evaluation, on which IP he will deploy the services. According to this understanding, it cannot be denied that SPs can determine the means of data processing[150]. Still, this does not make a SP a data controller as long as the determination of the means does not concern the essential elements of the means[151]. Since SPs are bound to constraints imposed on them by service consumers, one might well argue that SPs do not determine the essential element of the means.

It may be left open what "essential elements" of the means are here if the second requirement – determining the "purposes" – is not fulfilled by SPs. If the SP does not decide on the "why" of data processing, he may not be considered a data controller. Art. 2 lit. d) Data Protection Directive clearly refers to the data controller as the natural or legal person which determines both "the purposes **and** means [*emphasis added*]". Art.

[147] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 13, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[148] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 13, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[149] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 13, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[150] See Balboni, Data Protection and Data Security Issues Related to Cloud Computing in the EU, p. 6, available at http://ssrn.com/abstract=1661437.

[151] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 14, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

6 sub. (1) lit. b) Data Protection Directive provides that personal data be only collected for specified, explicit and legitimate purposes. In addition to this, they may not be further processed in a way incompatible with those purposes. To determine the purposes, SPs would have to define the reasons for which the data is processed. Typically, the purposes are defined by the entity using the services, rather than the SP. The SP would not process the personal data provided by the service consumer/subscriber if the latter had not asked the SP to process them. The SP is obliged to process the data only for purposes (i.e. CRM/HRM) of the service consumer/subscriber. SPs providing SaaS are usually not allowed to define the purposes for which the consumer processes the data. Since Art. 2 lit. d) requires the elements – "purposes and means" to be fulfilled cumulatively, SPs cannot be qualified as data controllers. As already mentioned above, SPs do not determine the purposes of the processing. Nevertheless, there could be scenarios where SPs determine the form and content of business processes and the kind personal data to be processed. Although the level of influence of the SP on the purposes increases in such situations, the data is still processed in the interest of the service consumer and not being used for the SP's own purposes. Hence, while SPs might have some influence on the means of data processing, they do not determine the purposes[152].

- **Involvement of one or multiple stakeholders: "alone or jointly with others"**

  Joint control occurs if different stakeholders determine with regard to specific processing operations either the purposes or those essential elements of the means which characterise a controller[153]. According to the already analysed elements above, this is not the case with SPs. Service consumers will usually not entitle SPs to determine what purposes the data may be used for in order to establish a joint controllership. Otherwise SPs could participate in the purpose determination process of the service consumer, which is usually not the case. Instead, SPs are simply providing economically efficient services without having interest in the data as such and without pursuing individual and independent purposes with the data. Rather, they are interested in subscribers using the services provided by them. If, for example, a service consumer transfers customer data to a SP, the SP is not supposed to use the data for his own purposes like selling the addresses or writing to the customers. His task relies exclusively on running the business application which provides for functions by which subscribers can manage their customer relations. Consequently, SPs do not jointly with the service consumer determine the purposes of data processing.

- **Common ground of the definition in Art. 2 lit. d) Data Protection Directive: exertion of control as normative condition**

  While all elements have been assessed rather separately now, there is still the risk that the findings do not reflect the factual circumstances of the operations performed upon personal data and lead to a situation where the role of a controller has been assigned

[152] See Hustinx, supra note 130, p. 3.

[153] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 19, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

to a stakeholder without taking into account the interests of the data subject. This risk is especially inherent in cloud computing (and hence the OPTIMIS project), where stakeholders can change quickly due to the optimised distribution of workload on suitable infrastructures.

What can be drawn from the definition in Art. 2 lit. d) Data Protection Directive as common ground is that being a controller requires a high level of influence on data processing. All elements in the definition mentioned so far refer to the possibility to exercise control over the whole data processing operation or set of operations at any given time and stage. As the individual elements have to be read together, it is imperative to recognise the normative approach of the term "controller" and take into account the purpose of the concept of controller, which aims at the allocation of responsibility. While it is important to look at the different elements in Art. 2 lit. d) Data Protection Directive in particular, the concept of data controller should not be based on a formal analysis. Instead, attention should be drawn to the factual analysis. According to the Explanatory Memorandum, the controller is the person ultimately responsible for the choices governing the design and operation carried out[154]. The power to control the data processing with regard to how the data processing effectively happens is therefore imperative to qualify for a data controller. This understanding of the term leaves room for a normative interpretation to determine the data controller. Accordingly, it is necessary to look whether the assessment of the different elements is consistent with the aim of the data controller concept to allocate responsibility with respect to the protection of the data subject's right to privacy. The final step to assess whether SPs could be considered data controllers is therefore to look whether the results above are in line with these aims. However, this last step in scrutinising who is the data controller could lead to a result which differs from the assessment of the particular elements. If, for example, most of the elements in Art. 2 lit. d) Data Protection Directive suggest a stakeholder could be considered a data controller, the final normative analysis might still come to a different conclusion solely because one of the elements is of such a high importance, i.e. by reasons of factual circumstances. Hence, in this final step it is necessary to ensure that the particular findings are being thoroughly balanced. If one of the elements appears to be of uttermost importance with regard to the facts and the aim of Art. 2 lit. d) Data Protection Directive, it may become the decisive element to identify the data controller.

So far, we have found SPs not to be controllers for several reasons: they lack the authority to decide on the objectives of data processing. Although SPs can determine the means of processing, they do not decide the purposes for which personal data is used. Finally, they cannot be regarded as joint controllers with the service consumer since their task is to adhere to the objectives given by the service consumer. As a consequence, SPs are considered data processors rather than data controllers. Instead, the subscriber is the sole controller in this scenario. With regard to the allocation of responsibilities, data subjects will have to address the service consumer[155] when exercis-

[154] COM (92) 422 final, p. 10.

[155] The service consumer is equivalent to the company deciding to move data into the cloud.

ing the rights deriving from the Data Protection Directive. The responsibilities and the compliance therefore remain with the entity which uses a SP, namely the service consumer/subscriber. The advantage of this result is that data subjects only have to deal with one data controller. They will in most cases already know the service subscriber and may even have a contractual relationship with him: where the data subject is an employee of the entity which runs the business application in the cloud, the employee will most probably have a work contract with the company acting as the service consumer/subscriber. In another situation concerning customers of a company, the data subjects (customers) will have service or purchase agreements with the service consumer. Data protection therefore accommodates to the contractual relationships involved here. Consequently, the data subject does not need to apply to an entity which is unknown to him (such as the SP) but rather address his contractual partner (service subscriber). Furthermore, the involvement of only a few data controllers reduces complexity for the data subject. Responsibilities are clearly allocated and remain in the sphere of the data subject's contracting party. Nevertheless, the SP is not completely taken out of the responsibility framework. As a data processor he has to comply with the instructions given by the service consumer/subscriber.

To conclude, the entity determining the objectives is the service consumer/subscriber. The SP does not have enough factual influence on the decision for which purposes the data is processed. The effective control of the processing operations stays with the service consumer who is also the data controller, while the SP can be considered the processor[156].

4.3.4.1.3 Infrastructure Providers

In federated cloud architectures such as designated in OPTIMIS, the SP deploys and operates the business services on the infrastructure of an IP. We therefore have to clarify whether IPs are data controllers within the federated cloud scenario. At the same time it has to be considered that several IPs use the OPTIMIS toolkit to establish a cooperation in which any IP can rent capacity from the others and allow these to use its capacity. Therefore, it is quite possible that more than one IP is involved in the data processing. Nevertheless, we will not focus on the situation where a cloud provider rents the capacity from another IP. Instead, this particular issue will be discussed in the "cloud bursting" section. Here, will analyse whether the *initial IP* selected by the SP can be regarded as a data controller.

- **Authority of the IP to "determine"**

  At first, it has to be assessed whether IPs have the authority to "determine". This would be the case if the IP decided the objectives of the processing. Being a data controller is primarily the result of the factual circumstance that an entity has chosen to process personal data for its own purposes[157]. It is questionable whether this applies to IPs. On the one hand, IPs do not choose to process the data for their own purposes. Rather, they essentially provide the technical means for SPs to process data in the in-

[156] Hustinx, supra note 130, p. 3; Balboni, supra note 150, p. 7: "in a cloud-computing environment it remains quite unclear and such roles still need to be determined on a case-by-case basis, in the view of the nature of the cloud services";

[157] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 8, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

terest of the service consumer. Moreover, the processing is not being initiated by the IP. In fact, this has already been done by the subscriber who has also decided the objectives of the processing. The element “determine” on its own suggests that IPs cannot be considered data controllers.

- **Subject of the determination authority: "purposes and means of the processing"**

  On the other hand, the preliminary element ("determine") and the third element ("purposes and means of the processing") have to be read together. It is evident that the initial IP selected by the SP determines the technical means of the processing. The former does not only provide the facilities (data centres), but also selects the hardware and software by which the processing is carried out. Furthermore, the IP is fully responsible for selecting other IPs when it comes to cloud bursting. The factual influence of the IP on the technical means therefore is relatively high. Since the element "means" also comprises the organisational ways of processing, it has to be considered whether IPs decide "how" data are processed. Although it is rather unlikely that IPs determine the kind of data being processed, they are perfectly able to decide who will have access to the data as well as to determine the location and security standards of the data centres and the storage period of the data. These elements can be considered essential means of the data processing[158]. Therefore it could be argued that IPs do not only decide on the technical means, but also on the organisational ways of processing.

  The question is whether IPs can also determine the purposes for the data being processed. This also depends on whether the SP and the IP are part of the same organisation[159]. Where the SP and IP are of the same entity, it is quite likely that in such a situation the high level of influence on the data processing leads to the qualification as a data controller. Where the SP and IP are part of different organisations and form separate legal entities, the IP only provides the technical infrastructure for the data processing operations, such as data centres and physical servers to operate the VMs deployed by the SP. Although IPs are storing and calculating and thus processing the data[160], their level of influence on the purposes is low. The purposes – why the data is used – have already been determined by the service consumer/subscriber. The IP is expected to provide the technical means for the data processing. Neither will IPs determine the form and content of the personal data collected, nor will they validate that data. Hence, IPs have no influence on the purposes for which personal data will be used. Their role is constrained to a mere provision of procedural assistance for data processing.

- **Common ground of the definition in Art. 2 lit. d) Data Protection Directive: exertion of control**

  While IPs in OPTIMIS do not seem to determine the purposes of the processing, they undoubtedly determine the means of the processing. The question is, whether this influence on the processing can be deemed to be of such high importance that IPs can be regarded as data controllers.

[158] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 14, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf; this interpretation is also in line with Article 29 Working Party's opinion 10/2006 (WP 128) on the SWIFT case where, despite other contractual agreements, SWIFT was found to be data controller because, among other considerations, it determined technical means such as the security standards and location of data centres.

[159] According to the "Description of Work", this scenario is also possible, see Annex I, p. 12.

[160] Pursuant to Art. 2 lit. b) Data Protection Directive, "storage" and "use" of personal data is considered processing.

In the federated cloud scenario designated by OPTIMIS, the SP is not aware of federations established by IPs. Instead, IPs decide autonomously whether and from whom they lease capacity[161]. Although SPs can pose some constraints regarding performance or transfer of personal data (i.e. in order to prevent personal data from being transferred to third countries without an adequate level of protection), the initial IP is fully responsible for selecting other IPs to externalise workload, while the SP has no influence on where VMs and data sets will be placed. Even though IPs do not determine the purposes of the data processing, their influence on determining the means is considerably high to such an extent that – from the point of view of the SP – the SP is not able to exercise control over which other IPs are involved in the processing of personal data as dynamic provisioning of data is solely the task of the IP. It is also doubtful that SPs could supervise the externalisation of resources, as this is part of the self-management of the IP. All the decisions regarding optimal placement of data are made by the IP, leaving little to no possibility of control for the SP. Thus, this characteristic feature of federated clouds within OPTIMIS gives IPs a significanty high level of influence on the data processing. If a data subject exercised the rights from the Data Protection Directive (i.e. erasure of data) by referring to the SP, the latter would possibly not be able to erase the data without the help of the IP. Moreover, the SP does not know which IPs are involved in the data processing as it is the duty of the IP to establish and manage federations. For this reason, the data subject should directly apply to the initial IP. Consequently, the initial IP used by the SP to deploy and operate the services is considered the data controller within OPTIMIS.

4.3.4.2 Multi-provider hosting

In a multi-provider hosting environment, the SP is responsible for the multi-cloud provisioning of the services. The SP contacts possible IPs, monitors the service operation and potentially migrates services from misbehaving IPs. It has to be examined who is the data controller in these scenarios in order to assess who will have to comply with the provisions of the Data Protection Directive. This section will therefore scrutinise the different stakeholders and look at their particular role as regards the status as a data controller.

4.3.4.2.1 Multi-cloud architecture (all OPTIMIS enabled)

With the plurality of actors involved in the process of OPTIMIS cloud computing, it becomes increasingly difficult to assign the obligations and responsibilities stemming from the Data Protection Directive. It is therefore a crucial issue to allocate responsibilities in the OPTIMIS multi-cloud scenarios as well.

In the multi-cloud scenario where all sites adopt the OPTIMIS toolkit, the SP is responsible for the service operation. If services fail to fulfil the agreed objectives, the SP can move the service to another IP. It is also possible for the SP to host parts of a service on multiple providers.

4.3.4.2.1.1 Service consumer / subscriber

Instead of operating customer relationship or human resources management software on-premise, the customer decides to run these applications on the infrastructure of a service pro-

[161] Annex I, p. 14.

vider. For this purpose, the subscriber needs to disclose the personal data to the SP. Therefore, as in the federated cloud scenario, the service consumer/subscriber decides to initiate a data flow to the SP[162]. By taking this decision, the service consumer/subscriber demonstrates that he is able to determine the means of the processing. Furthermore, the service consumer usually has already decided on the purposes for which he needs the data. Therefore, the service consumer can be considered a data controller.

4.3.4.2.1.2 Service Providers

The role of SPs in a multi-cloud scenario differs from the one in federated clouds. While the SP is unaware of the federation established by IPs in OPTIMIS federated cloud architecture, the SP plays a much more dominant role.

- **Authority of the SP to "determine"**

  The question is whether SPs decide the objectives of the data processing in multi-cloud scenarios. According to the Art. 29 Working Party, one should avoid a chain of (sub-) processors that would prevent effective control and clear allocation of responsibilities for processing activities[163]. At this early stage, it is still not clear which level of influence SPs have on data processing in this scenario. Yet, as already mentioned, the purposes of the data processing have already been determined by the customer of the SP and so far there is no evidence suggesting that SPs can actually determine the purposes of the data processing. Thus, as in the federated cloud scenario, we presume that SPs are simply deploying the services and do not decide the objectives of the processing.

- **Subject of the determination authority: "purposes and means of the processing"**

  Although SPs do not determine the purposes of the data processing, they have much more influence on the means used for the data processing in OPTIMIS multi-cloud architecture. In this scenario, the SP is responsible for the dynamic provisioning of the data being processed in the operation of the services. Where IPs do not fulfil the agreed objectives, the SP is able to migrate the service to another IP who will perform according to the requirements of the SP. The reason for moving data and services is to achieve the best possible performance for the subscriber. The decision of the SP to move the services to another IP inevitably includes the decision to transfer personal data to another IP. As a result, it would seem that in this scenario the SP determines the technical means of the processing. We will therefore now analyse the effect of this influence on the means of the processing as this could affect the final normative assessment.

  Since the term "means" comprises the organisational ways of processing, the question is whether the SP determines the essential elements of the means used for processing the data. What constitute "essential means" of the data processing is yet uncertain. In

[162] See Section 4,3,4,1,1,

[163] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 27, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

the original proposal, the definition of a data controller comprised the body which decides

"[…] what will be the purpose of the file, which categories of personal data will be stored, which operations will be applied to them and which third parties may have access to them".[164]

In the amended proposal, the data controller is the body who

"[…] processes personal data or causes it to be processed and who decides what is the purpose and objective of the processing, which personal data are to be processed, which operations are to be performed upon them and which third parties are to have access to them".[165]

Compared to the original proposal, it is obvious that the amended proposal extends both to the initiation of the data processing ("causes it to be processed") and the objective of the processing. Also, the wording has been slightly changed as regards the data processing operations ("applied" / "performed upon"). Remarkably, the definition of data controller provided in the amended proposal has been cut down to a rather short one in the final version of Art. 2 lit. d) Data Protection Directive. The latter defines the controller as the body

"[…] which alone or jointly with others determines the purposes and means of the processing of personal data".

One could argue that the intention of the shorter final version of the definition is to narrow the scope of data controllers. However, it cannot be interpreted as being in contradiction to the older version. Rather, the final version must be construed as being a shortened version comprising the sense of the initial and the amended proposal[166]. According to Art. 2 lit. d) Data Protection Directive, it is therefore key for data controllers to determine

- the purposes and
- the objective for which data is being processed
- the categories of data being processed
- the operations performed upon/applied to the data and
- the access management with regard to third parties for the data.

Since the purposes and objectives of the processing are covered by the first requirement in Art. 2 lit. d) Data Protection Directive ("determines the purposes"), the essential elements of the means must at least include

- the categories of data
- the operations performed upon the data and

[164] COM (1990) 314 final, p. 50.

[165] COM (1992) 422 final, p. 64.

[166] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 14, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

- the decision which third parties have access to them[167].

We will now further elaborate on whether SPs have the authority to determine the (essential) elements mentioned above. "Categories" of data refer to a set of data with particular features in common. It depends on the services offered by the SP which categories of data will be processed. Where SPs offer CRM business solutions, the services will include personal customer data collected by service consumer/subscriber. In situations in which SPs offer HRM applications, the services will include employee data. On the one hand it is possible that SPs determine categories of data by providing input fields which allow service consumers to fill in only specific data. On the other hand, CRM and HRM applications often need to be customised according to the business processes of the service subscriber. Each tenant then configures and customises the SaaS application to suit his specific needs. While the possibility to customise the services may be limited, they could still to some extent be configured by customers[168]. It is thus not certain that the SP ultimately determines the categories of data being processed.

Concerning the "operations performed upon personal data", SPs have the ability to decide on which IP they want to deploy and operate the services. In the event that an IP performs poorly, the SP is able to autonomously decide to migrate services and data needed for the services to another IP. Hence, the SP decides when personal data will be stored, how long it will be stored (storage period) and how the dynamic provisioning of the data is organised according to cost, trust, risk and eco-efficiency. It is therefore the SP who determines the activities carried out on the data.

The last essential element of the means is the decision "which third party may have access" to the personal data. Pursuant to Art. 2 lit. f) Data Protection Directive, a third party is any natural or legal person who is neither the data subject, nor the (actual) controller, nor the processor[169]. This raises the question whether the IP operating the services is one of the aforementioned entities. In actual fact, we have not yet discussed this topic. Nevertheless, this is not important here: the wording "which third parties may have access to them" in the amended proposal clearly aims to emphasise that already the possibility to disclose data to third parties suffices to qualify for a data controller. SPs are able to redeploy the services on the infrastructure of other IPs and transfer the data accordingly. It cannot be ruled out that the SP discloses personal data to an IP considered as third party. Without prejudice of the fact whether IPs are actually processors or even controllers themselves, the SP has the possibility to disclose personal data to third persons while deploying the services. Therefore, the SP takes the decision which third party may have access to the personal data.

To conclude, it can be argued that in the OPTIMIS multi-cloud architecture, SPs determine the operations performed upon the data and take the decision which third par-

[167] See Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 14, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[168] See Martin, "Customising SaaS", available at http://buildingsaas.typepad.com/blog/2006/08/customising_saa.html.

[169] Kotschy, in: Büllesbach/Poullet/Prins, supra note 55, Art. 2 note 7.

ties are to have access to them. Although the SP does not necessarily determine the categories of data being processed, the broad wording of Art. 2 lit. d) Data Protection Directive ("means") suggests that the other elements suffice to qualify for a data controller.

- **Involvement of one or multiple stakeholders: "alone or jointly with others"**

  In the multi-cloud scenario, the SP is responsible both for negotiating and monitoring each IP during execution by applying separation of concerns methods. Separation of concerns ensures the delineation and correlation of system elements such as designated in the OPTIMIS toolkit, to achieve order within a system and keep complex scenarios manageable. Therefore, in OPTIMIS no stakeholder should share in the responsibilities of another[170]. Separation of concerns is achieved by logical or physical constraints delineating a given set of responsibilities which should result in proper responsibility allocation[171]. Conversely, this means that it is the SP being solely responsible for the multi-cloud aspect of service operation. Neither service consumer/subscriber nor IP can migrate the services and transfer the data. Therefore, the SP is the entity which alone determines the means of the processing.

- **Common ground of the definition in Art. 2 lit. d) Data Protection Directive: exertion of control as normative condition**

  As in the federated cloud scenario, it is crucial to check whether the assessment of the SP as a data controller is in line with the aim of allocating responsibility and protecting the data subject's right to privacy. We have found SPs do not determine the purposes of the processing. As the definition in Art. 2 lit. d) Data Protection Directive requires both conditions to be fulfilled ("determines the purposes *and* means"), in fact the SP could not be regarded as a data controller. However, since the concept of data controller is based on a factual rather than a formal analysis[172], it is possible that we consider an SP a data controller if the level of influence is still considerably high.

  It could be argued that because of the determination of the essential means of the data processing, the SP is regarded as a data controller in this scenario. The significant influence of the SP stems from the control over the operations performed upon the data and the decision which third parties have access to them. The SP is solely and fully responsible for deploying, operating and migrating the services according to considerations of trust, risk, cost and eco-efficiency. This also means that the SP should be responsible for any failure of services, i.e. loss of data or in case the IP performs poorly and data is not accessible. Thus, while benefitting from dynamic provisioning of data and selecting the optimal IP with regard to cost and performance, the SP is running the risk of being held liable for selecting IPs which are not fulfilling the agreed upon terms. In order to clearly allocate responsibilities, the status of a data controller should be

[170] See for further details on the concept of separation of concerns http://en.wikipedia.org/wiki/Separation_of_concerns and Greer, The Art of Separation of Concerns, available at http://www.aspiringcraftsman.com/2008/01/art-of-separation-of-concerns/.

[171] Greer, ibid.

[172] See Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 9, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

consistent with the status of a stakeholder being in a position to control and decide which data flows are being initiated and to whom personal data will be transferred to. Additionally, one also has to consider the interests of the data subject: the data subject could refer to an IP in order to exercise his rights deriving from the Data Protection Directive, but in the meantime the SP might have already moved the services and personal data to another IP. In this situation it would be impossible for the data subject to consult the data and request corrections if the former IP does not process the data anymore. The IP would also not know where the data has been migrated to by the SP as he is not aware of other IPs hosting the service or parts of the service. It is thus an unreasonable demand to expect from the data subject to apply to an IP in a multi-cloud scenario since IPs can easily be substituted by an SP. Moreover, the SP will also redeploy the services in case the SP, after initial placement, identifies a better offer from another IP[173]. As performance of an IP can easily decrease or his operating costs may increase, the SP can easily migrate the services to another IP. Hence, the only fixed or steady stakeholder in the multi-cloud architecture is the SP, while IPs change frequently. Since it is the objective of the Directive to ensure that the responsibility for data processing is clearly defined and can be applied effectively, assigning the role of a data controller to the SP gives data subjects the most effective possibility to exercise data protection rights. Despite the fact that the SP does not determine the purposes, the significant influence of the SP on the data processing leads to the conclusion that he can be considered a data controller. This solution provides sufficient clarity to ensure effective application and compliance with the Data Protection Directive for the data subject[174].

4.3.4.2.1.3 Infrastructure Providers

As already mentioned, IPs have very limited authority to determine the means of data processing in a multi-cloud scenario. Albeit operating the underlying hardware infrastructure to operate the deployed services, IPs do not determine the categories of data being processed as this has already been done by the end user. Furthermore, the SP can impose constraints on the IP about whether data can be transferred to other IPs (i.e. in case of cloud bursting). Thus, the operations of the IP performed upon the data will clearly have to adhere to the service manifest specified by the SP. Consequently, the IP does not have the possibility to determine the objective of the operation or set of operations performed upon the data, as this is subject to the control of the SP. Finally, it would be disproportional to burden the data subject with ascertaining which IP is currently a data controller, since the SP can quickly substitute the initial IP by another IP. Otherwise the data subject would take the risk of not being able to exercise his data protection right. Consequently, IPs cannot be regarded as data controllers in this scenario.

4.3.4.3 Multi-cloud architecture (some OPTIMIS enabled)

This multi-cloud scenario differs from the previous one in that some of the IPs are not utilising the OPTIMIS toolkit. Although OPTIMIS will provide interoperability mechanisms for these IPs,

[173] Annex I p. 24.

[174] See Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 7, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

the SP will have recourse to less feature-rich SLA management capabilities. Additionally, the risk level for service provisioning will increase.

4.3.4.3.1 Service consumer / subscriber

Once again, the service consumer / subscriber is the entity initiating the data flow and determining the purposes for which personal data will be processed in the OPTIMIS cloud. Thus, the subscriber can be regarded as a data controller.

4.3.4.3.2 Service Provider

Unlike the multi-cloud architecture scenario where all stakeholders use the OPTIMIS toolkit, SPs are not able to resort to all features in the OPTIMIS toolkit where IPs do not use it. Nevertheless, OPTIMIS will provide for interoperability mechanisms to access IPs not operating the OPTIMIS toolkit. This means that – although not being able to negotiate every feature available in the OPTIMIS toolkit – SPs can still determine on which IPs they deploy the services. Additionally, they are able to redeploy the services on other IPs in case the non-OPTIMIS enabled IP does not fulfil the negotiated SLA. Similar to the multi-cloud scenario where all stakeholders deploy OPTIMIS, the SP is also able to migrate the services. Thus, the SP determines the activities performed upon the personal data in this scenario as well. Furthermore, SPs are able to deploy the services on IPs which may be regarded as third parties (namely different data controllers). Hence, similar to the previous multi-cloud scenario, SPs again take the decision which third party may have access to the personal data. The possibility to take this decision suffices to consider SPs decision makers of this essential element of the means in this scenario. Moreover, the exertion of control is also comparable to the previous scenario. Once more, the SP is solely and fully responsible for deploying, operating and migrating the services. As a result, he is also responsible in case data protection violations occur during one of these phases. Finally, the same considerations as in the previous scenario apply to this multi-cloud scenario as well: the data subject should apply to the stakeholder which guarantees the data subject's rights will be respected in practice. Since IPs can easily be replaced by the SP in this scenario as well, the SP is the only permanent stakeholder in this architecture. Consequently, SPs should be considered data controllers in this scenario as well.

4.3.4.3.3 Infrastructure Provider

As in the previous scenario, IPs provide the technical basis to operate the services. While they do not determine the purposes of the data processing, it may nevertheless be possible that IPs not operating the OPTIMIS toolkit are able to determine the operations performed upon the data, since they may not be subject to constraints on the activities carried out on the data. As SPs have to resort to less feature-rich SLA management capabilities in this scenario, the IP on which the service(s) are deployed might lack features which allow the SP to impose constraints regarding the disclosure of personal data. Still, the interoperability mechanisms will be developed as external (to OPTIMIS) drivers. According to the OPTIMIS Architecture Design Document (D1.2.1.1), OPTIMIS does not differ between OPTIMIS and non-OPTIMIS enabled IPs[175]. In both cases, the Service Deployment Optimiser filters out IPs that are unsuitable due to lack of capabilities. Thus, if the service manifest requests that an IP should not disclose personal data to any other IP and the IP lacks such a function, the service will not be deployed on this infra-

[175] OPTIMIS D1.2.1.1 Architecture Design Document, p. 13 et seq.

structure. Therefore, we assume that even if an SP uses a non-OPTIMIS enabled IP, the SP can still impose constraints on the operations performed upon the personal data. Failing this, the service would not be deployed on this IP at all. Along with the possibility to impose constraints on the processing of personal data, the IP does not have the power to decide which third parties shall have access to them, because the SP can restrict this data flow as well (as in the previous scenario). Based on these findings, no argument can be found to consider IPs in this multi-cloud scenario data controllers since they do not determine the purposes and the essential means of the processing.

4.3.4.4 Hybrid cloud

The hybrid cloud scenario aims at externalising resources to a public cloud in case the private cloud of an organisation is at full capacity. When the cloud optimiser triggers that more capacity is needed, some VMs are deployed to the infrastructure of a public cloud provider.

4.3.4.4.1 Private Cloud Provider

The private cloud provider is the organisation operating an internal infrastructure called "private cloud". A private cloud is an internal cloud, which can also be named as "corporate cloud" since it identifies the corporate IT infrastructure of the organisation. The organisation collecting personal data and operating its own infrastructure to process the data clearly determines the purposes and the means of personal data. Moreover, when a private cloud provider makes use of public cloud providers, he initiates a data flow by his own decision. For this reason, private cloud providers are regarded as data controllers.

4.3.4.4.2 Public Cloud Infrastructure Provider

The public cloud infrastructure provider is an external cloud provider offering resources to entities who have not enough internal resources to handle peak loads.

- **Authority of the public IP to "determine"**

  The question is whether public IPs decide the objective of the processing. IPs are generally not aware of any personal data they are processing. Consequently, it is unlikely that they repurpose and determine a new objective for the personal data being processed. Rather, the factual influence of the public cloud IP is confined to the supply or provision of external resources, in order to maintain service operation of the services deployed and operated in a private cloud. The objective of the processing has already been determined by the private cloud provider. Hence, any data disclosed to a public IP has a previously allocated objective specified by the private cloud provider for which the public IP processes the data. Determination authority entirely remains with the entity using the public infrastructure provider. Thus, it is unlikely that public IPs define objectives for which personal data shall be used.

- **Subject of the determination authority: "purposes and means of the processing"**

  To qualify for a data controller, the public IP would have to determine purposes and means of the processing. As already mentioned, public IPs do not determine the objective or purposes of the processing. However, it is still possible that public IPs determine the essential means of the processing. To recollect, the essential means consist of

- the categories of data
- the operations performed upon the data and
- the decision which third parties have access to them.

Since the task of public IPs is to provide resources to private cloud providers, they do not determine categories of data being processed. In fact, public IPs process those categories of personal data previously specified by the private cloud provider. Despite of this, public IPs may themselves use cloud bursting in order to handle peak loads. This would result in the determination of the public IP which operations are being performed upon the data. Pursuant to Art. 2 lit. b) Data Protection Directive, data processing is any operation or set of operations performed upon personal data such as collection, storage, use, disclosure erasure etc. For this reason, the entity determining the operations performed upon personal data concomitantly determines the processing of personal data. However, it remains to be seen whether it is the public cloud provider who determines which operations are being performed upon the data. Firstly, the public IP is only used to handle peak loads. This means that the operations performed upon the data are the same operations which would have been carried out on the data on-premise at the private cloud provider, but could not be processed there due to full capacity. In short, the public IP appears as the instrument of the private cloud provider to process the data[176]. Secondly, in a situation where both stakeholders – private and public cloud provider – use the OPTIMIS toolkit, which is able to impose constraints regarding i.e. disclosure to third parties, the public IP adheres to the service manifest sent by the private cloud provider which describes the functional and non-functional requirements of the service. Consequently, the private cloud provider can still exercise full control over the data in a hybrid cloud scenario. Only if the public cloud provider is non-OPTIMIS enabled and lacks a function to behave according to the set of instructions as defined in the service manifest, one could come to a different conclusion because it is no longer guaranteed the policies defined will be adhered to. Since we are assessing the OPTIMIS project here, we assume that the public cloud provider abides by the instructions in the service manifest given by the private cloud provider so that only the latter acts as a data controller.

- **Involvement of one or multiple stakeholders: "alone or jointly with others"**

  The public IP processes the data according to the service manifest sent by the private cloud provider. In more specific terms, this means that the public IP does not have any influence on the processing operations with regard to purposes and means. As a consequence, the private cloud provider determines purposes and means alone.

- **Common ground of the definition in Art. 2 lit. d) Data Protection Directive: exertion of control as normative condition**

  As a last step, it is key to analyse whether the recent findings are in line with the aim of Art. 2 lit. d) Data Protection Directive to allocate responsibility. Although a public IP acquires some level of control over personal data when they are processed in VMs in

[176] Instead, one could also describe the public IP as the "extended arm" of the private cloud provider.

his data centres, this amounts to nothing more than processing according to the service manifest and hence to the instructions given by the private cloud provider.

One further reason to deny public IPs the status of a data controller is the short-term allocation of external resources. Capacity utilisation can rise rapidly and result in peak loads, but conversely, workload can also normalize very quickly. This short period of time contradicts the concept of the controller whose first and foremost role is to determine who shall be responsible for compliance with data protection rules, and how data subjects can exercise the rights in practice[177]. As recital 25 Data Protection Directive clearly mentions, the principles of protection must be reflected in the right conferred on individuals to be informed that processing is taking place, to consult the data, to request corrections and to object to processing in certain circumstances. These rights would be of no avail if public IPs process data for a short time and could easily be substituted by other public IPs with better offers. Also, in the meantime of the data subject trying to assert his rights, the private cloud provider could have made use of a significant number of different public IPs. Consequently, the data subject would be burdened with the task to find out which public IPs have been processing his data. Since the data is only stored as long as the infrastructure of the private cloud provider is at full capacity and will be deleted afterwards, the right to consult the data or request corrections would be of no use to the data subject. In order to provide data subjects with a more stable and reliable reference entity for the exercise of their rights under the Data Protection Directive, responsibilities must be allocated accordingly. The most stable and reliable reference entity in a hybrid cloud scenario is the private cloud provider responsible for selecting public IPs to externalise resources. For this reason, the previous findings conform to the concept of controller and thus the public IP cannot be considered a data controller.

4.3.4.5 Summary

We will now briefly summarise our findings. In this section we identified the data controllers in the various cloud scenarios provided by OPTIMIS. As a reminder, 'data controller' means the natural or legal person who alone or jointly with others determines the purposes and means of the processing of personal data. National data protection law makes the necessary steps for legal compliance essentially dependent on the characterisation of a party as either a controller or a processor. Thus, for instance, a data controller must typically take steps such as giving notice of data processing to affected data subjects, registering data processing with the national DPA, assuming liability for any data protection violations etc. If a data subject wants to exert his right to have data rectified, blocked or erased, the data subject has to know which entity he has to apply to. Moreover, in a case where data has been processed unlawfully, the data subject may claim damages from the controller. Thus, identifying data controllers is of utmost importance for OPTIMIS. Data subjects, Data Protection Authorities and courts will always address the data controller as the person responsible for all processing operations. Moreover, all obligations in the Data Protection Directive are imposed on the data

[177] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 4, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

controller. As a consequence, the data controller is the person responsible to comply with these obligations.

By contrast, the data processor must adhere to the instructions given by the data controller and adopt adequate security measures[178]. Therefore, if it is not possible to determine the relevant data controllers and processors in OPTIMIS, it becomes virtually impossible to determine their specific compliance obligations.

Hence, one of the first steps in ensuring data protection compliance within OPTIMIS is to identify which stakeholder in the various scenarios is regarded as a data controller. For the purposes of this report, we identified the stakeholders who are most likely to be identified by data subjects, Data Protection Authorities and courts in section 4.3.4.

- In the **Federated Cloud Scenario**, the service consumer acts as a data controller since he takes the decision to start the initial data flow with regard to a specific purpose. This means that it is the obligation of the service consumer to process data and transfer them to a SP in accordance with the provisions of the Data Protection Directive. Conversely, the SP does not have the authority to 'determine' the objectives of the processing as this has already been done by the service consumer. Besides, the SP is not aware of federations built by the IP initially selected by him. This excludes any possibility to exercise control over the processing operations. Although all elements of the definition in Art. 2 lit. d) Data Protection Directive indicate that the SP cannot be regarded as a data controller, in a last step we recognise the normative approach of the concept of data controller and check whether the findings are consistent with the aim of this provision, to allocate responsibility with regard to the protection of the data subject's right to privacy. As a result, we find that the SP significantly lacks control over the federation established by an IP. This has an impact on the final result: A data controller clearly needs to exercise 'control' over the data that he processes. Where the factual circumstances suggest this is not the case and absence of control is evident, the person or body processing personal data cannot be regarded as a data controller. Instead, the appropriate role of this person or body is as a data processor. As we found that the SP has no significant level of control over the federation established by the IP, he is regarded as a processor for the service consumer. This means that all processing operations performed by the SP are performed on behalf (or in the interest) of the service consumer. Consequently, the service consumer is not only responsible for his own processing operations, but also for the processing of the SP (see Art. 17 sub (2) Data Protection Directive). By contrast, while the initial IP selected by the SP does not determine the purposes, his influence on determining the means of the processing is considerably high as he exercises sole and full control over the federation. Consequently, we regard the initial IP as a data controller. Thus, the initial IP also has to be aware that he must comply with all obligations provided for in the Data Protection Directive.
- The service consumer is again regarded as a data controller in the **multi-cloud scenario (all OPTIMIS)**. As opposed to the federated cloud scenario, the SP has a signifi-

[178] Kuner, supra note 32, margin no. 2.25.

cantly high influence because of the fact that he determines essential elements of the data processing. Here, the factual circumstances imply that the level of control of the SP over the processing is sufficiently high. Thus, he can be deemed data controller in this scenario. Conversely, in this scenario IPs are unaware of each other which indicates a certain lack of control over the data processing. It would also be disproportional to burden the data subject with ascertaining which IP is currently data controller to refer to. Thus, IPs cannot be regarded as data controllers. Accordingly, they are considered data processors.

- Likewise, in the **multi-cloud scenario (all OPTIMIS)** service consumers and SPs are deemed data controllers, while this is not the case for IPs.
- While private cloud providers initiate a data flow and determine purposes and means of the processing, public IPs appear as their instrument to process personal data in the **hybrid cloud scenario**. Consequently, private cloud providers are considered data controllers, while public IPs only handle peak loads and cannot guarantee the rights conferred on data subjects. Hence, they are denied the status of a data controller.

4.3.4.6 What OPTIMIS needs to do

Having identified the different data controllers in OPTIMIS, the OPTIMIS stakeholders (service consumer, SPs, IPs) operating the toolkit which are considered to be data controllers now have to be aware that it is their duty to comply with the obligations in the Data Protection Directive. This comprises all obligations described in section 4.2.3.

As we have not yet examined what this specifically means for OPTIMIS, there are still some open questions. According to this release of the Report, currently there are no specific compliance steps to be taken by OPTIMIS. However, we will give further guidance for data controllers on how to achieve compliance in the following releases of this Report.

4.3.4.7 Result

As a result, every stakeholder in OPTIMIS will know whether he is responsible to comply with the provisions of the Data Protection Directive, respectively the national transposition of the Directive as identified in section 4.3.3 and who is liable for data protection violations in the first place. Furthermore, data subjects will know where to apply in order to exercise their rights in the Data Protection Directive in practice. In addition to this, determining the data controllers in OPTIMIS will result in more transparency for the national Data Protection Authorities and will help them to clarify the roles of the involved stakeholders. This should also avoid ambiguities with regard to the designation of data controllers.

Stakeholders identified as data controllers who do not comply with the national data protection law could incur fines from Data Protection Authorities, as well as damage claims from data subjects.

Table 1 provides an overview of the different stakeholders and their status as a data controller:

Scenario/ Architecture	Service consumer/ subscriber	Service Provider	Infrastructure Provider
Federated cloud	✓	✗	✓
Multi-cloud (all OPTIMIS)	✓	✓	✗
Multi-cloud (some OPTIMIS)	✓	✓	✗

	Hybrid cloud operator		
Hybrid cloud	✓	-	✗

Table 1: The table shows the data controllers in the different scenarios of OPTIMIS. The green tick indicates that the stakeholder has been found to be a data controller, while a red X shows possible processors.

4.3.5 Processors within OPTIMIS

Data processing in highly complex infrastructures such as OPTIMIS poses a wide range of questions to the concept of contract data processing. It is questionable whether we can adhere to this concept in federated and multi-cloud scenarios where data is distributed on an unpredictable number of infrastructures. In OPTIMIS, the processing of personal data is externalised by a controller to other entities. These entities can either be controllers which are distinct from the original controller, or several data processors. These processors may have a direct relationship with the data controller, or be sub-contractors to a processor who processes data on behalf of a controller[179]. These complex (so called multi-level or diffused) structures[180] of processing personal data involve a plurality of actors. It is therefore imperative to clearly determine whether the involved entities act as controllers or processors. Based on these findings, the correspondent obligations and responsibilities have to be allocated to the actors.

Furthermore, the location of data being processed has an impact on contract data processing. As it is the controller who must exercise control on processing of personal, it has to be taken into account that lack of control might result from the mere fact of the unawareness of the data processing location. Contract data processing (which has some advantages over controller-to-controller relationships) in multi-cloud scenarios such as envisaged in OPTIMIS highly depends on the degree of influence exerted by the controller on the processor. The lack of knowledge of the location of personal data might therefore render contract data processing inadmissible. We will therefore also deal with the volatility of data in the context of the role of a processor. However, due to time constraints, we will address these issues in the next Report.

[179] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 27, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[180] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 27, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

4.3.6 Transfer of personal data to third countries

Most cloud computing scenarios, including the scenarios depicted above in the OPTIMIS project[181], are very complex and could involve the transfer of data to multiple jurisdictions. At this stage of the project, it is still unclear to which jurisdictions data will be transferred to within OPTIMIS. While there are no issues regarding the transfer of personal data within the EU and the EEA, cross-border transfers outside the European Union respectively the EEA cannot be ruled out. In that case, the assessment of data transfers becomes exceedingly complex.

We recognise that the transfer of personal data to third countries is an issue relevant to cloud computing and as such could also affect OPTIMIS. However, this issue is not our main focus since OPTIMIS is first and foremost a European project where all partners are located within the borders of the EU. Thus, we will provide some input on this matter, but not assess the interrelated legal problems in every detail.

Prima facie, any transfer of personal data to third countries which does not ensure an adequate level of protection is prohibited by Art. 25 Data Protection Directive. However, there are a number of legal instruments to enable data controllers to render such transfers legitimate. Further research on these issues will be provided following Reports.

4.3.7 Data Security within OPTIMIS

Without data security being implemented into cloud computing concepts, privacy would be merely a word devoid of content. Data security supports data protection in that it protects the right to informational self-determination based on a technical level[182]. Taking adequate security measures is therefore an integral part of data protection compliance[183].

Art. 17 sub. (1) Data Protection Directive consequently provides for a provision which requires the controller to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access. According to this provision, this shall particularly apply where the processing involves the transmission of data over a network. Since networks are expressly mentioned in the Data Protection Directive, data security measures are mandatory and therefore have to be implemented in OPTIMIS cloud infrastructures as well. Moreover, security measures not only have to be taken at the time of processing, but at the time of the design of the processing system[184]. Hence it is also imperative to consider security measures with regard to the protection of personal data. We will provide some input on this matter in our next Report.

4.3.8 Conclusions

Based on the previous findings, we can draw several conclusions. Firstly, the Data Protection Directive is applicable to cloud computing. It seems that the main challenge in cloud computing is to apply the law according to the specific cloud architecture.

[181] See section 3.3.1.1

[182] "Privacy through technology".

[183] Kuner, supra note 32, margin no. 5.135.

[184] See Recital 46 clause 1 Data Protection Directive.

With regard to the national law applicable, the location of personal data respectively the VMs processing the data is not decisive. Rather, it depends on the location of data centres and statutory seats which national data protection law cloud providers have to comply with. Admittedly, the location of personal data becomes relevant to the extent that only data centres processing the data determine the applicable law. Still, cloud computing proves to be a more stable and durable connection with a Member State than expected. This is why the determination of the national data protection law applicable should not be too difficult for cloud providers in OPTIMIS.

Assessing data controllers in OPTIMIS is a more challenging task to accomplish. This is mainly because of the need to perform a factual rather than a formal analysis. There are no specific criteria in Art. 2 lit. d) Data Protection Directive in order to qualify for data controller. Instead, the law follows a normative approach by using a remarkably short definition with a much wider and more dynamic meaning and scope[185]. The difficulty lies in the construction of this definition by having regard to the aim and scope of the Data Protection Directive. Although the Art. 29 Working Party provides some guidance in this matter, it is still necessary for the determination of a data controller to look at each particular case. The analysis has shown that the role of a data controller depends on the selected role in the different scenarios. It is therefore not possible in OPTIMIS to consider an SP or an IP a data controller generally. Instead, being a data controller stems from the fact of offering specific services in the scenarios. Where an IP decides to establish a federated architecture, he will be regarded as a data controller, while his role is reduced to a processor in a multi-cloud environment. Cloud providers in OPTIMIS therefore have to be aware of the specific situation or position they are engaged in to facilitate compliance.

Therefore, this definition can be subject to a different interpretation. However, any interpretation always has to be in accordance with the aim to allocate responsibility and ensure that this responsibility is clearly defined and can be applied effectively[186]. Our analysis of the different scenarios in OPTIMIS tried to adhere to this concept as well as to the Art. 29 Working Party "Opinion 1/2010 on the concepts of 'controller' and 'processor'" in order to provide guidance as comprehensible as possible not only to OPTIMIS for optimal compliance, but also to the European and the Member States' Data Protection Authorities.

As a result of this very broad definition, OPTIMIS should take into account the following suggestions with regard to a perspicacious allocation of responsibilities.

OPTIMIS must clearly

- distinguish between different stakeholders

  A separation of concerns within OPTIMIS helps to allocate responsibility to the different providers (either SP or IP). Furthermore, differentiating between the different stakeholders creates more transparency both for the data subject as well as for Data

[185] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 3, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

[186] Art. 29 Working Party, WP 169, Opinion 1/2010 on the concepts of controller and processor, p. 7, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

Protection Authorities who supervise the rights conferred on the individuals by the Data Protection Directive.

- define to what extent stakeholders determine the purposes and means of the data processing

  The clearer OPTIMIS delineates which constraints service consumers, SP or IPs can impose on other cloud providers, the easier it is to distinguish whether a stakeholder can be considered a data controller or processor. Thus, the developers of the OPTIMIS toolkit have to consider which level of influence on the data processing they assign to service consumers and cloud providers in the various scenarios. Since OPTIMIS focuses on an IaaS level rather than a SaaS level, it is important to assign the particular level of influence to each stakeholder with regard to the means of the data processing. Where the cloud provider is provided with a high level of influence to impose constraints on the data processing, it is very likely to regard him as a data controller.

However, there is the need for further research, especially with regard to encrypted personal data, processors, transfer of personal data to third countries and data security aspects. These issues will be discussed in the following Reports.

4.4 Intellectual Property Law

4.4.1 Introduction

Intellectual property rights have always been considered as one of the most important tools to protect and recover the investment of authors, researchers, institutions and inventors, allowing them to acquire a limited monopoly of their ideas and creations.[187]

The aim of this Section is to identify the various and most relevant intellectual property right issues involved in the OPTIMIS project as well as the scope of protection of such rights.

The research of this section addresses five main questions:

1. What kind of intellectual property rights are relevant in a Cloud computing environment and which legislation needs further analysis?
2. Can databases enjoy the database right and if so who owns the collection of data?
3. Applicable national law.
4. Does cloud computing create new sort of information and if so who owns such information?
5. License Agreements.

As indicated in the Description of Work, there are many intellectual property questions concerning ownership and rights in information and services places “in the cloud”. This section will analyse those intellectual property issues regarding the data, databases and computer programs. In this respect, the OPTIMIS project includes the creation of databases and file systems.

[187] A Guadamuz, *Open source licenses in scientific research* (SCRIPTed - Edinburgh, 2005), at p. 1.

Other aspects and the last three questions will be examined in more detail in the forthcoming Reports.[188]

At the outset, we based our analysis on the current legislation and the most relevant European directives. Therefore, this first analysis is based on the most important legislation in the realm of intellectual property rights and not in the contractual relationship between the main stakeholders in a Cloud computing environment. This should not be taken to mean that contractual relationships are less important. On the contrary, the agreements between the parties can clarify those property rights and help us to shed some light in our discussion in answering these questions.

Within the intellectual property rights section, we provide the international framework which describes the relevant international and European legislations. In particular, this relates to the international and European legislation in the field of copyrights, patents and trade secrets. In addition, we pay special attention to copyright issues within OPTIMIS embracing the current problems related to the protection of the software developed, copyright within the Cloud infrastructure and the databases accessible within the Cloud.

4.4.2 International Framework

There are several international treaties and pieces of legislations relevant in the field of intellectual property rights. The basic and most relevant is the TRIPS Agreement which we will analyse below in conjunction with other agreements and legislations such as the Bern Convention and WIPO[189] Copyright Treaty (WTC).

4.4.2.1 Relevant International Legislation

4.4.2.1.1 TRIPS

The "Agreement on trade-related aspects of intellectual property rights" (TRIPS) has been in force since 1995 and constitutes the basic and most comprehensive multilateral agreement on intellectual property. The TRIPS Agreement represents global minimum standards for protecting and enforcing nearly all forms of intellectual property rights (IPRs).[190]

The TRIPS-Agreement is binding for all members of the World Trade Organisation (WTO). As of February 2005, 148 countries are Members of the WTO[191] including all the Member States of the European Community.[192]

4.4.2.1.1.1 Copyrights

There are many provisions in TRIPS which relates to Copyright. One of the main consequences of this agreement is that disputes related to compliance with the Bern Convention can now be contemplated by the WTO.[193]

---

[188] See Annex I, DoW, Work Package WP7.2 at p. 91.

[189] World Intellectual Property Organization, available at <URL:http://www.wipo.int/portal/index.html.en>, [Accessed 30 August 2010].

[190] World Trade Organisation (WTO), Understanding the WTO: The Agreements available at: http://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm7_e.htm, [Accessed July 8 2010].

[191] World Health Organisation (WHO), WTO and the TRIPS Agreement available at: *http://www.who.int/medicines/areas/policy/wto_trips/en/index.html* [Accessed July 8 2010].

[192] World Trade Organisation (WTO), Frequently- asked questions, available at: http://www.wto.org/english/tratop_e/trips_e/tripfq_e.htm#Who%27sSigned [Accessed July 8 2010].

Article 9 paragraph 1) of the TRIPS Agreement establishes a relationship with the Bern Convention, which means that all signatory states have to comply with Art. 1 to 29 of the Bern Convention (1971)[194] and paragraph 2) stipulates that copyright protection shall extend to expressions and not to ideas, procedures, methods of operations or mathematical concepts as such.

Article 10.1 of the TRIPS agreement establishes the protection of computer programs: "Computer programs, whether in source or object code, shall be protected as literary works under the Convention" and Art. 10.2 stipulates that compilations of data or other materials, in legible form by machine or another, which for selectivity criteria and disposition of their contents constitute intellectual creations, will be protected as such. This protection, which does not include the data or materials themselves, will be understood regardless of any author's right that subsists in respect to the data or materials as such.

Moreover, Art. 12 of the TRIPS agreement sets up the term of protection which shall be no less than 50 years from the end of the calendar year of authorised publication, or, failing such authorised publication within 50 years from the making of the work, 50 years from the end of the calendar year of making.

Finally, the TRIPS agreement provides a very flexible margin regarding the limitations and exceptions as according to Art. 13 this is facultative to each Member State. That is, no minimum standard is required.

4.4.2.1.1.2 Patents

Patent law is one of the strongest means of protection in the realm of intellectual property law, providing the inventor or his employer a limited monopoly not exceeding 20 years. The invention must meet exacting standards such as the novelty or improvement of a product that it must be more than simply an obvious and common application of technology. Furthermore, the invention must include an inventive step and be subject of industrial application which puts the patent application process under a thorough and cumbersome examination process.[195]

The general regulation for patentable subject matter is established in Art. 27 of the TRIPS Agreement which stipulates that "Patents shall be available for any invention, product or process in all fields of technology, provided that the invention is new, involves an inventive step and is capable of industrial application. Patents shall be available and patent rights enjoyable, without discrimination as to the place of invention, the field of technology and whether products are imported or locally produced."[196]

As previously mentioned this Report will not deal with a detail analysis of patents; if relevant further aspects will be examined in the forthcoming versions of the Cloud Legal Guidelines.

---

[193] Bently/Sherman, Intellectual Property Law, Third Edition, Oxford, p. 43.

[194] Bern Convention for the protection of Literary and Artistic Works, available at: http://www.wipo.int/treaties/en/ip//trtdocs_wo001.html [Accessed July 8 2010].

[195] Bainbridge, Intellectual Property, 4th Edition, p. 317.

[196] Art. 27 of the TRIPS Agreement.

4.4.2.1.1.3 Trade Secrets

Section 7 of the TRIPS Agreement provides a protection of undisclosed information. According to Article 30 of the TRIPS Agreement, in order to ensure effective protection against unfair competition Members shall protect undisclosed information.

Art. 39 (2) of the TRIPS Agreement states the following:

> Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practice so long as such information:
>
> > (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
> >
> > (b) has commercial value because it is secret; and
> >
> > (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

Infringing trade secrets implies always an improper action of obtaining information which leads to the right for damages and compensation.[197]

4.4.2.2 Other relevant treaties

4.4.2.2.1 Bern Convention and WIPO Copyright Treaty (WCT)

Both the Bern Convention and WIPO Copyright Treaty (WCT) have played an important role in influencing the current European legislation. They both form the basis for many of the European legislative provisions which were transposed into the European directives which are going to be discussed in the following sections. A detailed analysis of the Bern Convention and the WCT treaty will exceed the purpose of this Report therefore we will mention some of their provisions only when is relevant. For example, according to Article 3 of the WIPO Copyright Treaty (WCT)[198], the contracting parties shall apply *mutatis mutandis* the provisions of Article 2 to 6 of the Convention[199] in respect of the protection provided for, in the WCT Treaty. These articles are very important in the structure of the international protection system. For example, in Article 3 of the Convention we may find the criteria of eligibility for protection, such as, the nationality of author, place of publication of work, residence of author, etc.

In particular, the Convention states that its protection shall apply to authors who are nationals of one of the countries of the Union[200], for their works, whether published or not, and to authors who are not nationals of one of the countries of the Union, for their works first published

[197] Wiegele, Biotechnology and International Relations: The Political Dimensions, University of Florida Press 1991, p. 82.

[198] Article 3 of the WIPO WCT Treaty, available at: <URL:http://http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html#P53_3973 [Accessed 28 September 2010].

[199] Bern Convention for the Protection of Literary and Artistic Work available at: <URL:http://www.wipo.int/treaties/en/ip//trtdocs_wo001.html [Accessed 28 September 2010].

[200] Article 1 of the Convention provides that "The countries to which this Convention applies constitute a Union for the protection of the rights of authors in their literary and artistic works."

in one of those countries, or simultaneously in a country outside the Union and in a country of the Union.[201]

Furthermore, Article 3 (3) of the Convention refers to the definition of "published works", which means works that are published with the consent of their authors.

Finally, similarly to Article 10 (2) of the TRIPS Agreement the WCT states in Article 5 that "Compilations of data or other material, in any form, which by reason of the selection or arrangement of their contents constitute intellectual creations, are protected as such." The protection of such compilations should not extend to the data or the material itself and is without prejudice to any copyright subsisting in the data or material contained in the compilation.[202]

4.4.2.3 Relevant European Legislation

4.4.2.3.1 Copyrights

Copyright is a property right given to some specifics types of works such as literary works, films and sound recordings. The owner of the copyrighted material enjoys exclusive rights in relation to his work, such as making a copy for selling. The owner is also allowed to license his work and if a person infringes such right the owner can claim for damages. Copyright extends beyond literary works, films and recordings and covers broadcasting and storing it in a computer as well as other areas such as computer software.[203]

In principle, copyright law should not establish a monopoly. It is therefore permissible to any other person to produce a similar work as long as it is not taken from the other. One of the main characteristics of copyright law is that it does not protect the ideas but rather the way that idea has been expressed.[204]

Within the EU, several specific copyright related directives have been adopted. Relevant to Cloud computing and the OPTIMIS project are Directive 2001/29/EC[205] on the harmonisation of certain aspects of copyright and related rights in the information society, Directive 91/250/EEC on the legal protection of computer programs and Directive 96/9/EC on the legal protection of databases.

4.4.2.3.1.1 Directive 2001/29/EC on the harmonisation of certain aspects of copyrights and related rights in the information society

Directive 2001/29/EC also known as the Information Society Directive or the "INFOSOC Directive" aims to adapt the legislation on copyrights and related rights to technological developments and especially to the information society.[206]

---

[201] Article 3 of the Bern Convention.

[202] Art. 5 of WCT.

[203] Bainbridge, p. 29

[204] Bainbridge, p. 30

[205] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society [hereinafter the "INFOSOC Directive] available at:http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML [Accessed 28 September 2010]

[206] Europa, Summaries of EU legislation, Copyright and related rights in the information society: harmonisation of certain aspects available at:
http://europa.eu/legislation_summaries/internal_market/businesses/intellectual_property/l26053_en.htm [Accessed 25

According to the INFOSOC Directive, technological development has multiplied and diversified the vectors for creation, production and exploitation. There is no need to implement new concepts for the protection of intellectual property law however copyrights and other related rights should be adapted to new forms of economy and exploitation realities.[207]

Article 2 of the INFOSOC Directive provides the exclusive right for authors, to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part, of their works.[208]

In addition, the INFOSOC Directive provides for the exclusive right of authors to authorise or prohibit any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them.[209]

Furthermore, Article 4 of INFOSOC Directive provides for the exclusive right of authors, in respect of the original of their works or of copies thereof, to authorise or prohibit any form of distribution to the public by sale or otherwise.

The INFOSOC Directive provides for several exceptions and limitations. In particular and worthy to mention to Cloud computing is Article 5 (1) which refers to the temporary acts of reproduction mentioned in Article 2, which are "transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable: (a) a transmission in a network between third parties by an intermediary, or (b) a lawful use of a work…"[210]

It must also be noted that the INFOSOC Directive provides for the requirement of the Member States to provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in the Directive, and the requirement to take all the measures necessary to ensure that those sanctions and remedies are applied.[211]

Finally, according to Recital 30 of the INFOSOC Directive, it is provided that the rights referred to in this Directive may be transferred, assigned or subject to the granting of contractual licenses, without prejudice to the relevant national legislation on copyright and related rights.

4.4.2.3.1.2 Directive 91/250/EEC on the legal protection of computer programs

According to Directive 91/250/EEC [hereinafter the "Computer Program Directive"], Member States shall take into account the provisions of the Bern Convention for the Protection of Literary and Artistic Works. That is, within the EU a computer program is copyright protected, as literary work within the meaning of the Bern Convention.[212] There is no definition of computer program provided within the wordings of the Directive, however Article 1 (1) includes the preparatory design material within the scope of the term 'computer programs'. It also includes the expression in any form of a computer program and excludes however the ideas and princi-

October 2010].

[207] Recital 5 of the INFOSOC Directive.

[208] Article 2 of the INFOSOC Directive.

[209] Article 3 of the INFOSOC Directive.

[210] Article 5 (1) of the INFOSOC Directive.

[211] Article 8 of the INFOSOC Directive.

[212] Art. 1 (1) of the Computer Program Directive.

ples which underlie any element of a computer program, including those which underlie its interfaces.[213]

The Computer Program Directive stresses the originality criteria for the computer software in the sense that it is the author's own intellectual creation and no other criteria shall be applied to determine its eligibility for protection.[214]

Article 2 of the Computer Program Directive establishes authorship rights to a natural person or group of natural persons who have created the program or depending on national legislation of the Member States the person designated as the rightholder. Furthermore, it allows collective works as long as this is provided by the domestic law of each Member State. In addition, it establishes joint ownership when the computer software has been created by a group of natural persons jointly.

When computer software is created by an employee in the execution of his duties following the instructions of an employer, economic rights shall remain to the employer.[215]

The Computer Program Directive also establishes restricted acts such as the permanent or temporary reproduction of a computer program by any means and in any form, in part or in whole taking into account that some activities such as loading, displaying, running, transmission or storage of the computer program needs such reproduction, thus such activities shall be subject to the rightholder's authorisation. Furthermore, the translation, adaptation, arrangement and any other alteration of a computer program as well as the reproduction of the results, without prejudice to the rights of the person who alters the program, and; any other form of distribution to the public including the rental of the original or copies of the computer program.[216]

Article 5 of the Computer Software Directive provides some exceptions to the restricted acts. For instance, in the absence of a contract the acts of Article 4 e.g. reproduction, running, transmission, storage, translation, adaptation, etc. shall not require authorisation by the rightholder where they are necessary for the use of the computer program by the lawful acquirer according to its intended purpose. Furthermore, the person having a right to use a copy of a computer program is entitled to observe, study or test the functioning of the program without the rightholder's authorisation.

As a summary it could be said that the protection of computer programs shall be granted to all natural or legal persons eligible under domestic copyright legislation as applied to literary works[217] being the term of its protection that it is granted for the life of the author and for fifty years after his death.[218]

[213] Art. 1 (2) of the Computer Program Directive.

[214] Art. 1 (3) of the Computer Program Directive.

[215] Art. 2 (3) of the Computer Program Directive.

[216] Art. 4 of the Computer Program Directive.

[217] Art. 3 of the Computer Program Directive.

[218] Art. 8 (1) of the Computer Program Directive.

4.4.2.3.1.3 Directive 96/9/EC on the legal protection of databases

In the European Community, copyright pertaining to databases is regulated by the "Database Directive" from 1996, as well as the "INFOSOC Directive" from 2001.[219]

The Database Directive provides for a two-fold protection. The first scheme of protection is as intellectual creation by copyright. In accordance with this, databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation shall be protected as such by copyright. No other criteria shall be applied to determine their eligibility for that protection.[220] In this respect, a database must exhibit originality in order to be entitled to copyright protection. In databases within the Cloud there are a number of factors that must be considered in order to fulfil the originality criteria such as: innovative technical features e.g. new search methods or unique structure of the contents where data is differently arranged as in comparison to the traditional standard methods.[221]

The second scheme of protection is the database right also known as the "sui generis" right which provides a protection to non-original databases provided there is a substantial investment in the creation of such a database.

4.4.2.3.2 Patents

4.4.2.3.2.1 European Patent Convention

Art 52 of the EPC establishes four requirements for the granting of a patent: The product or process in question has to be 1) an invention, 2) novel, 3) which involves an inventive step and 4) subject of industrial application.

The EPC also gives some examples in Art 52 (2) of what shall not be regarded to be an invention: "(a) discoveries, scientific theories and mathematical methods; (b) aesthetic creations; (c) schemes, rules and methods for performing mental acts, playing games or doing business, and programs for computers; (d) presentations of information."

Article 52 (1) and 52 (2) of the European Patent Convention (EPC) may therefore apply when the deployment of the OPTIMIS Cloud infrastructure produces an additional technical effect which is subject to industrial application.

4.4.2.3.3 Trade secrets

The rationale behind the principle of trade secrets is that inventors have the right to keep their information secret in order to profit from them. Trade secrets can be defined as:

> "any formula, pattern, device or compilation of information which is used in ones business, and which gives...(a business person) an opportunity to obtain an advantage over competitors who do not know or use it".[222]

---

[219] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [hereinafter the Database Directive] and Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society [hereinafter the INFOSOC Directive].

[220] Art. 3 (1) of the Database Directive.

[221] Helling, Retrieving the Sources of Legal Decision-Making, Technical Possibilities and Related Legal Issues, 2004, p. 545.

[222] Wiegele, Biotechnology and International Relations: The Political Dimensions, University of Florida Press,1991, p. 82.

Trade secrets differ from other intellectual property rights such as patents and copyrights since both permit the owner to disclose or use the information in public. On the contrary, trade secrecy law does not provide a bundle of exclusive rights but grants protection against unlawful access to information.[223]

The subject matter of trade secrecy is very broad, including any type of information that has an economical value and is not regarded to be part of the common knowledge. Typical examples protected under trade secrecy law are technical and non-technical data[224], commercial and financial information about customers and employees[225], a formula i.e. a recipe or an algorithm, a "pattern" e.g. drawings to produce machinery devices and compilation of information such as customers, marketing and geological information which are usually taken before a court.[226]

In Europe there is no specific directive regarding trade secrets, therefore the recommendation is to check the domestic law of the Member States where trade secret protection is needed. However, the general rule is to seek protection under national unfair competition legislation.[227] An analysis of each nation's unfair competition legislation will exceed the purpose of this Report, therefore we will limit our analysis to the provisions in the TRIPS Agreement.

4.4.2.4 Summary

In section 4.4 we provide an overview of the international framework and European directives which OPTIMIS needs to take into consideration. It is important to position the project Consortium within the appropriate framework so as any of the aforementioned provisions can be consulted accordingly. We have structured this section in a way that all topics which govern the realm of intellectual properties in a Cloud computing environment and as a consequence in OPTIMIS are covered. Specific analysis of other intellectual property rights will be covered in the forthcoming reports. Efforts have been made where possible to highlight the relevance of each European directive. As the development of the OPTIMIS computer program is in an early stage, below we highlight two of the fundamental recommendations which should be taken into account.

4.4.2.5 What OPTIMIS needs to do

In case OPTIMIS wish to obtain:

- **Copyrights protection of computer programs:** In order to obtain copyright protection a certain degree of originality in the creation of such software is needed.

For example: While developing the source code and the machine code of OPTIMIS's computer programs, originality in the sense that it is the author's own intellectual creation shall be sought. This is also true for the adaptation of existing protected computer programs, taking

[223] McJohn, Intellectual Property: Examples & Explanations, Aspen, 2006, p. 344.

[224] Myers, Principles of Intellectual Property Law, Thomson West, 2008, p. 327.

[225] Cornish/Llewelyn, Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights, Sweet & Maxwell,2007, p. 10.

[226] McJohn, Intellectual Property: Examples & Explanations, Aspen, 2006, p. 348.

[227] Helpdesk on Intellectual Property Rights related issues in EU-funded projects available at: http://www.ipr-helpdesk.org/faqs_trade_secrets.html [Accessed October 4 2010].

into account there is the necessary degree of creativity involved in such adaptation. It follows, that every adaptation of the existing computer software also needs to comply with the terms and conditions for the use of such program.

- **Patentability of computer programs:** In order to be able to file a patent application, as patentability of computer programs as such is excluded, it is necessary to prove that the given software contains a "technical effect". The given software will need to meet certain requirements, the decisive factor being that the software invention when run in a computer produces a technical contribution to the state of the art.

For example: If the execution of a computer program developed within OPTIMIS operates in a more efficient way e.g. is faster, it consumes less energy, it uses less storing space enabling the operation system to be less cost expensive and eco-efficient, etc., it could be subject to a patent application.

Results:

As a result, if copyright protection in the computer program is achieved, the authors of the given software will be protected against mere copying. This is also true for the adaptations of existing protected computer programs provided there is the necessary degree of creativity involved in such adaptation.

As a result of obtaining a patent, the protection will be granted to the idea or concept of the computer software, thus providing a stronger means of protection in comparison to copyrights.

The figure below depicts the international and European framework which is relevant for OPTIMIS. It also shows how the abovementioned treaties influence the European directives and domestic law of each Member State of the EU.

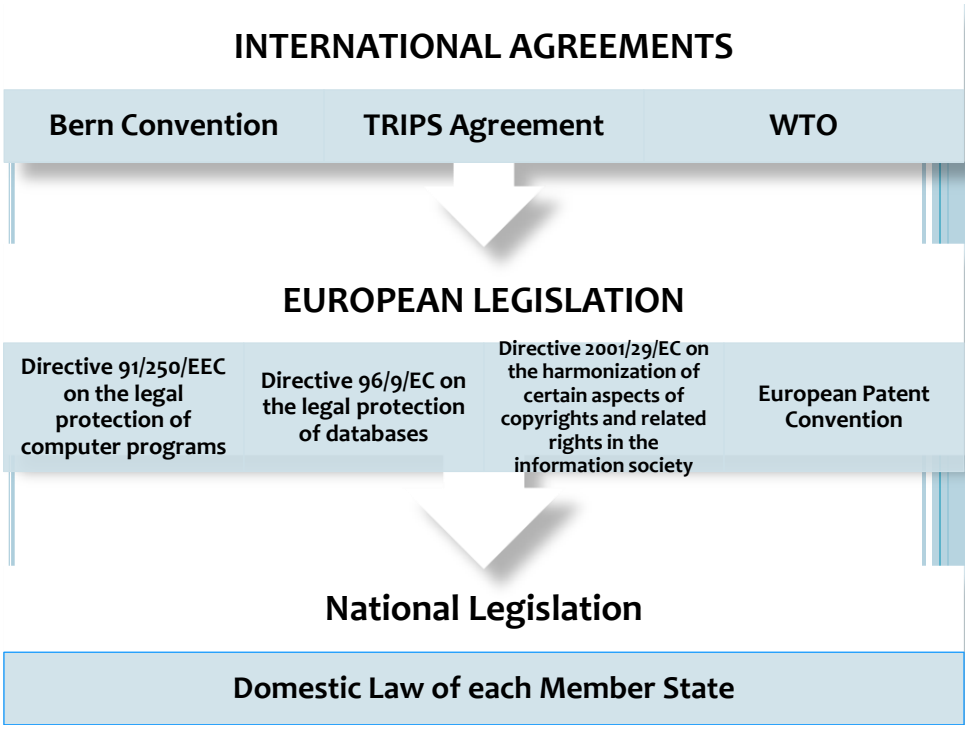


Figure 1: Intellectual Property International and European Framework

4.4.2.6 Intellectual Property Rights within OPTIMIS

4.4.2.6.1 Copyrights and Database Right

4.4.2.6.1.1 Cloud computing infrastructure

There are different ways of depicting a Cloud computing infrastructure. The best way to illustrate and understand how complex the infrastructure is, is by using the six layer structure. Therefore if we draft a pyramid (See figure 2 below) the whole infrastructure (infrastructure as a service) is placed at the bottom followed by the storage capabilities (databases) in the fifth place. The platform (as a service) which lessens deployment and applications without having the necessity of buying the costly and complicated hardware and software, would be located in the fourth place of the pyramid. The third layer is composed by the different applications which leverage the Cloud in software application, usually excluding the necessity to install and run the application on the client's own computer, therefore alleviating the burden of maintenance of the software, support and other operations. The second layer is called the 'services" as these are the software systems designed to support the interaction between different machines over the network. Finally, at the top of the pyramid are the clients.[228] Within all this complex infrastructure we need to take special care of copyrights issues taking into account the legal provisions of the international and European framework.

[228] Johnston, The 6 layer Cloud computing stack, available at: http://samj.net/2008/09/taxonomy-6-layer-cloud-computing-stack.html [Accessed 6 October 2010].

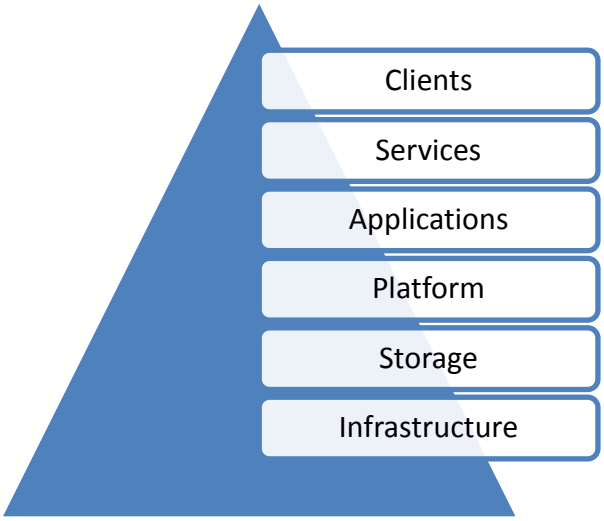


Figure 2: Layers in the cloud computing infrastructure

As can be seen in the figure above, "storage" capabilities i.e. databases play an important role in a typical Cloud computing infrastructure. Within a Cloud computing environment there are different kinds of databases. They all have unique features which allow them to serve cloud computing applications. Most of these databases have been adapted to operate in "distributed environments" meaning they can run on a wide number of servers in multiple locations.[229]

For this reason, we consider it important to provide an analysis of the relevant intellectual property issues regarding databases within OPTIMIS.

4.4.2.6.1.2 Databases within OPTIMIS

OPTIMIS provides for a special trust framework.[230] More precisely, this consists of a reputation based framework which establishes a reputation rank by collecting statistics and other data concerning the reliability of the cloud providers using OPTIMIS. The data are stored in databases at each provider, regardless whether IP or SP. These databases contain "historical data" which enable both SPs and IPs to perform a risk assessment when receiving offers from other OPTIMIS enabled stakeholders. When receiving an offer from another provider (SP or IP) a cloud provider will look for information in his historical database in order to verify the expected integrity of a provider's guarantees with respect to the presented SLAs.[231] In the course of time, these databases become more and more valuable to the cloud provider, as they contain useful information about previous collaborations with other cloud providers. The more reliable the contractual partners of an IP and SP are, the more end users will trust a cloud provider providing this information to his individual customer. Thus, it is not too much to say that the historical databases created by an IP or SP constitute one of the main assets in OPTIMIS once they are established and provided with the relevant information. Having recognised the importance of the databases for the cloud providers using OPTIMIS, it becomes clear that copyright protection is desirable for several reasons. In the first place, it prevents other cloud

[229] Jackson, Cloud computing leaving relational databases behind, available at: http://gcn.com/Articles/2008/09/19/Cloud-computing-leaving-relational-databases-behind.aspx [Accessed 6 October 2010].

[230] OPTIMIS Requirement Analysis D.1.1.1.1 p. 28.

[231] Annex I, DoW, p. 25

providers from legally using the content of the databases without the owner's consent. In the second place, the owner of a database is able to license the content or parts of the contents of the database to another cloud provider without running the risk of unauthorised reproductions or making available to the public by the license. Copyright law therefore gives the owner of the database the necessary legal protection for any potential exploitation.

However, it is questionable whether databases containing information about the reliability of the various cloud providers which have been previously used, fall under the scope of the Database Directive. One could argue that such a collection of data does not constitute a substantial investment in the obtaining of the contents of that database, since the data will be collected automatically by the OPTIMIS risk assessment components.[232]

Below we describe the historical databases within the OPTIMIS risk assessment components from both a service provider and infrastructure provider standpoint.

4.4.2.6.1.2.1 Service Provider

From a Service Provider standpoint, the Risk Assessor component within the Service Provider retrieves historical SLA data from the historical database to estimate the risk of the offer from the Infrastructure Provider's SLA quote. This allows the Service Provider to view the risk factor as the reliability estimates for Infrastructure Provider's offers, based on data contained in the historical database.[233]

It is envisaged that the Service Provider will create a list of Infrastructure Providers that will be contacted for quotes. It can operate in a number of modes, for example by returning a list of Infrastructure providers who have offered similar SLAs in the past. This is achieved thanks to the historical database together with the other components (See figure no. 3 below).[234]

The information stored in the historical database i.e. the SP's dealing history with various IPs (offers accepted, rejected, service failures, etc.) is a key asset for the risk assessment tool.[235]

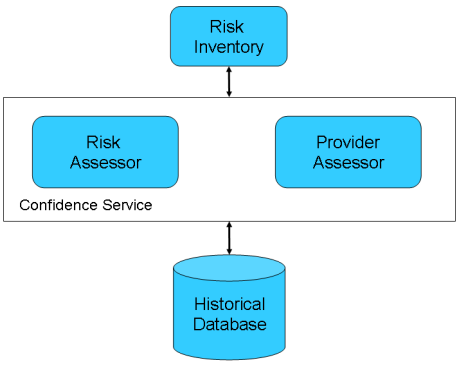


Figure 3: Historical Database within the Service Provider Risk Assessment components[236]

[232] OPTIMIS Arquitecture Design Document D1.2.1.1 at p. 27.

[233] D. 1.2.1.1. at p. 27

[234] D. 1.2.1.1 at pp. 27-28

[235] D. 1.2.1.1 at pp. 27-28

[236] Graphic taken from Architecture Design Document D1.2.1.1 p. 27.

The historical database contains a compilation of statistics data relating to previous offers, so the Service Deployment Optimiser (SDO) makes use of the 'confidence service' to query and assess the risk for the IP's generated offers using the risk assessor component.[237]

4.4.2.6.1.2.2 Infrastructure Provider

In the same vein, depending on the risk models to be developed in the context of the project, the Infrastructure Provider will have a similar historical database for its own risk assessment prior to making an offer and during service operation. The following graphic illustrates the risk architectural components for the infrastructure provider and shows where the historical databases are located within this infrastructure.[238]

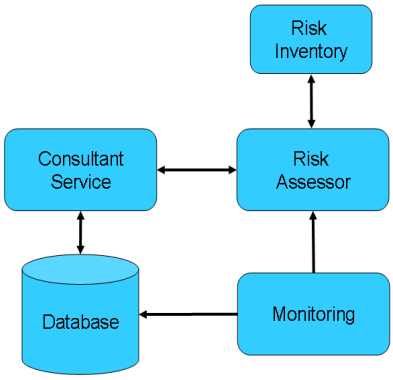


Figure 4: Historical Database within the Infrastructure Provider Risk Assessment components[239]

The historical database at the Infrastructure Provider level contains valuable information to perform a risk assessment aimed at increasing the performance and quality of an IP. The image above depicts all the components which use the historical database to process the risk assessment. The Consultant Service for instance, utilises the historical database to produce statistics and supports the risk assessor in order to estimate the risks. The Consultant Service uses a data-mining mechanism to build these statistics including static and dynamic information about the IP's resources and services operation such as current workload, system outages, temporary performance shortages, monitored network traffic, expert's availability, or general information concerning number of services to operate. In addition, the monitoring component uses monitored data to determine bottlenecks in the IP's infrastructure.[240]

[237] D. 1.2.1.1 at pp. 27-28

[238] D. 1.2.1.1 at pp. 28-29.

[239] Graphic taken from Architecture Design Document D1.2.1.1 p. 29.

[240] D. 1.2.1.1 at pp. 28-29.

4.4.2.6.1.3 Legal issues involved within the Cloud computing accessible databases

The database right can be perceived as both an opportunity to ensure property rights for a number of enterprises involved and also as a potential legal obstacle that may stop the further exploitation of Cloud computing business activities. For this reason, we expound below the most relevant legal issues relevant for this discussion.

4.4.2.6.1.3.1.1.1 The Definition of a Database

From the outset, it is important to assess whether the historical databases in the OPTIMIS architecture fall under the definition of a database as within the scope of the Database Directive.

> Article 1 of the Database Directive states:
>
> 1. This Directive concerns the legal protection of databases in any form.
> 2. For the purpose of this Directive, 'database' shall mean a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.
> 3. Protection under this Directive shall not apply to computer programs used in the making or operation of databases accessible by electronic means.

As can be seen the scope of the definition of a database in the scope of the Database Directive is very broad and it is intended to be that way so as to embrace different kinds of databases.[241] The term database include literary, artistic, musical or other collections of works or collections of other materials such as texts, sound, images, numbers, facts, and data which are systematically or methodically arranged and which can be individually accessed by electronic or other means.[242] It follows that nearly every database within a Cloud computing scenario including the abovementioned historical databases fall under the scope of the legal definition of Article 1 of the Database Directive. This is due to the reason that historical databases in OPTIMIS contain static and dynamic data[243] necessary to estimate risks such as previous SLA transactions (offers accepted, rejected, etc.) This information is separable from one another without their contents being affected and therefore are regarded to be "independent materials" in the meaning of Art. 1 (2) of the Database Directive. Classification of the database also requires that the independent materials must be systematically or methodically arranged and individually accessible by electronic means which clearly seems to be the case within the OPTIMIS historical databases.

4.4.2.6.1.3.1.1.2 Legal Conditions for their protection

According to Article 7.1 of the Database Directive "Member States shall provide for a right for the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents of that database".[244]

The Database Directive does not provide a real definition of the term investment, however Recital 7 and 40 of the Directive provide further guidance regarding the sort of investment

[241] Derclaye, The Legal Protection of Databases: A comparative analysis, 2008, p. 54.

[242] Recital 17 of the Database Directive.

[243] Annex 1, DoW at p. 111

[244] Article 7.1 of the Database Directive.

which can be not only measured in terms of financial resources but also in human resources, technical equipment, time, effort and energy.[245]

It can therefore be distinguished into three types of investment: financial, material or human. Financial investment, i.e. how much money the maker of the database has spent. Material investment, for instance, technical equipment to build up the database such as hardware infrastructure. Human investment, for example how much time, effort and energy has been invested in the creation of the database.[246]

4.4.2.6.1.3.1.1.3 Object of the investment

The investment established in Art. 7 of the Database Directive must be directed towards the obtaining, verifying and presenting the contents of the database.

a) Obtaining: The term obtaining clearly refers to the "collection" of data and not to the "creation" of data, as this has been already ruled by the European Court of Justice (ECJ):[247] "the resources used to seek out existing materials and collect them in the database, and not to the resources used for the creation as such of independent materials".[248] Defining the term obtaining within the context of the OPTIMIS project is of paramount importance since this will determine whether databases fall within scope of the Database Directive or not.

b) Verifying: The verification of the contents of a database can be done at the moment of its initial creation or in the case of on-line databases this can be done afterwards in order to check the veracity of the information in a regular basis.[249]

c) Presenting: Presenting the contents of a database refers to the way the compilation of data is showed to the users. That is, the presentation of the contents of a database is the result of the user's interface.[250] As a corollary, it also includes the arrangement of the database and whether this arrangement involves intellectual creation as this would represent a qualitative investment in the presentation of the database.[251]

4.4.2.6.1.3.1.1.4 Rights and Infringement

Article 7.1 of the Database Directive provides a right for the maker of a database to prevent extraction and/or re-utilisation of the whole or a substantial part of the contents of a database.[252]

Article 7.2 (a) defines the terms 'extraction' and 're-utilisation' as follows:

[245] Recital 7 and 40 of the Database Directive.

[246] Derclaye, The Legal Protection of Databases: A comparative analysis, p. 73.

[247] See for example C-46/02 *Fixtures Marketing Ltd. v. Oy Veikkaus* at [10], [11], [42] and [44],, see also C-444/02 *Fixtures Marketing Ltd v. OPAP* at [40]

[248]C-338/02 *Fixtures Marketing Ltd v. AB Svenska Spel* at [24], For more information see Derclaye, The Legal Protection of Databases, Cheltenham, 2008, pp. 92-93.

[249] Davison, The Legal Protection of Databases, p. 86.

[250] Virtanen, Database rights in safe European home: the path to more rigorous protection of information, pp. 231-232.

[251] Davison, The Legal Protection of Databases, p. 84.

[252] Article 7.1 of the Database Directive.

> (a) 'extraction` shall mean the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form;
>
> (b) 're-utilisation` shall mean any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission.

Furthermore, Article 7.5 states:

> The repeated and systematic extraction and/or re-utilisation of insubstantial parts of the contents of the database implying acts which conflict with a normal exploitation of that database or which unreasonably prejudice the legitimate interests of the maker of the database shall not be permitted.

In this respect, worthy to mention is a rather recent ruling of the European Court of Justice in the *Directmedia* case[253] submitted at the end of 2008, which foresees a rather optimistic panorama for database owners. In this case the ECJ has broadened the scope of protection by making clear the sort of acts which constitute infringement of the database right.[254]

Below we will further expound this case as it might be very relevant for OPTIMIS:

The *Directmedia* case was concerned with the infringing act of "extracting" substantial parts of a database created by a German university professor which included details of the most important poems between the years 1730 and 1900 in the eyes and judgment of the professor[255], together with a team of academics in the University of Freiburg.[256]

The database was different to that in the *British Horserace Board (BHB) v. William Hill* and *Fixture Marketing*[257] cases (see below in the following section) as its content included "pre-existing" material as opposed to the one in the BHB. Therefore, the issue whether data was created or obtained was out of question as the poems could be found by anybody in different texts of literature. The creation of the database clearly represented a substantial investment in terms of effort and time since 1100 poems were chosen from a group of 20.000, using as a reference the frequency they were cited in other publications including relevant information from the author and title of the publication, as well as an opening line and year of publication of each poem. In addition, all the poems were statistically analysed and many poems were categorised in a standard form accordingly. The compilation of this database took 2 and a half years to be completed and the estimated costs were around 35.000 Euros. All in all, it could be

[253] C-304/07 *Directmedia GmbH v Albert-Ludwig Universitat Freiburg* [hereinafter the „Directmedia case"] available at: http://curia.europa.eu/jurisp/cgibin/gettext.pl?lang=en&num=79918990C19070304&doc=T&ouvert=T&seance=ARRET [Accessed 6 October 2010].

[254] Nettleton, ECJ rules on acts of „extraction" that infringe database right, Computer Law & Security Review, ELSEVIER, p. 181.

[255] Ewan Nettleton, p. 182

[256] Ormsby Prentice, Extracting New Value from the Database Right – ECJ Decision in Directmedia Case available at: http://newsweaver.ie/mop/e_article001294984.cfm?x=b11,0,w [Accessed 6 October 2010].

[257] C-203/02 *The British Horse-racing Board (BHB) Ltd v. William Hill Organization Ltd*., (United Kingdom).

confidently concluded that the database represented a substantial investment measured not only in terms of money but considerable time, effort and human resources.[258]

The alleged Defendant, Directmedia Publishing argued that they had not taken substantial parts of the database by the traditional means of copying and pasting but rather admitted to having consulted the anthology of poems selected by the University of Freiburg and therefore have only included a number of entries from the University database of poems which totals 856 poems.[259]

Directmedia Publishing produced at the end a CD-ROM titled "1000 poems everyone should have" therefore representing almost 98% of the content of the University's anthology of poems clearly indicating the breach of extracting a substantial part of the database.

The question whether the infringement constituted a substantial part was not an issue then since 98% clearly indicates the majority of the contents of the database. Indeed, the Regional German Court decided in favour of the German Professor, indicating that the database right was infringed. Nonetheless, when the case was brought to the second instance before the Federal Court of Justice (Bundesgerichtshof), another question arose in the scope of the interpretation of the infringement act of the "extraction" of the content of the database as the alleged defendant argued not to have copied but rather selected them and excluded a number of poems which they considered not to be relevant. In this situation, the German Federal Court chose to rise the following question to the ECJ[260]:

> "can the transfer of data from a database protected in accordance with Article 7 (1) of [Directive 96/9/EC] and their incorporation in a different database constitute an extraction within the meaning of Article 7 (2) (a) of that directive even in the case where the transfer follows individual assessment resulting from consultation of the database, or does extraction within the meaning of that provision presuppose the (physical) copying of data?"[261]

The ECJ, in the light of the Advocate General Sharpston's opinion have clearly rejected a limited interpretation suggested by the German court. In her opinion, the act of transcribing the contents of a database after consultation is equal to the damage produce by copying it by electronic means and therefore prejudices the investment of the maker of the database under similar circumstances.[262]

In this respect, the Advocate General judged the following:

> "'extraction' within the meaning of Article 7 (2) (a) of the Directive does not presuppose the (physical) copying of data. In order to constitute an 'extraction' within the meaning of Article 7 (2) (a) of the directive, it is immaterial whether the transfer of data from a database protected in accordance with Article 7 (1)

[258] Ewan Nettleton, p. 182

[259] Ormsby Prentice, Extracting New Value from the Database Right – ECJ Decision in Directmedia Case available at: http://newsweaver.ie/mop/e_article001294984.cfm?x=b11,0,w [Accessed 6 October 2010]..

[260] Nettleton, p. 183.

[261] C-304/07 *Directmedia GmbH v Albert-Ludwig Universitat Freiburg* at [21].

[262] Nettleton, p. 183.

> of the Directive and their incorporation in a different database takes place following individual assessments of the data after consulting the database".[263]

The ECJ decision in the *Directmedia* case can have a positive impact in the production of databases and their business. It may force competitors to create a database from scratch instead of using a shortcut.[264] The broad interpretation of the ECJ is relevant for the protection of the content of those databases within the Cloud, provided the criteria of Article 7 are met.

4.4.2.6.1.3.1.1.5 The ECJ Decisions and distinction between "creating" and "obtaining" data.

In the year 2004 the ECJ ruled four cases[265] which may have direct impact in determining whether the historical databases or any other database within "the Cloud" fall within the scope of the Database Directive. Each ruling in the four cases refers to similar facts and data in the areas of football and horse-racing. The countries involved were the United Kingdom, Finland, Greece and Sweden.[266] These decisions provide the fundamental guidelines in determining the eligibility criteria for database protection, since it made a distinction between the investment criteria in the 'creation' of data on the one hand, and in the 'obtaining' of data on the other.[267]

The decisions established that investment in the "creation" of data, for instance, by drafting a list of events such as football fixtures and horse-racing schedules, does not qualify for the substantial investment criteria stated in Article 7 (1) of the Database Directive. Therefore, the ECJ denies the protection of those databases where the creator of which has invested only in generating the contained data.[268]

> "Finding and collecting the data which make up a football fixture list do not require any particular effort on the part of the professional leagues. Those activities are indivisibly linked to the creation of those data, in which the leagues participate directly as those responsible for the organisation of football league fixtures. Obtaining the contents of a football fixture list thus does not require any investment independent of that required for the creation of the data contained in that list".[269]

The ECJ clearly establishes a difference between the terms 'creating' and 'obtaining', stressing that the preparation of those football fixtures needs different groups of people (e.g. football clubs, supporters association and police authorities) to organise the events and fixtures. In addition, to create such fixtures different factors are needed, such as making decisions to avoid overlapping of matches, etc.[270]

---

[263] C-304/07 *Directmedia GmbH v Albert-Ludwig Universitat Freiburg* at [59].

[264] Ormsby Prentice, Extracting New Value from the Database Right – ECJ Decision in Directmedia Case, available at: http://newsweaver.ie/mop/e_article001294984.cfm?x=b11,0,w [Accessed 6 October 2010].

[265] Fixtures Marketing Ltd v. Oy Veikkaus Ab C-46/02 (Finland), Fixtures Marketing Ltd v. AB Svenska Spel C-338/02 (Sweden), Fixtures Marketing Ltd v. OPAP Case C-444/02 (Greece), The British Horse-racing Board Ltd v. William Hill Organization Ltd C-203/02 (United Kingdom).

[266] European Commission, DG Internal Market and Services Working Paper: First Evaluation of the Directive 96/9/EC on the legal protection of databases, p. 13.

[267] Gaster, "Obtinere" of Data in the eyes of the ECJ: How to interpret the Database Directive after the British Horseracing Board Ltd. Et al. V. William Hill Organisation Ltd., p. 135.

[268] Davison (2005), p. 113.

[269] Fixtures Marketing Ltd v Oy Veikkaus decision at [44].

[270] *Ibid.* at [10] and [11].

Similarly to those football fixture cases the ECJ adopted an identical approach in the *British Horse-racing Board (BHB) Ltd v. William Hill* case:

> "The resources deployed by BHB to establish, for the purposes of organising horse races, the date, the time, the place and/or name of the race, and the horses running in it, represent an investment in the **creation** of materials contained in the BHB database".[271]

As an analogy, Databases within a Cloud computing scenario can be very complex and significant, containing diverse information for different purposes. For this reason it is relevant to assess whether the data collected in the databases within the OPTIMIS architecture are similar to those databases created by sport fixtures.

4.4.2.6.1.3.1.1.6 Who owns the collection of data?

At the outset it is important to make a distinction between the 'author' and the 'maker' of the database. The first is the person who made the actual database and the latter is the person who invested in the creation of such database.

According to the Database Directive, the "author" of a database shall be the natural person or group of natural persons who created the database or, where the legislation of the Member States so permits, the legal person designated as the right-holder by that legislation.[272]

The 'author' is the person "who made the work possible".[273] That is, the person in charge of preparing the structure and arranging the data of the database. The author will enjoy the so called 'moral rights' which protects non-economic rights.[274] The 'author' is "the person who has created the work in question."[275]

The 'maker' of the database is the person who takes the initiative and the risk of the investment in the obtaining, verifying or presenting the contents of the database, excluding subcontractors in particular from the definition of maker.[276]

There may be several relationships and activities connected with the creation of databases within the OPTIMIS architecture, therefore "joint making" by one person taking the initiative and another taking the risk is possible.[277]

Last but not least, since database right is an assignable property right, it is also possible to grant license rights and license schemes accordingly.[278]

4.4.2.6.1.3.1.1.7 Duration of the Database Right

The database protection lasts for 15 years. Running from the date of completion of the making of the database and expiring fifteen years from the first of January of the year following the

[271] BHB decision at [80].

[272] Article 4 of the Database Directive.

[273] Bently, Intellectual Property Law, p. 115.

[274] Bently, Intellectual Property Law, p. 231.

[275] Bainbridge, Intellectual Property, Fourth Edition, p. 74.

[276] Recital 40 and 41 of the Database Directive.

[277] Bently, Intellectual Property Law, p. 301.

[278] Bently, Intellectual Property Law, p. 301.

date of completion.[279] In case a database is made available to the public in any form before this period, the term of protection by that right shall expire fifteen years from the first of January of the year following the date when the database was first available to the public.[280]

According to Article 10 (3) of the Database Directive, any substantial change, evaluated qualitatively or quantitatively, to the contents of a database, including any substantial change resulting from the accumulation of successive additions, deletions or alterations, which would result in the database being considered to be a substantial new investment, evaluated qualitatively or quantitatively, shall qualify the database resulting from that investment for its own term of protection.[281] Within the context of the historical databases in OPTIMIS, this means that any substantial change in the obtaining, verification or presentation of the contents such as updating of data, or corrections and deletions of old data may grant for another period of 15 years of protection.

4.4.2.6.2 Conclusion

Cloud computing infrastructure creates great challenge from both legal and technical points of view. The different layers within the infrastructure pose a range of copyright issues which can be classified in three main aspects.

Firstly, the OPTIMIS infrastructure envisages many computer programs and different applications, which will allow users to execute their activities in a better fashion. In this respect, we have to refer to Directive 91/250/EC on the legal protection of computer programs. The main provisions of this directive need to be taken into consideration being the originality criteria a general rule requirement in all expressions of the computer programs. Copyrights protection starts automatically when the computer software has been created. It protects the source code and the machine code against mere copying but does not protect the idea as such. Therefore, as long as the adaptations of the software developed are not trivial and a minimum of creativity and originality is demonstrated, the computer programs developed during the course of the project will enjoy copyright protection.

Secondly, copyright protection can be analysed by taking into account the whole picture of a Cloud computing environment. As we have seen there are many layers in a Cloud computing infrastructure e.g. platform, storage capabilities, applications, etc. which are geographically distributed in many different places. In this sense, the way these layers are organised and put together will vary greatly from one Cloud computing environment to another. It follows that the way the OPTIMIS architecture expresses its infrastructure may give rise to copyright protection whether it shows a certain degree of creativity.

Thirdly, taking into account the digital networked nature of Cloud computing, it is subject to copyright infringements, since every time someone wants to send copyrighted material over the network, this may immediately result in electronic copying of the work. While there are some legal exceptions for these situations, it is advisable to acquire the consent of copyright

[279] Article 10 (1) of the Database Directive.

[280] Article 10 (2) of the Database Directive.

[281] Article 10 (3) of the Database Directive.

owners so that the copyrighted works can be safely processed, copied and stored within the Cloud.[282]

Finally, it is clear that Cloud computing needs storage capabilities. Within the Cloud, there are many kinds of databases. They all have different features and components which allow them to store different sorts of data. In order to illustrate this situation in a better way, we have made an analysis of one of the main assets of the project, which is the risk assessment tool where the so called 'historical databases' play an important role.

The question of whether these databases falls under the scope of the definition given by the Database Directive is undisputable, provided that the legal definition is broad enough to include any kind of databases. We have provided an analysis of the main provisions of the Database Directive together with the most relevant cases in light of the ECJ decisions.

While the Database Directive provides protection for those databases showing a qualitatively and/or a quantitatively substantial investment in either the obtaining, verification or presentation of the content of that database, and while the *Directmedia* case expands the scope of its protection, the ECJ decisions in the *BHB* and *Football Fixtures* cases narrowed the interpretation of the term 'obtaining', establishing a difference between the terms 'creating' and 'obtaining' data, concluding that data created does not qualify for the substantial investment criteria stated in Article 7 of the Database Directive.

This is a fundamental question that needs to be assessed on a case by case basis within the databases of a Cloud computing environment. In order to illustrate this situation we have described and analysed the workflow of data within the OPTIMIS risk assessment components where data needs to be stored in the historical databases.

In this respect, from a Service Provider point of view, data will be taken from the SP's dealing history with various Infrastructure Providers (offers accepted, rejected, service failure, etc). This information will be generated and stored within each Service Provider's server. This is envisaged as an automated process without human intervention. Therefore, we arrive at the conclusion that data can be regarded as being created and not obtained, as this data will be taken and analysed in the course of each transaction between the Service Provider and the various Infrastructure Providers.

The same analysis is true in the databases within the Infrastructure Provider. We therefore arrive at the conclusion that database protection in the scope of the Database Directive is hard to achieve. Nevertheless, as they are part of the risk assessor components they will most probably enjoy copyright protection.

4.4.2.7 Summary

In this section we identified whether the Cloud computing accessible databases can obtain either copyrights and/or database rights also known as *sui generis* rights, which aim at protecting the investment. We used the example of the "historical databases" which are part of the risk assessor components in OPTIMIS, which aims at storing "historical data" that enable

[282] See GRIDipedia, The European GRID Market Place available at: http://www.GRIDipedia.eu/GRIDipr.html [Accessed 7 October 2010].

both SPs and IPs to perform a risk assessment when receiving offers from other OPTIMIS enabled stakeholders.

On the one hand, in order to enjoy copyright protection, the decisive factor is the originality criteria (i.e.) the way in which the author of the databases selects and arranges data. On the other, in order to enjoy the *sui generis* right, the decisive factor is to show that there has been a substantial investment in the obtaining, verifying and presenting the content of the database. This assessment need to be done qualitatively and quantitatively. Another decisive factor is the way the data is obtained. If data is "created" while processing the risk assessor components, the historical databases will **not** enjoy the *sui generis* right. However, if the data is "obtained" in a way that is collected from other sources, database owners can enjoy such a right.

4.4.2.8 What OPTIMIS needs to do

In case OPTIMIS wish to obtain:

- **Copyrights:** In order to be eligible for copyright protection a certain degree of originality in the way OPTIMIS databases select and arrange the data needs to be added.

For example: new ways of indexing, querying systems, and clustering data can both improve the usability potential of a database and at the same time add a quota of originality. Different tools and applications, new ways of grouping documents into different categories (in row, columns, etc and in different subjects and fields) coupled with the creativity of the author of the database can both improve the performance of databases and provide the minimum necessary criteria to obtain copyright protection. Therefore, it is advisable to add a certain degree of human intervention, as the creativity of the author is needed to comply with the originality criteria. If such requirements are not met i.e. if the given database consists of the typical standard and routine selection and arrangement e.g. in alphabetical order then the database would not obtain copyright protection.

- ***Sui generis* right:** In order to obtain the *sui generis* right, it is necessary to show there is a substantial investment in obtaining, verifying and presenting the content of the database. In the same vein, it is therefore advisable to have a certain degree of human intervention involved.

For example: historical databases within the risk assessment components could have the possibility to add human assistance during the operation of the databases in e.g. verifying whether the data is accurate and/or in presenting the content of the database. By doing this, it could be argued that there is an investment measured in terms of effort, time and human resources in the way the data is verified and presented in the database and as a corollary (it) obtains the *sui generis* right. (unsure of desired meaning)

In addition, as to solving the question of whether data is "created" or "obtained" what OPTIMIS could do is devise a legal and economic strategy to circumvent this. For instance, as for the historical databases within the Risk Assessor Components, concerns are taken into consideration that the "historical databases" will be located with each provider. On the one hand, data could be kept secret with all necessary measures of access control in each database. On the other, another database which is a mirror of the historical databases could be

created in a way that human resources could "obtain" the data and present it in a different way.[283]

Results:

As a result, taking into account that databases play an important role in a Cloud computing environment and as these databases e.g. historical databases in OPTIMIS become more and more valuable to the cloud provider as they contain useful information about previous collaborations with other cloud providers, clarifying these copyright issues as well as access rights and the use of the given databases is a must.

In addition, if the *sui generis* right is achieved, it will enable the owner of the database to have a legal protection against the unauthorised acts of copying and distribution to the public, and then being able to license the whole or parts of the content of the database to another cloud provider.

4.5 Analysis of Green Legislation relevant to OPTIMIS

4.5.1 Introduction

Rising global warming, increased energy costs and its socio-economic implications have motivated the OPTIMIS project to optimise the consumption of electricity and to reduce the CO_2 (carbon) emissions.

According to the European Parliament resolution of 4 February 2009 on the challenge of energy efficiency through information and communication technologies, the ICT sector represents about 2% of the current global CO2 emissions.[284] The ICT industry in comparison to other industry sectors together with the research community has potentially the ability and the tools to reduce its direct CO2 output and therefore one of the main objectives of the OPTIMIS project is to help to achieve this goal. Governments are struggling to find a solution on how to reduce CO2 emissions and many ideas to enforce this have been submitted.[285] The 'carbon footprint' which is the amount of greenhouse gas emission an organisation produces is calculated by the assessment of the total energy usage, including all components of the organisation's operation which consume power or generate waste and by-products.

We acknowledge that the ICT industry in comparison to other industry sectors has potentially the ability to reduce its direct CO2 output and reduce energy costs. This is particular relevant to the business sector not only for ecological reasons but mainly economical. That is, as businesses are using a lot of energy in their datacentres this is also costing them a lot money. In addition, the new concept of corporate social responsibility has switched to a rather more

[283] See for instance Davison/Hugenholtz, Football fixtures, horse races and spin-off: The ECJ domesticates the database right, EIPR, 2005, 27, pp.113-118

[284] Recital G of the European Parliament resolution of 4 February 2009 on the challenge of energy efficiency through information and communication technologies, available at: <URL:http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0044+0+DOC+XML+V0//EN> [Accessed 29 August 2010].

[285] For a thorough global assessment of strategic opportunities for information and communication technology solutions that can help speed the reduction of CO2 emissions see: Buttazzoni,,WWF Sweden Report, "The potential global CO2 reduction from ICT use: Identifying and assessing the opportunities to reduce the first billion tonnes of CO2", 2008, pp. 1-109.

environmental responsibility. Company managers and other stakeholders prefer to deal with those companies which are in line with those legal issues involved. Therefore, ene of the main objectives of OPTIMIS is to help to achieve this goal. For these reasons, the EU and its Member States are struggling to find a solution and many ideas to enforce this have been submitted.

According to a communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, addressing the challenge of energy through Information and Communication Technologies, there is a top priority to develop a sustainable integrated European climate and energy policy package to guide the EU towards a competitive and secure economy while promoting energy savings and climate-friendly energy sources. Current trends are unsustainable as it is foreseen that there will be a rise of 25% of the final energy consumption in the EU by the end of 2012 if nothing were to change. This means that the European policy of economic growth needs to transform into a low-carbon and high energy-efficiency economy and detached from energy consumption.[286]

Within the OPTIMIS project life cycle, one of the main components which plays a key role as far as the whole infrastructure concerns, are "servers" and "data centres". If we were to consider all the servers installed around the world including all their energy consumption together with their necessary infrastructure such as their cooling system, uninterruptable power supply, etc. it can be estimated that worldwide energy consumption by servers rose from 58 billion KWh in 2000 to 123 billion KWh in 2005. These figures reflect about 1% of the total amount of energy consumption in the world.[287]

4.5.2 The United Nations Framework Convention on Climate Change

The United Nations Framework Convention on Climate Change (UNFCCC) was adopted in New York on 9th May 1992. The main purpose was to gradually stabilise greenhouse gas emissions in a way convenient to the promotion of sustainable development in a cooperative and supportive open international economic system.[288] The UNFCCC entered into force on 21 March 1994. Currently, 196 States have ratified the Convention including all the EU Member States.[289]

The Convention categorises countries (or "Parties") taking into account varying commitments. Annex I contain a list of the industrialised countries ("Parties"). The list includes all European Member States which committed to reduce their level of CO2 emissions.[290]

---

[286] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Addressing the challenge of energy efficiency through Information and Communication technologies*, Brussels, 13.5.20087 COM(2008) 241 final, p. 2.

[287] Federal Ministry for the Environment, Nature Conservation and Nuclear Safety (BMU),, "Energy Efficiency Data centres, Best Practice Examples from Europe, the USA and ASIA", 2008, p.6.

[288] Generalitat de Catalunya, Climate Change Website, The United Nations Framework Convention on Climate Change, available at: <URL:http://www20.gencat.cat/portal/site/canviclimatic/menuitem.75e3e8b36ded92ae9b85ea75b0c0e1a0/?vgnextoid=55f884a0883d7210VgnVCM1000008d0c1e0aRCRD&vgnextchannel=55f884a0883d7210VgnVCM1000008d0c1e0aRCRD&vgnextfmt=default&newLang=en_GB> [Accessed 29 August 2010].

[289] Generalitat de Catalunya available at: <URL:http://www20.gencat.cat/portal/site/canviclimatic/menuitem.c4833b494d44967f9b85ea75b0c0e1a0/?vgnextoid=2b7484a0883d7210VgnVCM1000008d0c1e0aRCRD&vgnextchannel=2b7484a0883d7210VgnVCM1000008d0c1e0aRCRD&vgnextfmt=default> [Accessed 29 August 2010].

[290] *Ibid.*

4.5.3 The Kyoto Protocol

The first international relevant piece of legislation is the so called Kyoto Protocol which constitutes a landmark in terms of climate change legislation. In December 1997 members of the United Nations gathered in Kyoto to seek a global agreement on how to deal with the implications of the rise of CO2 emissions and which steps are necessary to reduce it. As carbon dioxide is gas produced through the burning of the main energy sources for most people in the world such as wood, coal and hydrocarbons mostly produced in industrialised countries, the Kyoto Protocol seeks a balance between those developed or industrialised countries which produces more carbon emissions and developing countries which produces less carbon emissions. This is in order to promote economic growth with the provision and commitment that they will face restrictions in the near future.[291]

The most important feature of the Kyoto Protocol is that it establishes binding targets for 37 industrialised countries, including the European Community, for lowering greenhouse gas (GHG) emissions. This is due to the reason that developed countries are mostly responsible for the actual level of GHG emissions as a consequence of their industrial activity.[292]

4.5.4 OECD Guidelines - Recommendation of the Council on Information and Communication Technologies and the Environment

The Organisation for Economic Co-operation and Development (OECD) is a forum of 30 countries[293] which cooperate together to find solutions and exploit opportunities, while addressing economic, social and governance challenges of globalisation.[294]

Taking into account that the OECD aims at building a "stronger, cleaner, fairer world economy", and as indicated in the Ministerial Declaration on Green Growth[295] special efforts and international cooperation are essential for the development of clean technology including reinforcement of green Information Communication Technology (ICT) this "Recommendation" focuses on governmental policy and environmental performance, including the raising of public awareness, the improvement of business performance and the change of consumer behavior.

The OECD Guidelines have established a check list of principles which provide Members states a general framework for enhancing the contribution of information and communication technologies to improving environmental performance.

---

[291] Global warming, *Global warming: Kyoto and its implications*, available at: <URL:http://earthguide.ucsd.edu/globalchange/global_warming/02.html> [Accessed 25 July 2010].

[292] UNFCCC, Kyoto Protocol, available at: <URL:http://unfccc.int/kyoto_protocol/items/2830.php> [Accessed 29 August 2010].

[293] Current OECD countries are: Australia, Austria, Belgium, Canada, Chile, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States. For more information see: <URL:http://www.oecd.org/pages/0,3417,en_36734052_36761800_1_1_1_1_1,00.html> [Accessed 29 August 2010].

[294] The OECD brochure available at: <URL:http://www.oecd.org/pages/0,3417,en_36734052_36734103_1_1_1_1_1,00.html> [Accessed 29 August 2010].

[295] Declaration on Green Growth (C/MIN(2009)5/ADD1/FINAL) adopted at the Council Meeting at Ministerial level on 25 June 2009.

The OECD Guidelines recommend to coordinate ICT policies in conjunction to climate, environment and energy policies in order to improve environmental performance, sustainable resource management, tackle climate change and enhance energy efficiency; thus aiming at bridging together all the stake holders including policy makers and other experts in the field of ICT, climate, energy and environment.[296]

The OECD Guidelines support research and innovation in green technologies and services being one of the key recommendations relevant to our discussion that "Members should support long-term basic research, and where possible stimulate research and development in resource-efficient ICTs and "smart" applications for example through technology-neutral tax incentives or carbon offset mechanisms, and encourage user-driven innovation…".[297]

Recital 6 of the OECD Guidelines establishes that Members should encourage best practice mechanisms as follows:

> "Members should encourage the wide sharing of best practices to maximise the diffusion of green ICTs and "smart" ICT-enabled applications in the public and private sector, including governments, businesses, civil society and regional and international organisations. They should exchange information and good practices on how to ensure data protection, security and privacy in "smart" ICT-enabled applications. They should themselves share good practices in measuring economic and social environmental impacts of ICTs and ICT-enabled applications. Finally, they should use these principles to review and collect information on national policies and initiatives and exchange information on policy development".[298]

4.5.5 European Policy

The EU was part of many climate change initiatives, starting in 1991 with its first Community strategy to restrict carbon dioxide emissions, followed by the signature of the Kyoto Protocol on 29 April 1998. By the end of May 2002, all EU member states committed to the ambitious plan of reducing CO2 emissions by 8% between 2008 and 2012 with respect to the baseline in the year 1990.[299]

For this reason, the EU has taken several strict measures in order to accomplish this plan which lies in the European Climate Change Programme and the EU greenhouse gas emissions trading scheme.[300] By the end of 2008, the EU implemented an Integrated Climate Change and Energy

[296] Recital 1 of the OECD Recommendation of the Council on Information and Communication Technologies and the Environment, 8 April 2010, C(2010) 61, available at:

<URL:http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=259&Lang=en&Book=False> [Accessed 29 August 2010].

[297] *Ibid* at Recital 3.

[298] *Ibid* at Recital 6.

[299] Generalitat de Catalunya, European Policy, available at:

<URL:http://www20.gencat.cat/portal/site/canviclimatic/menuitem.daafef89898de25e9b85ea75b0c0e1a0/?vgnextoid=e6e11df5e87d6210VgnVCM1000008d0c1e0aRCRD&vgnextchannel=e6e11df5e87d6210VgnVCM1000008d0c1e0aRCRD&vgnextfmt=default&newLang=en_GB> [Accessed 29 August 2010].

[300] Ibid.

Policy aiming at reducing 20% of energy consumption through energy efficiency mechanisms and lowering greenhouse gas emissions by 20% (and to 30 % when international agreements take place).[301]

4.5.6 The European Union Greenhouse Gas Emission Trading System (EU ETS)

The EU Greenhouse Gas Emission Trading System (EU ETS) is based on Directive 2003/87/EC, which entered into force on 25 October 2003. This Directive is well suited to the United Nations Framework Convention on Climate Change and the Kyoto Protocol.[302] In January 2005 the EU ETS started to operate as the biggest multi-country, multi-sector Greenhouse Gas Emission Trading System world-wide. The EU ETS system places a Central Administration at EU level which is in charge of checking each transaction through the "Community Independent Transaction Log"[303]. In order to keep a close track of the ownership of the allowances traded in the EU, ETS uses the same process as that of a bank which keeps track of the ownership of money.[304]

The EU ETS is the first international trading system for CO2 emissions with coverage of more than 10.000 installations in the energy and industrial field. All in all, it covers almost 50% of Europe's carbon emissions.[305]

The EU ETS established a trading currency scheme based on emission allowances. According to Article 3 (a) of the EU ETS Directive 'allowance' means "an allowance to emit one tone of carbon dioxide equivalent during a specified period, which shall be valid only for the purposes of meeting the requirements of this Directive and shall be transferable in accordance with the provisions of this Directive".[306] One allowance equals one tone of CO2 i.e. the right holder of one allowance has the right to emit one tone of carbon. In order to implement this at national level, EU member states must design a so called National Allocation Plan (NAP) for each trading period under the ETS scheme. Within each NAP there is a limit or "cap", on the total number of allowances granted. This system creates a limited number of allowances which can be tradable in the market. For instance, companies which manage to keep their carbon emissions below the level of allowances can sell their surplus of allowances thus economically profit from them. Conversely, companies using their carbon allowances to the limit will need to purchase more allowances or take any other measures to reduce their carbon emissions, such as investing in new energy efficient technology or using less carbon-intensive sources of energy. Companies may choose one or combine the best economical and ecological mechanisms.[307]

The allowance system operates in a way that each member state has to prepare and publish, under the terms of the Emission Trading Directive, a NAP for each period. Currently we are in

[301] Ibid.

[302] Recital 22 of Directive 2003/87/EC.

[303] European Commission, Community Transaction Log, available at: <URL: http://ec.europa.eu/environment/ets/> [Accessed 29 August 2010].

[304] European Commission, Emission Trading System, available at: <URL:http://ec.europa.eu/environment/climat/emission/index_en.htm> [Accessed 29 August 2010].

[305] MEMO/06/452, Brussels, Nov. 2006, Questions and Answers on Emissions Trading and National Allocation Plans for 2008 to 2012, p.1.

[306] Article 3 (a) of the EU ETS Directive.

[307] MEMO/06/452, Brussels, Nov. 2006, p.1.

the 2008-2012 period, therefore as indicated there is a limited number of allowances in the market.[308]

The way of assessing the allocation plans is related to the Kyoto Protocol and each Member State's Kyoto target. The European Commission is in charge of assessing the allocation plans based on 12 criteria set in Annex III of the Emission Trading Directive. Within the scope of the preparation of the NAP, member states can use any of the Kyoto mechanisms to buy emission credits through any of the international emission trading systems.[309]

4.5.7 European Parliament Resolution of 4 February 2009 on the challenge of energy efficiency through information and communications technologies

The European Parliament resolution of 4 February 2009 on the challenge of energy efficiency through information and communication technologies [hereinafter "the Resolution"][310] aims at increasing awareness for ameliorating energy efficiency in the EU, by acknowledging the importance of ICTs in meeting this objective.[311]

The Resolution calls on the Commission and Member States to commit to increase awareness (for instance through demonstration projects), "of the importance of ICTs for improving energy efficiency in the EU economy and as driving forces behind increased productivity and growth and cost reductions that make for competitiveness sustainable development of EU citizens' quality of life".[312]

Even though the Resolution is not a legally binding document, it is very relevant as it makes the topic of ICT and its influence in combating and adjusting to climate change one of the top priorities in the forthcoming Council Presidencies.[313]

Furthermore, it calls on the Commission and the Member States to take energy efficient actions from a holistic point of view i.e. taking into account not only technical components separately but the entire systems including those necessary legislative changes.[314]

The Resolution also encourages Member States to gradually reduce CO2 emissions through the implementation of green strategies based on the use of ITs and ICTs,[315] and urges them to develop an action plan to decrease the consumption of energy through further use of green procurement and ICT solutions for the public sector.[316]

---

[308] *Ibid* at p.2.

[309] *Ibid* at p.2.

[310] European Parliament resolution of 4 February 2009 on the challenge of energy efficiency through information and communication technologies, available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0044+0+DOC+XML+V0//EN [Accessed July 8 2009].

[311] Joint Parliament Meeting, Towards a European Energy Community for the 21st Century?, European Parliament Brussels, June 2010, p. 3.

[312] Numeral 1 of the Resolution.

[313] Numeral 2 of the Resolution.

[314] Numeral 3 of the Resolution.

[315] Numeral 4 of the Resolution.

[316] Numeral 5 of the Resolution.

The Resolution put emphasis on lowering carbon emission and encourages the promotion of financial incentives for smart grid technologies which uses 'advanced remote sensing' that helps "to reduce energy losses by identifying leakages, blockages or other problems in major energy infrastructures".[317]

In addition, calls on the Member States to facilitate new business models, specially within the energy market, and the economy as a whole, in connection with electronic trading in energy, through the abilities and potential of ICTs.[318]

Generally speaking, the Resolution mentions the implementation of new technologies in a range of different sectors such as the automotive industry, construction of buildings, etc. Relevant for the OPTIMIS project is Numeral 25 which encourages the ICT industry in lowering its "carbon footprint by complying with the highest efficiency and innovation standard through entire product lifecycles…recommends, further, the use of software and operating systems that consume the least energy".[319]

Finally, the Resolution calls on the Commission and the Member States to improve the regulation framework in a rather more supportive and favourable way for a better access to finance of SMEs, which can play a key role in implementing ICT-based solution for energy efficiency.[320]

4.5.8 Directive 2005/32/EC on the eco-design of Energy-using Products (EuP)

The EcoDesign of Energy using Products (EuP) Directive (2005/32/EC)[321] [hereinafter the EcoDesign Directive] was adopted on 11 August 2005 and was extended to embrace Energy related Products (ErP) on 20 November 2009 (2009/125/EC). The aim of this Directive is to decrease the environmental impact of a wide range of energy using products all the way through their life cycles.[322] It sets up a framework for the background of the Community ecodesign requirements for energy-using products (EuP), aiming at ensuring the free movement of those products within the EU internal market.[323]

The scope of the EcoDesign Directive is very broad as it includes products that use any kind of energy inter alia electricity, fossil fuels or renewable energy sources including products used for generation, transfer and measurement of energy.[324]

The EcoDesign Directive contains 19 different sections for a wide variety of devices. Section 7 regulates the "external power supplies". The provisions within this section aims to protect the environment by forcing the manufacturers of electric and electronic products to maintain a

[317] Numerals 7-8 of the Resolution.

[318] Numeral 10 of the Resolution.

[319] Numeral 25 of the Resolution.

[320] Numeral 27 of the Resolution.

[321] EcoDesign Directive 2005/32/EC, the Amending Directive 2008/28/EC and EcoDesign Directive 2009/125/EC available at: <URL:http://ec.europa.eu/enterprise/policies/sustainable-business/documents/eco-design/framework-directive/index_en.htm> [Accessed 29 August 2010].

[322] Cobham, EcoDesign Directive Compliance Service, available at: http://www.era.co.uk/Services/ecodesign.asp [Accessed 25 October 2010].

[323] Kemna, et al., Methodology for Ecodesign of Energy-using Products (EuP), The Netherlands, 2005, p. 1.

[324] Cobham, EcoDesign Directive Compliance Service, available at: http://www.era.co.uk/Services/ecodesign.asp [Accessed 25 October 2010].

certain level of energy efficiency thus saving money, lowering carbon emissions and protecting the environment.[325]

The scope of the EcoDesign Directive might be of relevance for OPTIMIS as there are different categories of products under revision by the Commission. Until now, more than 40 categories have been scrutinised ranging from large volume products to large energy users in industry.[326]

It is therefore relevant for OPTIMIS to take the provisions of the EcoDesign Directive as this will not only facilitate legal compliance but can also bring down costs and increase the sales opportunities as a "green" product.[327]

4.5.9 Directive 2008/101/EC and Directive 2009/29/EC and current implementation into national law

Between November 2008 and April 2009 two new European Directives have been approved which reform substantially the European Trading System. On the one hand, Directive 2008/101/EC amends Directive 2003/87/EC so as to include aviation activities in the scheme for greenhouse gas emission allowance trading within the Community.[328] On the other hand, Directive 2009/29/EC[329] amends Directive 2003/87/EC (The EU ETS Directive) so as to improve and extend the greenhouse gas emission allowance trading scheme of the Community.

Directive 2008/101/EC is not going to be discussed in this document as this is not relevant for the OPTIMIS project. However, Directive 2009/29/EC is applicable as it takes part in the so called community legislation package on energy and climate change, whose main purpose is to launch a series of measures to ensure compliance with the European Council commitment of March 2007, to reduce global emissions of greenhouse gases in the Community to at least 20% and to 30%, as long as other countries commit themselves to a comparable reduction adequately according to their responsibilities and capabilities.[330]

According to Directive 2009/29/EC requirements from January 2013, the amount of allowances is determined at EU level. The calculation and publication of this amount corresponds to the European Commission, in accordance with the requirements of the Directive 2009/29/EC. The total volume of rights is determined using the allocation procedure to be adopted in all Member States for 2008-2012. It starts from the midpoint of the period, and annual and linearly

[325] Ansmann, EcoDesign Directive, available at:

http://www.ansmann.de/cms/businessdivision/consumroot/chargers-and-power-supplies/power-supplies/ecodesign-directive-eup.html [Accessed 25 October 2010].

[326] A summary of the status of the implementing measures can be found at the following site: http://www.era.co.uk/services/eco-design-status.asp [Accessed 25 October 2010].

[327] Cobham, EcoDesign Directive Compliance Service, available at: http://www.era.co.uk/Services/ecodesign.asp [Accessed 25 October 2010].

[328] Directive 2008/101/EC of the European Parliament and of the Council of 19 November 2008 amending Directive 2003/87/EC.

[329] Directive 2009/29/EC of the European Parliament and of the Council of 23 April 2009 amending Directive 2003/87/EC so as to improve and extend the greenhouse gas emission allowance trading scheme of the Community available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0029:en:NOT [Accessed 25 October 2010].

[330] See <URL: http://noticias.juridicas.com/base_datos/Admin/l13-2010.html> [Accessed 29 August 2010]

decreases 1.74%. This corresponds approximately to a 21% reduction in 2020 compared to 2005 for all sectors affected by trade in emission rights.[331]

Both Directives, in particular the latter, formed the basis for major improvements and reforms at national level. For this reason, we think it is relevant to go through the current situation in Europe and in particular to assess the domestic green legislation of those countries where the OPTIMIS project will be more engaged in developing its technical infrastructure e.g. United Kingdom, Germany, Spain and Sweden. Respectively, these countries will be analysed in the forthcoming Report. Noteworthy to mention is the recent United Kingdom's Carbon Reduction Commitment Energy Scheme (CRC) which began its introductory phase in April 2010.

The CRC is a mandatory cap and trade scheme for public and private UK organisations based in the United Kingdom, supplementing the Climate Change Agreement (CCA) and the EU ETS.[332] However, unlike the EU ETS, the CRC targets emissions from energy use rather than emissions from energy production,[333] placing carbon use responsibility on a broader consumer base.
Only organisations whose energy consumption meets a certain threshold must participate in the CRC,[334] and participation requirements are split into two categories depending on the amount of electricity that a given organisation consumes. Those meeting only the initial threshold consumption figure must report their energy use; however, full participants[335] must both record and monitor CO_2 emissions as well as purchase allowances equivalent to their emissions allowances each year.[336]
The UK is the first country in Europe taking the CRC into account. However, this commitment is likely to spread all over Europe[337]. This is the reason why we consider it relevant to collate these legal requirements and other current trends at national level in the next Report.

4.5.10 Non-Legislated Data Centre Energy Initiatives

4.5.10.1 Introduction

There are numerous areas of environmental and energy efficiency related legislation, mostly emerging, which could have some impact on the provision of datacentre and cloud services. However alongside these laws, there are a large number of de facto standards, metrics and industry initiatives which are having, or will likely have, a direct and in some cases very immediate bearing on how data centre operators manage and report on their energy efficiency. In most cases, these rules and benchmarks do not have any direct legal weight; however, this

[331] Recital V <URL: http://noticias.juridicas.com/base_datos/Admin/l13-2010.html> [Accessed 29 August 2010]

[332] At least 90% of [an organization's] total footprint emissions must be regulated either by CRC or by EU ETS or CCAs. For more information see; *The CRC Energy Efficiency Scheme: User's Guide*, p. 32, available at:

<URL:http://www.decc.gov.uk/assets/decc/what%20we%20do/a%20low%20carbon%20uk/crc/1_20100406154137_e_@@_21934crcpdfawv9.pdf> [Accessed 29 August 2010].

[333] European Commission Memorandum State aid N 629/2008 – United Kingdom CRC (Carbon Reduction Commitment), p. 2., available at: <URL:http://ec.europa.eu/community_law/state_aids/comp-2008/n629-08.pdf> [Accessed 29 August 2010].

[334] *Id.* at 11. All organizations that had at least one half hourly meter settled on the half hourly market in 2008 are required to do something under the CRC.

[335] *Id.* Full participants are those who's 2008 annual energy supply through all HHMs was at least 6,000MWh.

[336] *Id.* at 6.

[337] Rachel A. Dines (2010), *From London To Munich – Where To Collocate Your Data centre? And With Which Provider?*, p. 5.

may change in the coming decade as legislation spreads. Furthermore, it is likely that many of these de facto standards will either form the basis of new laws and rules, or will be adopted by powerful buyers and incorporated into procurement documents. This could have the effect of making the adoption of these standards mandatory, in the sense that suppliers have no choice but to conform if they wish to be considered for business.

An example of this is the US Executive Order 13423, which mandates that 95% of the equipment that Federal Government departments buy must conform to the EPEAT standard for energy efficiency and environmental standards. Although EPEAT is not a law, the purchasing power of the Government effectively mandates its adoption by suppliers.

In the context of the energy efficiency considerations as represented in the OPTIMIS project, it may be necessary – or advisable – for reference to these standards and benchmarks to be made, either in the data collection stage, the runtime environments and the service level agreements. It is possible that some procurers would not be able to place contracts without reference to these standards.

A second consideration, discussed in work package 4.1 on data collection, is that most datacentre/IT operators do not have the technology installed to make granular or real time measurements of their energy use – nor are they likely to for many years. It may therefore be a sensible strategy for OPTIMIS to adopt some badging or certification schemes that service or platform providers can demonstrate conformance and energy efficiency by reference to these standards.

If a check box or drop list for conformance to such standards is incorporated in the OPTIMIS tool, these fields should be editable and extensible by the user, as they are likely to change over time. At present, conformance to energy efficiency or carbon standards cannot be verified electronically (i.e by web service), although in some cases conformance is available on text based web pages.

4.5.10.2 Datacentre energy and carbon ratings

4.5.11.2.1 Energy efficiency metrics

In its relatively brief history, PUE (Power Usage Effectiveness) has emerged as the de facto metric for measuring the efficiency of datacentres. Formulated by the Green Grid, an influential international group made up of vendors and some end-users, the metric has been widely adopted in spite of its obvious limitations. PUE is discussed in more detail in work package 4.1, regarding energy efficiency data collection. Its significance in the legal areas relates to its use in procurement documents for datacentre services, and in some cases in planning regulations related to datacentres.

The PUE ratio is also commonly expressed as a percentage, known as DCIE (datacentre infrastructure efficiency), based on its mathematical reciprocal (i.e PUE of 1.5 equals 50% efficiency).

The PUE of a datacentre is a ratio derived from dividing total data centre power by IT equipment power. The closer to 1 the result (i.e the lower the figure, as figures below 1 are not possible), the more energy efficient the data centre. It is widely acknowledged there are many limitations – most notably the PUE only applies to the efficiency of power, cooling and facilities, and says nothing about the efficiency or otherwise of the IT equipment or how it is being used.

Furthermore, high availability datacentre designs are usually necessarily less energy efficient,

which the simple ratio fails to register. Another challenge is that PUE measurements relate to single datacentres – averages of many datacentres may be misleading.
In spite of this, PUE is very widely used and is making its way into regulations and laws. Japan, the European Commission and the United States announced in April 2010 that all three governments would adopt PUE as their official datacentre energy efficiency metric. This lays the groundwork for deeper penetration of PUE requirements into planning codes in particular. Some jurisdictions have already gone down this road. Amsterdam sets a maximum design PUE of 1.3 as a planning permission criterion. Zurich goes a step further, reserving the right to withhold an operating permit if a new datacentre fails to achieve a 1.4 PUE in service. The PUE metric is also used in the European Code of Conduct (CoC), which could also find its way into laws or procurement documents at some stage. Furthermore, many datacentre service providers now report that customers are asking PUE numbers in procurement documents. It should be stressed that there is no regulatory agency that monitors or certifies PUE ratings, and therefore the figures, widely cited, have no legal status, and are prone to distortion by technical and marketing staff.

4.5.11.2.2 Other metrics

At present, there are multiple metrics that have been proposed or are being considered that provide either a fairer measurement of datacentre energy efficiency, or they measure some other aspect (such as IT equipment efficiency, use of renewable power, reuse of waste heat. Such measurements will be discussed in more detail in WP4. However, at present, none of these metrics looks as though they will be widely adopted.

Comment regarding OPTIMIS: PUE measurements are now being mentioned in planning codes, procurement documents and codes of practice; it is very likely that this will extend into cloud services. It is therefore advisable that OPTIMIS considers introducing a simple mechanism for the sharing of PUE data. However, given that PUE data is necessarily crude and incomplete, the use of this metric should be treated with caution.

4.5.10.3 Datacenter Facility Sustainability Ratings

While the US EPA Energy Star system, and the European DC COC rate the energy efficiency of the IT, heating, ventilation and cooling elements of a data centre, other systems exist to consider the sustainability of the whole physical facility. Such Green building standards have a wider remit, covering energy, carbon, resource use (including through the supply chain) and the impact of the building on the local and wider community and on the people who work in or near it. The most popular of these standards are BREEAM and LEED.

4.5.10.3.1 LEED

LEED (Leadership in Energy & Environmental Design) standard is the de facto measure of building project sustainability in the US. Developed by the US Green Building Council (USGBC), the rating attempts to classify and certify building projects according to their overall sustainability.
LEED is a point-based system by which building projects earn points for satisfying specific green building criteria which include water efficiency, energy & atmosphere, materials & resources, Indoor environmental quality, and innovation in design. Facilities are then certified as Sliver, Gold or Platinum depending on points scored. As well as the one-off certifi-

cation process, LEED for Existing Buildings: Operations & Maintenance is an additional scheme which allows the on-going sustainability of a facility to be measured. Unfortunately, although some datacentres have sought certification, LEED is not widely applicable to computing facilities. However a datacentre specific adaption is in the final stages of development.

4.5.10.3.2 BREEAM

Outside the US, the UK-developed Building Research Establishment Environmental Assessment Method (BREEAM) standard is widely used. BREEAM, like its younger US cousin LEED, is a points-based system for rating buildings. It is, however, more flexible, in that those seeking certification can select or deselect criteria according to how appropriate they are to certain buildings. It supports the development of bespoke templates that are function-specific. This has made it easier for BRE Global, the approvals and certification body that manages BREEAM, to introduce a new data centre standard. The new datacentre specification focuses on buildings with few employees, with high energy use and where factors such as air quality and natural daylight are less important.

Comment regarding OPTIMIS: While BREEAM and LEED may not provide IT infrastructure energy efficiency data directly, they could be useful to OPTIMIS by providing a quantifiable rating for a service providers' facilities. This would not directly relate to energy efficiency of computer systems but would provide a specific rating - either in numerical figures or "silver", "gold" or "platinum" - which identify how sustainable a facility being used to handle a cloud work-load or project is seen to be. If deemed suitable, the LEED or BREEAM ratings of a providers non-IT facilities could also be included to give an overall picture of organisational sustainability.

4.5.10.4 Low carbon sources of Power

Large datacentres face a multiplicity of challenges related to their electricity use: these include the scale of their consumption; the availability of reliable sources; the need for uninterrupted supply; increasing prices and electricity related operating costs; and, of course, the environmental footprint, primarily in terms of C02 emissions associated with power production and consumption.

All of these factors are expected, over time, to encourage the increasing use of off-grid energy sources, and renewable energy sources, both off-grid and on-grid. Because some of these energy sources will have a much lower carbon content than others, buyers of datacenter services may seek out datacenter operators that use renewable or low carbon energy sources. This will be especially true of purchasers with stringent low carbon targets (many large companies do so - many of these targets can be viewed at the Carbon Disclosure Project web site at www.cdproject.net/) or organisations that have been mandated to purchase from low carbon suppliers.

For these reasons, there may now be emerging a requirement for datacenter service providers to quantify and certify the carbon emissions associated with the power they use and the services they deliver. In addition (see section below on carbon reporting), many organisations are seeking to understand the environmental impact of their entire supply chain, and so may seek out this data for reporting purposes.

Reporting on the carbon content of power is fraught with difficulties, legal and technical, and most attempts to do so will ultimately involve making compromises on the accuracy of the data (see work package 4.1 on energy use data collection). However, as legislation and environmental issues builds, some form of information relating to the carbon content of energy consumed is likely to be required.

- Grid energy sources.

Although the carbon content of grid power can vary widely, most electricity is either classified as “renewable” or “non-renewable”. There is some debate over nuclear power, but it is not usually classified as renewable (although it does have a very low carbon content), and utilities therefore there is no need to buy credits for it under the European Emissions Trading scheme.

In order to claim they are providing a completely non-carbon service, datacenters may purchase renewable power. This can be done in two ways: first, they can buy renewable energy certificates (RECs) from the utility supplier. The money from these goes, ultimately, to the generators of renewable power who supply the grid. Utilities in most countries, certainly in Europe, have a legal requirement to buy a certain amount of renewable power, and therefore RECs or ROCs (renewable obligation certificates) are legally recognised.

As well as purchasing from the grid, datacentres may also tap into local existing renewable energy sources that are also supplying the grid. This local source of power - for example, from a nearby hydro-plant or combined heat and power generator, may not necessarily involve RECs.
A further complication is that some datacenter operators claim to have low or no carbon emissions, because they buy carbon offsets to cancel out the carbon emissions associated with their energy use. In most cases, these offsets are voluntary and the certification process has no legal status.
Recently, it has been suggested that the distinction between “renewable” and “non renewable” is too simple, since most utilities use a mix of generating sources. A more accurate approach is to incorporate the average annual carbon figure per Kwh of electricity into any model of carbon emissions - this data is available from the energy supplier. This approach may provide a better numerical base for measuring the carbon content of power used for datacenter services. In the future, it may be possible to access this data from web services or from a signal supplied across the Smart Grid from the utility company.

- Microgeneration.

Another option for datacentres is to use micro-generation or off-grid sources. These include the use of local or even on-site wind turbines, fuel cells, solar panels or hydroelectric power the facility. The use of on-site generation, other than using traditional diesel generators for emergency standby, is very rare among datacenters. However, there are some examples, and it is likely to become more common.
Where datacenter operators use local renewable generation, they will want this represented in any carbon or efficiency rating that they give to their services. At present, there is no recognised means of doing this (microgeneration is not covered under the UK Carbon Reduction

Commitment, for example, it is a cause of much contention). However, the Green Grid is working on an extension to the PUE metric that will take into account any clean energy generated locally.

Comment regarding OPTIMIS: There is currently no legal or statutory method for assessing the true or estimated carbon content of power supplied to datacenters. However, estimates are easily available and very useful for simple models (see work package 4.1). The use of renewable energy certificates would provide a credible way of proving the low carbon emissions of a datacenter service; carbon offsets are more problematic, but mechanisms should be considered that enable datacentre providers to use these. The use of the Green Grid microgeneration metric will be tracked for possible use in the future.

4.5.10.5 Carbon Footprint datacenters and companies

While legislation is increasingly forcing large emitters of carbon to report their emissions, many organisations, including smaller producers not covered by legislation, are beginning to voluntarily track their GHG (greenhouse gases) levels in anticipation of tighter rules. This includes buyers of datacentre servers, and datacenter owners and operators. Clearly, it is important that common and accurate methods for measuring and calculating carbon emissions are used. De-facto and approved standards are therefore merging for these voluntary, and mandatory, reporting mechanisms:

- GHG Protocol

When it comes to specific greenhouse gas metrics, no single, globally applied standard for measuring carbon emissions has been agreed on. However the GHG Protocol has become a de facto standard. Developed in partnership between the World Resources Institute (WRI) and the World Business Council for Sustainable Development (WBCSD), the protocol provides standards and guidance for companies and other organisations preparing a GHG (greenhouse gas) emissions inventory. It covers the accounting and reporting of the six greenhouse gases covered by the Kyoto Protocol — carbon dioxide (CO2), methane (CH4), nitrous oxide (N2O), hydrofluorocarbons (HFCs), perfluorocarbons (PFCs) and sulphur hexafluoride (SF6).

The protocol places emissions within a framework that is divided into three categories. Scope one is concerned with direct emissions such as those from a factory; scope two covers indirect emissions through the products or services bought by the company - for example purchased electricity. Scope three is focused on indirect sources such as outsourced services. However most companies are unlikely to directly interface with the protocol but will rather deal with the standards it states which are detailed below:

- Carbon reporting Standards: ISO 14064 and 14001

ISO 14064-1 is one of four standards devised by the International Organisation for Standardisation (ISO) for reporting on greenhouse gases and makes use of the GHG Protocol. It specifies the principles and requirements for design, development, management and reporting of an organisations GHG inventory. The other standards apply to reporting at project level; to validation and verification; and to accreditation or other forms of recognition. ISO 14001 meanwhile addresses the environmental impacts of an organisation in general. Either standard can be

used by itself, or an organisation can use both. While ISO 14001 is a good first step to evaluate the 'environmental' health of a company, it does not provide a carbon footprint or measure emissions.

- PAS 250
A standard for reporting greenhouse gas emissions at a corporate level is only part of the story. The other half concerns the embodied carbon in goods produced, and the emissions associated with services. For just this purpose, the Publicly Available Standard (PAS) 2050 is a measurement methodology being developed by the British Standards Institute on behalf of the Carbon Trust and the British government's Department for Environment, Food and Rural Affairs (Defra). It aims to ensure that assumptions made for modeling and data are consistent across companies and products, in order to ensure comparable carbon footprinting. PAS 2050 is being actively expanded outside the UK, with personnel involved in developing the standard also working with the World Resources Institute.

- Data centre specific reporting
The recent focus on datacentres by the EPA, the EU and the Green Grid has led some organisations to raise questions about carbon-footprinting applications and services delivered by datacentres. At present, this activity is in the early stages, and any legislation or benchmarking in this area must be considered to be a long way off. Two influential UK bodies, the British Computer Society (BCS) and the Carbon Trust, have joined forces to develop open source software that can be used to model energy efficiency and carbon emissions in datacentres on a per-service basis. The simulation tool has been developed by some of the advisors to the EU on how to measure datacentre efficiency. Although there has been no indication of this, the EU could recommend the use of such metrics in a future iteration of the datacentre Code of Conduct.

Comment regarding OPTIMIS: Many datacenter service providers make claims regarding the carbon efficiency of their operations, and ultimately, it would be useful if these claims were consistent and verifiable. If some form of carbon reporting is integrated into OPTIMIS, including the carbon content of power, it should be consistent with any existing protocols and standards such as the GHG Protocol.
As it stands, incorporating this level of comprehensive environmental data is largely beyond the scope of OPTIMIS, although some suppliers may choose to supply such information. If they do so, plugging in GHG information relating to an entire service providers' business - using ISO standards - may prove more realistic than trying to pull out specific contributions of IT infrastructure alone. The carbon footprint of the entire service provider could be used a proxy until such time that the specific data centre or IT infrastructure carbon reporting becomes available.

4.5.10.6 European Rating Systems

4.5.10.6.1 European Data Centre Code of Conduct
The European Code of Conduct on Data Centres Energy Efficiency has been developed in response to the raise of energy consumption in data centres and the current needs to decrease the economic, environmental and energy supply security impacts. The aim is to inform and

foster the improvement of energy efficiency in the planning and operation of data centres. The Code of Conducts aims to achieve this by raising awareness and recommending energy efficient best practices and targets.[338]

The Code of Conduct it is not a legally binding document but a voluntary initiative with the objective of bringing stakeholders together. Parties signing up will be expected to follow this set of best practices recommendations and abide to the principles described therein. The Code contains a comprehensive list of best practices as well as documentary aids and measurement procedures. Data centres may be entitled to use the Code logo if such improvement programs have been recognised by the EU Commission.[339]

It is important to mitigate the energy consumption of data centres by reducing the substantial amount of redundant power and cooling systems. The Code of Conduct poses a set of general principles and practical actions to help all parties involved to address energy efficiency issues. Therefore, data centres owners and operators, data centre equipment and component manufacturers, service providers, and other large procurers of such equipment will be invited to participate in the Code of Conduct.[340] Nevertheless the Code of Conduct is addressed primarily to the data centres owners and operators, who may become "participants" by signing the document, it is also addressed to the supply chain and service providers who may become "endorsers".[341]

The Code of Conduct considers the data centre as a complete system including all buildings, facilities and rooms which contain enterprise servers, server communication equipment, cooling and power equipment. Therefore, the focus of this Code could be described in two main areas: 1) IT Load: which relates to the consumption efficiency of the IT equipment in the data centre, and; 2) Facilities Load: which includes the mechanical and electrical systems that support the IT electrical load e.g. cooling systems (chiller plants, fans, pumps), air conditioning units, Uninterruptible Power Supply (UPS), Power Distribution Units (PDUs), etc.[342]

In order to achieve the status of 'participant',[343] for existing data centres, an initial energy measurement of at least one month and an energy audit or assessment to identify the most relevant saving opportunities, is the first step. Following, an action plan must be prepared and submitted containing those best practices within three years of approval of the plan. For those data centres which were recently constructed or renovated during and after the year 2005, it suffices to submit the energy measurement coupled with the description of those best practices implemented, and for the new data centres (under construction or recently completed) a full description of the best practices in order to make the data centre "best in class" must be adopted and included in the application form.[344]

---

[338] European Commission, *The EU-Code of Conduct on Data Centres Energy Efficiency*, 2008, p. 3.

[339] Federal Ministry for the Environment, Nature Conservation and Nuclear Safety, Energy-Efficient Data Centres: Best-Practice Examples from Europe, The USA and Asia, 2010, p. 39.

[340] European Commission, The EU-Code of Conduct on Data Centres Energy Efficiency, 2008, p. 4.

[341] European Commission, The EU-Code of Conduct on Data Centres Energy Efficiency, 2008, p. 7.

[342] *Ibid* at p. 5.

[343] For a full list of 'participants' please see, European Codes of Conduct for ICT, available at: <URL:http://re.jrc.ec.europa.eu/energyefficiency/html/standby_initiative_dc_participants.htm> [Accessed 18 July 2010].

[344] European Commission, The EU-Code of Conduct on Data Centres Energy Efficiency, 2008, p. 8.

In order to achieve the status of 'endorser'[345], the following organisations are eligible according the Code of Conduct[346]:

- Vendors
- Consultancies (designer, engineering, maintenance and service companies)
- Utilities
- Government
- Industry Associations/Standard bodies (e.g. ASHRAE, BSC)
- Educational Institutions

The above mentioned organisations are expected to use this Code of Conduct in order to develop products, solutions and programs to allow data centres and operators to meet the expectations of this Code. In addition, organisations which become involved in some aspects of the design, building or operation of data centres may take some actions which help to achieve the overall goals of the Code of Conduct of improving the energy efficiency of the data centre. This will depend primarily on the activity of those organisations involved. For instance, an educational institution might emphasise and extend the treatment of energy efficiency, and a manufacturer of IT components might develop specific material to help raise user awareness of energy efficiency issues, or might introduce or encourage the use of high efficiency products.[347] The Code of conduct spells out how energy efficient datacentres should be run, and sets up a metrics and monitoring system. Participation is voluntary for now, but the CoC is seen by many as a framework document and as a data collection methodology for a future European Directive.

The EU's goal is to ensure that datacentres are demonstrably improving. To that end, it will collect significant amounts of data from datacentres, including energy use and adoption of technologies and best practices. It will also develop, adopt and publicise metrics, so that datacentres can be compared and (eventually) given targets. As a start, it will use Green Grid's Datacentre Infrastructure Efficiency (DCIE) ratio (the reciprocal of PUE or Power Usage Effectiveness) and at least two others which, when ready, will attempt to get a view on the overall effectiveness of the IT operation.

In order to qualify for COC status, participating datacentres must file a detailed report, as well as monthly IT and total facility energy use reports, at least twice a year. In this way, it will create a framework for data collection for the future. Initially, at least, the EU will collect the data, both for auditing and for anonymised analysis. If the Code of Conduct works well, it could be made mandatory under European law to encourage energy efficiency among non-participants; conversely, if it doesn't produce results, the EU will seek a tougher approach.

Comment regarding OPTIMIS: Participation in The DC COC is one of the single most useful measures when it comes to plugging energy efficiency information into the OPTIMIS platform. Datacentres could either expose the same energy use information on to the OPTIMIS platform,

[345] For a full list of 'endosers' please see, European Codes of Conduct for ICT, available at: <URL:http://re.jrc.ec.europa.eu/energyefficiency/html/standby_initiative_dc_endorsers.htm, [Accessed 18 July 2010].

[346] European Commission, The EU-Code of Conduct on Data Centres Energy Efficiency, 2008, p. 9.

[347] European Commission, The EU-Code of Conduct on Data Centres Energy Efficiency, 2008, p. 9-10.

directly or via the EU, or a check box could confirm CoC registration and participation. A limitation is that only 32 companies have signed up, although many are large telecoms players who are likely to offer cloud services. The reporting processes embedded in the code should help to provide a foundation for similar reporting which could be a requirement for participation in OPTIMIS.

Companies signed up to the code so far are:	*Belgacom* *France Telecom-Orange* *TDC Services* *Telecom Italia* *Telefonica* *Turk TelekomA1 Telekom Austria AG* *Bracknell Forest Borough Council* *British Telecommunications plc* *Business & Decision* *Bytesnet BV* *EvoSwitch Netherlands B.V.* *FUJITSU Services* *Hewlett-Packard* *IBM Deutschland Business Services GmbH* *IBM United Kingdom Limited* *INTEL* *LAMDA Hellix S.A.* *Memset Ltd. Corporate level* *Microsoft Corporation* *Onyx Group Limited* *Petroleum Geo-Services (PGS)* *Reed Specialist Recruitment* *TCN Telehousing* *TelecityGroup CoC* *The UK Grid Network Ltd* *Thomson Reuters* *TISSAT S.A.* *UK Meteorological Office* *VCD Infra Solutions* *Vodafone Group Service GmbH* *Bull SAS*

Table 2: The table shows the companies signatories of the European Code of Conduct.

4.5.10.6.2 Code of Conduct on Energy Consumption of Broadband Equipment

Cloud services are not only underpinned by data centres or other computing facilities but also rely on communications networks. By 2015 electricity consumption from broadband services and its associated infrastructure will account for 50 TWh per year. It is the energy efficiency of the network provision which is the focus of the EU Broadband Equipment Code of Conduct.

Although the code is focused on consumer and home network technologies, it also relates to

wider network equipment including DSL network equipment,, combined DSL/narrowband network equipment, wireless broadband network equipment, cable service provider equipment and powerline service provider equipment.

The broadband code could also have direct relevance for datacentre providers who have dedicated relationships with one or more telecoms provider. If the datacenter is signed up to the datacentre code and the telecoms provider providing data services to its facility is likewise signed up to the broadband code, it could be seen to add an extra level of energy efficiency to the facility and the services it provides.

Comment regarding OPTIMIS: As with the datacentre code, the broadband code could provide another way to assess the energy efficiency of service providers hoping to interact with OPTIMIS. Cloud service providers may own broadband infrastructure directly - as with BT - in which case the code will be specifically relevant. Where this is not the case, then the code may not be directly relevant. However, having relationships/partnerships with broadband code approved telecoms partners could also be seen as environmentally beneficial to service providers.

Companies signed up to the code so far are:	*A1 Telekom Austria AG* *Belgacom* *British Telecom* *KPN* *France Telecom-Orange* *OTE* *Portugal Telecom* *Telefonica* *Telenor* *Turk Telekom* *Alcatel-Lucent* *CISCO* *Deutsche Telekom* *Huawei Technologies* *Nokia Siemens Networks* *Swisscom* *TDC Services* *Telecom Italia* *Telia Sonera* *Technicolor*

Table 3: The table shows the companies signatories of the Code of Conduct on Energy Consumption of Broadband Equipment.

(NB: Separately it may be worth considering if the energy efficiency of the broadband network itself should be factored into OPTIMIS energy efficiency calculations generally).

4.5.10.6.3 European equipment energy labelling schemes

While the US Energy Star for datacentres certification and its European counterpart the Data-centre Code of Conduct seek to assess an entire facility, numerous equipment level rating schemes also exist. In Europe these include the German Blue Angel scheme and its Scandinavian counterpart the Nordic Ecolabel or Nordic Swan. Both are primarily consumer focused but do include some computing equipment. Legislative measures also exist in the form of the 2005 Energy-Using Products (EuP) Directive which is covered elsewhere in this report. The European Union has also adopted the bulk of the Energy Star energy-efficient labelling scheme established by the EPA. The scheme was recently extended to include Data Centre equipment in the US and some elements of this may inform the drafting of the European Data Centre Code of Conduct. However at present only desktop computers and monitors are included in the European version of the scheme.

Comment regarding OPTIMIS: While not directly focused on data centre infrastructure, purchasing equipment which is compliant with these schemes could provide some evidence that a cloud provider is taking some energy efficiency measures. During the lifetime of OPTIMIS some of these schemes may be extended to include servers and storage systems and therefore will become more relevant.

4.5.10.7 Non-European Rating Systems

4.5.10.7.1 US Energy Star Data Centre Energy certification

The US Energy Star certification system covers a variety of products from household white goods right up to datacenters. Regarding datacenters, the Energy Star rating is awarded to the top quartile of energy efficient facilities in operation.
The EPA (Environmental Protection Agency) is not alone. Both The Green Grid and the US Dept. of Energy have also initiated datacenter energy efficiency data collection and registration schemes. The three groups are co-operating to ensure that data collection techniques are consistent, and it seems likely that these schemes may join together at some stage.
-Criteria:
Facilities must reapply for Energy Star each year, based on their performance over the previous 12 months. Points are awarded on a 1-100 scale, each point corresponds to one percent. A score of 80 means a facility is more energy efficient than 80% of a group of similar buildings nationwide. Energy Star requires an annual PUE to measure efficiency. Facilities must submit data on all of the energy delivered to a building, from all fuel sources, for an entire year. “IT load” is measured at the output of the UPS (Uninterruptible Power Supply).

-Public Disclosure:
EPA’s performance scale uses a zip code to calibrate the weather’s influence on PUE, as some sites will benefit more from free cooling opportunities, etc. Although voluntary, the EPA seeks to get datacentre operators to improve their energy efficiency by encouraging a certain amount of public disclosure. Energy Star rated datacentres are listed in a publicly available registry. Co-location and hosting firms might even win business on the basis of efficiency ratings. Operators who refuse to apply may be looked upon as suspect.

Comment regarding OPTIMIS: At present, Energy Star for datacentres is not running in Europe, although previous Energy Star schemes have eventually crossed the Atlantic. While OPTIMIS is European focused, it can also be anticipated that it will attract either the European operations of US companies or interest pure US players. Therefore it makes sense for the OPTIMIS project to assess how it might be consistent with Energy Star schemes, and how it might access the Energy Star datacentre registry at some point in the future.

4.5.10.7.2 Energy Star for Servers, Storage and Power Supplies

As well as rating the overall datacentre, Energy Star certification can also be applied to specific equipment including servers, storage and even power supplies. The scheme sets a bar that approves about 25 % of the most energy efficient products, and gives the market time to catch-up. Then it raises the bar again.

-Energy Star for Servers:
This is currently under revision but is likely to be based on the SPECPower metric from the Standard Performance Evaluation Corporation (SPEC). The benchmark evaluates the power and performance characteristics of computer servers. SPECPower ratings are already available for viewing on the SPECPower website for certain machines.

-Energy Star for Data Storage:
This relates to large data storage devices such as storage arrays and related networking equipment. This is also in the development stage. Draft 1, Version 1.0 has recently been published.

-Energy Star for Uninterruptible Power Supplies:
This relates to high specification supplies used in datacenters and computing facilities to ensure consistent power. This is currently in the drafting/development stage with a specification expected by the end of 2010.

Comment regarding OPTIMIS: For those service providers whose datacentres are not certified under either the Datacentre Code of Conduct or the US Energy Star certification, the equipment level scheme could provide a useful proxy. Asking service providers to give details of how much of their equipment is covered by the Energy Stat scheme could provide a useful, if not overly accurate, guide to the sustainability/energy efficiency of their operations.

4.5.10.7.3 Energy Star for Servers, Storage and Power Supplies

The Electronic Product Environmental Assessment Tool (EPEAT) was developed through the US EPA and is managed by the Green Electronics Council. The system currently covers desktop and laptop computers, thin clients, workstations and computer monitors.
EPEAT gives product a simple rating based on 51 detailed environmental criteria ranging from reduction/elimination of environmentally sensitive materials to energy conservation, to packaging. Once a product adheres to all the criteria it is awarded the basic Bronze level of certification. However, manufacturers can choose to go beyond this stage by achieving 50 %, or for the Gold level 75%, of an extra optional set of criteria. These optional criteria include eliminat-

ing materials such as PVC.
At present, EPEAT does not cover servers, but the work to create this standard is under way and is expected in 2011.

Comment regarding OPTIMIS: EPEAT may be extended to include servers within the lifetime of the OPTIMIS development period which could have ramifications for assessing cloud providers infrastructure. While EPEAT will not be extended to DCs or cloud services anytime soon, OPTIMIS could require details of how much of a cloud provider's server estate is EPEAT certified for example.

4.5.10.8 Related and Relevant EU Initiatives

4.5.10.8.1 The ICT4EE Forum

Established by the European Commission and parties from the IT industry on 23 February 2010, the forum focuses on two key aspects of Eco-efficient IT: first, how the technology industry can curb its energy use; and second, how it can help other sectors do likewise. By mid 2010, four industry associations had signed up to represent the European, Japanese and American ICT industries: DigitalEurope; Global e-Sustainability Initiative (GeSI); the Japanese Business Council Europe (JBCE); and TechAmerica Europe.
The forum is made up of three working groups that started their work in April 2010 looking at: energy efficiency of ICT processes (focusing on the development of measurement standards); using ICT to improve energy efficiency in other sectors (buildings, transport, and energy transformation); and informed and coordinated policy making.

Comment regarding OPTIMIS: One of the ICT4EE working groups is focused on the energy efficiency of ICT processes and developing measurements. This could potentially yield metrics or methodologies relevant to OPTIMIS. However, the initiative is currently in its early stages.

4.5.10.8.2 Games and Fit4Green

The EU is directly funding two projects in 2010 focused on energy efficiency of data centres:

-Games:

The stated goal of GAMES (Green Active Management of Energy IT Service Centres) is to develop more sophisticated datacenter energy monitoring and control tools. The project organisers claim that current data centre energy monitoring tools work in isolation and do not consider the interaction between applications, computing hardware, and aspects of the physical facility such as cooling and power supplies.

The Games project aims to produce energy monitoring and control tools that factor in these interactions to allow for more efficient design and operation of energy efficient facilities. The result according to the consortium will be a 25% increase in efficiency for datacenters that adopt the tools it develops. The Games consortium is made up of a business, and research organisations including IBM Israel, and the University of Stuttgart. The project is set to run over 30 months from 2010.

-Fit4Green:

Fit4Green (Federated IT for a sustainable environmental impact) is focused on creating a series of software plug-ins for existing data centre management tools. The plug-ins are designed to facilitate the movement of virtual machines or virtual work-loads between servers within a datacenter but also between federated datacenters.

The aim is to allow virtual workloads to be moved to the most optimal environment from an energy efficiency perspective. This will include the ability to switch off servers for example which are no longer being used as a result of virtual machines being moved to another better utilised device. Fit4Green is a 30 months project begun in 2010 and includes organisations such as Imperial College London, HP, and the University of Mannheim.

Comment regarding to OPTIMIS: Games and Fit4Green are still in the early stages and so are unlikely to benefit OPTIMIS directly during 2010/11. However there may be scope to share basic energy efficiency research in the short-term which would be beneficial to all parties.

Longer term, OPTIMIS could also look to encourage service providers and customers who sign up to use its cloud framework to explore the energy saving tools being developed under both GAMES and FIT4Green within their datacenters.

Fit4Green may also yield some useful research regarding the energy efficiency implications of virtual machine sharing between cloud-specific datacenters. In the future this could potentially mean that shifting workloads for energy efficiency reasons – i.e. moving a workload to a cloud provider – becomes a motivating factor that ranks alongside existing reasons for adopting the OPTIMIS framework (such as lack of capacity).

4.5.11 Summary of non-legislative energy efficient metrics, certifications and initiatives

Name	Authority	Geography	Focus	Legal weight/Influence	Awareness/Take-up	Relevance To Optimis
PUE (Power Usage Effectiveness)	Green Grid/De-facto	Global	DC Energy usage metric	De-facto standard	High awareness, Med adoption	OPTIMIS is to include a mechanism for sharing of PUE data and acceptable ranges for participate in various levels of OPTIMIS.
BREEAM/ LEED		US and Europe	Energy Efficient Facilities	Voluntary	High awareness, low adoption	Whether participants' physical facilities adhere to energy efficient building standards.
GHG Protocol	World Resources Institute	Global	Greenhouse gas report-	De-facto Standard	High awareness, adoption patchy	OPTIMIS Carbon reporting mechanism must be

	(WRI) and the World Business Council for Sustainable Development (WBCSD),		ing metric			based on standards such as the GHG Protocol
ISO 14064	International Organisation for Standardisation (ISO)	Global	GHG Reporting	Voluntary	Medium	To ascertain whether SP carbon claims are reliable
ISO 14001	International Organisation for Standardisation (ISO)	Global	Environmental Impact reporting	Voluntary	Medium	To ascertain whether SP environment claims are reliable
PAS 2050	PAS 2050	UK but expanding	Embodied carbon in goods produced,	Emerging	Low	To ascertain whether SP carbon claims are reliable
European DC Code of Conduct	European Commission	Europe but US interest	Data Centre Energy Efficiency	Developing (only 32 companies)	Low	DC energy efficiency information
European Broadband Code of Conduct	European Commission	Europe	Broadband equipment – home and network	Developing	Low	Efficiency of broadband equipment
Blue Angel, Nordic Swan, EU Energy Star	German, Scandinavian, EU authorities	Europe	Energy Efficient Labeling of computer equipment	Established but consumer focused	Med	Indicator that participant takes efficiency seriously
US Energy Star Data Centre	US EPA	US and some international	Overall data centre efficiency metric	Established and growing	Low	Important for rating US service providers interacting with OPTIMIS
Energy Star For Servers, Storage and Power Supplies	US EPA	US and some international	Energy Star rating for hardware	Developing – storage and Power still emerging	High awareness, low adoption	Could provide a useful, if not overly accurate, guide to the sustainability/energy efficiency of their operations.
EPEAT	US EPA/ Green Electronics Council	US	Sustainability rating for equipment	Established but server specific still emerging	Medium	OPTIMIS could require details of how much of a cloud provider's

						server estate is EPEAT certified for example.
ICT4EE Forum	European Commission	Europe e but with involvement of international vendors	Industry/public initiative focused on green IT	Emerging	Low	Learnings could be shared with OPTIMIS
GAMES (Green Active Management of Energy IT Service Centres) and Fit4Green	European Commission	Europe but with involvement of international vendors	Focused on datacentre efficiency metrics and management	Emerging	Low	Findings could be shared with OPTIMIS

Table 4: The table shows a summary of non-legislative energy efficient metrics, certifications and initiatives.

4.5.12 Conclusion

By the end of 2008 the EU implemented an Integrated Climate Change and Energy Policy aimed at reducing 20% of energy consumption through energy efficiency mechanisms and lowering greenhouse gas emissions (and 30% when international agreements take place).

The European Parliament Resolution of 4 February 2009 on the challenge of energy efficiency through information and communication technology called on the Commission and the Member States to take energy efficient actions from a holistic point of view i.e. taking into account not only technical components separately but the entire systems including those necessary legislative changes emphasising the gradually reduction of CO2 emissions through the implementation of green strategies based on the use of ITs and ICTs.

This resolution also called on the Commission and Member States to improve the regulatory framework taking into consideration SMEs which can play an important role in implementing ICT-based solutions for energy efficiency.

The European Union Greenhouse Gas Emission Trading System (EU ETS) operates as the largest multi-country, multi-sector Greenhouse Gas Emission Trading System world-wide. In this respect, Directive 2009/29/EC is very relevant as takes part of the so called 'community legislation package on energy and climate change' which main purpose is to launch a series of measures to ensure compliance with the European Council commitment of March 2007, to reduce global emissions of greenhouse gases.

Alongside these laws there are a number of the so called "soft laws" which are not legally binding documents, however influence enormously the legislation. Many examples of these have been provided aiming at predicting the following steps the European legislators are going to make. A good example of this is the European Code of Conduct on Data Centres Energy Efficiency which poses a set of general principles and practical actions to help all parties involved

to address energy efficiency issues. Therefore, data centres owners and operators, data centre equipment and component manufacturers, service provider, and other large procurers of such equipment will be invited to participate in the Code of Conduct. Here again, our estimation is that this Code of Conduct will be compulsory in the near future.

Finally, we have made an attempt to provide a comprehensive list of de facto standards, metrics and other industry initiatives from a European and international perspective as we believe these rules and benchmarks could be useful for OPTIMIS. Some of these initiatives such as energy efficiency metrics e.g. PUE (Power Usage Effectiveness) which have emerged as de facto standards, have been very recently announced by the European Commission to be officially adopted as their official datacenter energy efficiency metric.

4.5.13 Summary

The summary of green legislation and quasi-legal initiatives outlined in section 4.5 provides a useful guide to the environment in which OPTIMIS is being developed. Effort has been made where possible to highlight the relevance of each law, initiative or project to the goals of the wider project.

However there are a number of practical recommendations and action points which should also be highlighted to make best use of the information assimilated thus far. These include practical steps on the application of existing metrics, how to work with industry standards and bodies, the need to design for future legal changes, and the use and cooperation with other EU funded projects with similar goals – particularly around energy efficient technology.

What OPTIMIS needs to do

EU Datacentre Code of Conduct: Section 4.5.10.6.1 examines the development of the European Code of Conduct for Datacentre efficiency and its implications for OPTIMIS. Questions have been raised over the likelihood of the code forming the basis of a law which would seek to regulate measures taken by datacentre owners and operators to improve energy efficiency. Our research indicates that the development of such a law is unlikely in the near future. Although most of the Code is concerned with internal datacentre operations, the next stage of OPTIMIS research should ensure that future developments – and any future laws anticipated, and any possibilities for using the EU CoC are explored. We recommend liaising with the Joint Research Council to ensure that this covered.

Integrating with PUE: Section 4.5.10.2 covers the range of energy efficiency metrics including PUE and its reciprocal DCIE. The section suggests that OPTIMIS develops some way to use PUE data in the OPTIMIS toolkit (There are clear signs in the market that some procurement contracts now require that datacentre operators provide PUE metrics). Practically, this should involve liaison with the European arm of the Green Grid, which developed the PUE metric, especially for anticipating future developments (there are now many variations of the PUE metrics). Most datacentres, certainly by 2014, will have either a real time PUE figure (available as a web service) or an average figure that can be automatically collected or manually input, and ability to use this data should be in the relevant SLAs.

Collaborating with EU green metric projects: Section 4.5.10.8.2 outlines a number of relevant EU projects which aim to develop green metrics or methodologies that could be relevant to

OPTIMIS. Overtures have already been made to the project leaders of both GAMES and Fit4Green, with the aim to share findings in a mutually beneficial manner. However, as highlighted in the report, both efforts are in their relative infancy and it will be mid 2011 until they begin to be useful to efforts under OPTIMIS.

Links have also been established to the REViSITE project which is investigating into the net impact of ICT on energy efficiency in the four sectors of construction, grids, lighting and manufacturing. The project is attempting to achieve a common impact assessment model and a roadmap which are non sector specific. The project's leaders have signalled an interest in the OPTIMIS project and the ability of Cloud computing in general as a way to harness energy efficiency.

Anticipating carbon laws: As explained, the laws regarding carbon reporting are likely to change and evolve significantly in the coming two decades. Furthermore, legislation will vary widely from country to country, both within the EU and beyond. Although there are no laws that currently require carbon or energy reporting by datacentres, some buyers of services are or will be mandated to ask suppliers to provide carbon or energy data. It is therefore important that the OPTIMIS toolkit be designed in a way that carbon and/or energy data be provided, and that it is done in such a way that this data is appropriately granular (by application or data stored, for example) and can be automatically collected by reporting tools. Given that the great majority of a datacentre provider carbon use is related to operational energy purchased from the grid, the tool should be designed to collect or input data provided by the utility.

Providing evidence of claimed compliance: Using the OPTIMIS toolkit, datacentre operators will be asked to provide data on energy use and conformance with certain codes and standards, some of which involve certification by third parties. At present, we have not devoted time to considering how this data might be verified. We believe this an area for future discussion and research.

Exploration of issues relating to multiple datacentres: Compliance with rules and standards, and energy use and efficiency, can vary widely from datacentre to datacentre. We recommend that future research for OPTIMIS considers how suppliers that wish to move workloads between datacentres can or should report this to their customers. We further recommend that the toolkit should include an option that the work is carried out in single or specified conformant datacentres. The Fit4Green project is undertaking some work in this area and could be a subject for collaboration with OPTIMIS in the future.

Designing for kitemarks and external standards: In the field of eco-efficiency, there are many standards and kitemarks that are used by buyers of services. Sometimes, large buyers are mandated by government to adopt these standards. It is not necessary for the OPTIMIS toolkit to build an understanding of all these standards. However, we recommend that the toolkit be designed to allow for simple fields to be added so that suppliers can indicate compliance.

Annex A. References

Books and Articles

Bainbridge	Intellectual Property, 4th Edition., London, 1999.
Bently/Sherman	Intellectual Property Law, Third Edition, Oxford, 2009.
Bercusson	European Labour Law and the EU Charter of Fundamental Rights, 1st Edition, Baden-Baden 2006.
Bülles-bach/Poullet/Prins	Concise European IT Law, New York 2006.
Buttazzoni	WWF Sweden Report, "The potential global CO2 reduction from ICT use, Identifying and assessing the opportunities to reduce the first billion tonnes of CO2", 2008.
Carey	Data Protection – A Practical Guide to UK and EU Law, New York 2009.
Cornish/Llewelyn	Intellectual Property: Patents, Copyright, Trade Marks and Allied Rights, Sixth Edition, Sweet & Maxwell, 2007.
Dammann	RDV 2002, 70-77.
Dammann/Simitis	EG-Datenschutzrichtlinie, Baden-Baden 1997.
Davison	The Legal Protection of Databases, Cambridge, 2003.
Derclaye	The Legal Protection of Databases, A comparative analysis, Chelten-ham, 2008.
Dines	From London To Munich – Where To Collocate Your Data centre? And With Which Provider? (2010).
Djemame et al.	Introducing Risk Management into Grid, IEEE Computing Society, 2006.
Ehlers	European Fundamental Rights and Freedoms, Berlin 2007.
Ehmann/Helfrich	EG- Datenschutzrichtlinie, Kurzkommentar, Köln 1999.
Forgó/Krügel	MMR 2010, 17-23.
Gaster	"Obtinere" of Data in the eyes of the ECJ: How to interpret the Data-base Directive after the British Horseracing Board Ltd. Et al. V. William Hill Organisation Ltd, CRi, 2005.
Guadamuz	Open source licenses in scientific research , SCRIPTed - Edinburgh, 2005.
Hawellek	MMR-Aktuell 2010, 300069.
Helling	Retrieving the Sources of Legal Decision-Making, Technical Possibilities and Related Legal Issues, in Scandinavian Studies in Law, Volume 47, (Peter Wahlgren ed.), Stockholm, 2004.

Hijmans/Scirocco	Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty Be Expected to Help?, 46 CML Rev. 2009, 1485-1525.
Kemna	R. B.J., et al., Methodology for Ecodesign of Energy-using Products (EuP), The Netherlands, 2005.
Kosta/Dumortier	The Data Retention Directive and the principles of European data protection legislation, MR-Int. 2007, 130-136.
Kühling/Seidel/Sivridis	Datenschutzrecht, Frankfurt am Main 2008.
Kuner	European Data Protection Law – Corporate Compliance and Regulation, 2nd Edition, New York 2007.
Lawrence	Eco-Efficient IT: Policy, Legislation and Compliance - Eco-IT, Nov 2008.
Liebwald	The New Data Retention Directive, MR-Int. 2006, 49-56.
McJohn	Intellectual Property: Examples & Explanations, Aspen, 2006.
Myers	Principles of Intellectual Property Law, Thomson West, 2008.
Nettleton	ECJ rules on acts of „extraction" that infringe database right, Computer Law & Security Review, Vol. 25, Issue 2, ELSEVIER, London 2009.
Schultze-Melling	IT-Compliance – Challenges in a Globalized World, CRi 2008, 142.
Simitis	From The Market to the Polis: The EU Directive on the Protection of Personal Data, 80 Iowa L. Rev. 445 (1995).
Smith/Nair	The Architecture of Virtual Machines, 2005 Computer (IEEE Computer Society), Vol. 38 Issue 5, p. 32.
Virtanen	Database rights in safe European home: the path to more rigorous protection of information, Digipaino, 2005.
Wiegele	Biotechnology and International Relations: The Political Dimensions, University of Florida Press, 1991.

Electronic Material

Art. 29 Working Party	WP 37, Privacy on the Internet – An integrated EU Approach to On-line Data Protection, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37en.pdf
	WP 114, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp1

14_en.pdf.

WP 136, Opinion 4/2007 on the concept of personal data, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

WP 169, Opinion 1/2010 on the concepts of controller and processor, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf.

WP 172, Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf.

WP 177, Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp177_en.pdf.

Balboni Data Protection and Data Security Issues Related to Cloud Computing in the EU, available at: http://ssrn.com/abstract=1661437.

Brown Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, Working Paper No. 1: The Challenges to European Data Protection Laws and Principles, Oxford 2010, available at: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_1_en.pdf.

Burt Gartner Predicts Rise of Cloud Integration Services, http://www.eweekeurope.co.uk/news/news-security/gartner-predicts-rise-of-cloud-integration-services-1350.

Conolly The US Safe Harbor – Fact or Fiction? available at: http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf.

Department of Energy and Climate Change Climate Change Agreement, Policy and Legislation, available at: http://www.decc.gov.uk/en/content/cms/what_we_do/change_energy/tackling_clima/ccas/ccas_policy/ccas_policy.aspx.

Climate Change Act, available at: http://www.decc.gov.uk/en/content/cms/legislation/cc_act_08/cc_act

_08.aspx.

(2010) "Government Response to Consultation on the Form and Content of New Climate Change", available at: http://www.decc.gov.uk/assets/decc/Consultations/ccaFormContent2nd/1_20100323111626_e_@@_ccaGovernmentResponse.pdf.

European Commission

MEMO/06/452, Brussels, Nov. 2006, Questions and Answers on Emissions Trading and National Allocation Plans for 2008 to 2012, available at: http://ec.europa.eu/environment/climat/pdf/m06_452_en.pdf.

Memorandum State aid N 629/2008 – United Kingdom CRC (Carbon Reduction Commitment), available at: http://ec.europa.eu/community_law/state_aids/comp-2008/n629-08.pdf.

Community Transaction Log, available at: http://ec.europa.eu/environment/ets/.

Emission Trading System, available at: http://ec.europa.eu/environment/climat/emission/index_en.htm.

DG Internal Market and Services Working Paper: First Evaluation of the Directive 96/9/EC on the legal protection of databases, 2005, available at: http://ec.europa.eu/dgs/internal_market/evaluation/evaluationdatabasesdirective.pdf.

The EU-Code of Conduct on Data Centres Energy Efficiency, 2008, available at: http://re.jrc.ec.europa.eu/energyefficiency/pdf/CoC%20data%20centres%20nov2008/CoC%20DC%20v%201.0%20FINAL.pdf.

Federal Ministry for the Environment, Nature Conservation and Nuclear Safety Germany (BMU)

"Energy Efficiency in Data centres, Best Practice Examples from Europe, the USA and ASIA", 2008, available at: http://www.bmu.de/files/pdfs/allgemein/application/pdf/broschuere_rechenzentren_en_bf.pdf.

Greer

The Art of Separation of Concerns, available at: http://www.aspiringcraftsman.com/2008/01/art-of-separation-of-concerns/.

Helbing

How the New EU Rules on Data Export Affect Companies in and Outside the EU, http://www.thomashelbing.com/en/how-new-eu-rules-data-export-affect-companies-and-outside-eu.

Jackson

Cloud computing leaving relational databases behind available at: http://gcn.com/Articles/2008/09/19/Cloud-computing-leaving-

relational-databases-behind.aspx.

Johnston The 6 layer Cloud computing stack available at: http://samj.net/2008/09/taxonomy-6-layer-cloud-computing-stack.html.

Korff Comparative Study on Different Approaches to New Privacy Challenges, Particular in the Light of Technological Developments, Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments, London 2010, available at: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf.

EC Study on Implementation of Data Protection Directive, Cambridge 2002, available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf.

Kupferman The Low Down on Cloud Brokers, available at: http://www.regexprn.com/2009/08/low-down-on-cloud-brokers.html.

Martin "Customising SaaS", available at: http://buildingsaas.typepad.com/blog/2006/08/customising_saa.html.

Miscellaneous Carbon Disclosure Project, available at https://www.cdproject.net.

Cloud Balancing, Cloud Bursting and Intercloud, available at: http://devcentral.f5.com/weblogs/macvittie/archive/2009/07/09/cloud-balancing-cloud-bursting-and-intercloud.aspx.

Cloud Computing: The Key Issues and Solutions, available at: http://www.ffw.com/publications/all/articles/cloud-computing.aspx.

Data centre, available at http://en.wikipedia.org/wiki/Data_center.

EPEAT definition, available at http://www.epeat.net/.

EU Code of Conduct, available at: http://re.jrc.ec.europa.eu/energyefficiency/html/standby_initiative.htm.

Global warming, *Global warming: Kyoto and its implications*, available at: http://earthguide.ucsd.edu/globalchange/global_warming/02.html.

GRIDipedia, The European GRID Market Place available at: http://www.GRIDipedia.eu/GRIDipr.html.

Helpdesk on Intellectual Property Rights related issues in EU-funded projects, available at:

http://www.ipr-helpdesk.org/faqs_trade_secrets.html.

http://en.wikipedia.org/wiki/Separation_of_concerns.

http://europa.eu/legislation_summaries/internal_market/businesses/intellectual_property/l26053_en.htm.

http://noticias.juridicas.com/base_datos/Admin/l13-2010.html.

http://www.ansmann.de/cms/businessdivision/consumroot/chargers-and-power-supplies/power-supplies/ecodesign-directive-eup.html.

http://www.decc.gov.uk/en/content/cms/what_we_do/change_energy/tackling_clima/ccas/eligibility/eligibility.aspx.

http://www.diss.fu-ber-lin.de/diss/servlets/MCRFileNodeServlet/FUDISS_derivate_000000001587/2_3.pdf.

http://www.era.co.uk/Services/ecodesign.asp.

http://www.era.co.uk/services/eco-design-status.asp.

PAS 2050, available at: http://www.bsigroup.com/Standards-and-Publications/How-we-can-help-you/Professional-Standards-Service/PAS-2050.

SPECPower, available at http://www.spec.org.

The Carbon Reduction Commitment, available at: http://www.decc.gov.uk/en/content/cms/what_we_do/lc_uk/crc/crc.aspx.

The CRC Energy Efficiency Scheme: User's Guide, available at: http://www.decc.gov.uk/assets/decc/what%20we%20do/a%20low%20carbon%20uk/crc/1_20100406154137_e_@@_21934crcpdfawv9.pdf.

Virtual machine, available at: http://en.wikipedia.org/wiki/Virtual_machine.

World Intellectual Property Organisation, available at: http://www.wipo.int/portal/index.html.en.

O'Neill How Cloud Service Brokers Enable the Cloud Marketplace, available at: http://www.soatothecloud.com/2010/02/how-cloud-service-brokers-enable-cloud.html

OECD http://www.oecd.org/pages/0,3417,en_36734052_36761800_1_1_1_1_1,00.html.

Recommendation of the Council on Information and Communication Technologies and the Environment, 8 April 2010, C(2010) 61, available at: http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=259&Lang=en&Book=False.

Ormsby Prentice, *Extracting New Value from the Database Right – ECJ Decision in Directmedia Case* available at: http://newsweaver.ie/mop/e_article001294984.cfm?x=b11,0,w.

Poullet et. al. Discussion paper – Cloud computing and its implications on data protection, Namur 2010, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_yvespoullet1b.pdf.

Rawson et. al. The Green Grid Data centre Power Efficiency Metrics: PUE and DCiE, available at: www.thegreengrid.org/Global/Content/white-papers

Rubin Dynamic Cloud Fitting – The Future in Automated Cloud Management, available at: http://www.cloudswitch.com/blog/category/Cloud%20Service%20Brok

ers.

Spiegel Online 'German High Court Limits Phone and E-Mail Data Storage', available at: http://www.spiegel.de/international/germany/0,1518,681251,00.html.

Stackhouse Location Factors for Data centres, available at: http://www.areadevelopment.com/siteSelection/august09/data-centers-electricity-climate-space008.shtml?Page=1

European Data Protection Supervisor Opinion of 18 March 2010 of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf.

Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005) 438 final), 2005 OJ C 298, 29.11.2005, pp. 3 et seqq, available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2005:298:0001:0012:EN:PDF.

The Register 'Data Retention Directive Receives Rubber Stamp',available at: http://www.theregister.co.uk/2006/02/24/data_retention_directive_ratified/.

Trujillo Naturkatastrophen, gesetzliche Regelungen und Steuern bewerten – Die Standortwahl von Rechenzentren wird international, available at: http://www.searchdatacenter.de/themenbereiche/physikalisches-umfeld/allgemein/articles/100922/

UNFCCC Clean Development Mechanism, available at: http://unfccc.int/kyoto_protocol/mechanisms/clean_development_mechanism/items/2718.php.

Emissions Trading, available at: http://unfccc.int/kyoto_protocol/mechanisms/emissions_trading/items/2731.php.

Joint Implementation, available at: http://unfccc.int/kyoto_protocol/mechanisms/joint_implementation/items/1674.php.

Kyoto Protocol, available at: http://unfccc.int/kyoto_protocol/items/2830.php.

Vaquero et. al. A Break in the Clouds: Towards a Cloud Definition, available at: http://www.systems.ethz.ch/education/past-courses/fs09/NIS/reading/cloud-definition.pdf.

World Health Organisation (WHO) WTO and the TRIPS Agreement, available at: *http://www.who.int/medicines/areas/policy/wto_trips/en/index.html*.

World Trade Organisation (WTO) Frequently- asked questions, available at: http://www.wto.org/english/tratop_e/trips_e/tripfq_e.htm#Who%27s Signed.

Understanding the WTO: The Agreements, available at: http://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm7_e.htm.

Zerdick "Folgerungen aus der Vergemeinschaftung der Justiz- und Innenpolitik für den Datenschutz", available at: http://www.datenschutz.hessen.de/download.php?download_ID=187.

Legislation

Bern Convention for the protection of Literary and Artistic Works, available at: http://www.wipo.int/treaties/en/ip//trtdocs_wo001.html.

Declaration on Green Growth (C/MIN(2009)5/ADD1/FINAL) adopted at the Council Meeting at Ministerial level on 25 June 2009.

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society available at:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML.

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society.

Directive 2002/21/EC of the European Parliament and of the Council Of 7 March 2002 on a Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive) OJ L 108, 24.04.2002.

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009; the consolidated version of Directive 2002/58/EC is available in the leaflet "Regulatory framework for electronic communications in the European Union" by the European Commission,
http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.p

df.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications), OJ L 201, 31.07.2002.

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services

Directive 2009/29/EC of the European Parliament and of the Council of 23 April 2009 amending Directive 2003/87/EC so as to improve and extend the greenhouse gas emission allowance trading scheme of the Community, available at:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0029:en:NOT.

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

EcoDesign Directive 2005/32/EC, the Amending Directive 2008/28/EC.

EcoDesign Directive 2009/125/EC, available at:
http://ec.europa.eu/enterprise/policies/sustainable-business/documents/eco-design/framework-directive/index_en.htm.

European Parliament resolution of 4 February 2009 on the challenge of energy efficiency through information and communication technologies, available at:
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0044+0+DOC+XML+V0//EN.

European Parliament resolution of 4 February 2009 on the challenge of energy efficiency through information and communication technologies, available at:
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0044+0+DOC+XML+V0//EN.

Generalitat de Catalunya, Climate Change Website, The United Nations Framework Convention on Climate Change, available at:
http://www20.gencat.cat/portal/site/canviclimatic/menuitem.75e3e8b36ded92ae9b85ea75b0c0e1a0/?vgnextoid=55f884a0883d7210VgnVCM1000008d0c1e0aRCRD&vgnextchannel=55f884a0883d7210VgnVCM1000008d0c1e0aRCRD&vgnextfmt=default&newLang=en_GB.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF.

WIPO WCT Treaty, available at:
http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html#P53_3973.

Judgments

ECJ, Judgment of 9 November 2004 – Case C-203/02 - The British Horse-racing Board Ltd v. William Hill Organisation Ltd (United Kingdom).

ECJ, Jugdment of 9 Oktober 2008 – Case C-304/07 - *Directmedia GmbH v Albert-Ludwig Universitat Freiburg,* available at: http://curia.europa.eu/jurisp/cgibin/gettext.pl?lang=en&num=79918990C19070304&doc=T&ouvert=T&seance=ARRET.

ECJ, Judgment of 9 November 2004 - Case C-338/02 - Fixtures Marketing Ltd v. AB Svenska Spel (Sweden).

ECJ, Judgment of 9 November 2004 – Case C-444/02 - Fixtures Marketing Ltd v. OPAP (Greece).

ECJ, Judgment of 9 November 2004 – Case C-46/02 - Fixtures Marketing Ltd v. Oy Veikkaus Ab (Finland).

ECJ, Judgment of 25 July 1991 – Case C-221/89 – Factortame.

ECJ, Judgment of 30 November 1995 – Case C-55/94 – Gebhard.

ECJ, Judgment of 6 November 2003, Case C-101/01 margin no. 95 et seqq, OJ C 7, 10.01.2004, p. 3 et seq - Lindqvist.

Annex B. License conditions.

This is a public Report that is provided to the community under the license Attribution-NoDerivs 2.5 defined by creative commons http://www.creativecommons.org

This license allows you to

to copy, distribute, display, and perform the work

to make commercial use of the work

Under the following conditions:

Attribution. You must attribute the work by indicating that this work originated from the IST-OPTIMIS project and has been partially funded by the European Commission under contract number IST – 257115

No Derivative Works. You may not alter, transform, or build upon this work without explicit permission of the consortium

For any reuse or distribution, you must make clear to others the license terms of this work.

Any of these conditions can be waived if you get permission from the copyright holder.

This is a human-readable summary of the Legal Code below:

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORISED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED. BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. Definitions

"Collective Work" means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this License.

"Derivative Work" means a work based upon the Work or upon the Work and other pre-existing works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work will not be considered a Derivative Work for the purpose of this License. For the avoidance of doubt, where the Work is a musical composition or sound recording, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered a Derivative Work for the purpose of this License.

"Licensor" means all partners of the OPTIMIS consortium that have participated in the production of this text

"Original Author" means the individual or entity who created the Work.

"Work" means the copyrightable work of authorship offered under the terms of this License.

"You" means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

2. Fair Use Rights. Nothing in this license is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3. License Grant. Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

to distribute copies or phonorecords of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works.

For the avoidance of doubt, where the work is a musical composition:

Performance Royalties Under Blanket Licenses. Licensor waives the exclusive right to collect, whether individually or via a performance rights society (e.g. ASCAP, BMI, SESAC), royalties for the public performance or public digital performance (e.g. webcast) of the Work.

Mechanical Rights and Statutory Royalties. Licensor waives the exclusive right to collect, whether individually or via a music rights society or designated agent (e.g. Harry Fox Agency), royalties for any phonorecord You create from the Work ("cover version") and distribute, subject to the compulsory license created by 17 USC Section 115 of the US Copyright Act (or the equivalent in other jurisdictions).

Webcasting Rights and Statutory Royalties. For the avoidance of doubt, where the Work is a sound recording, Licensor waives the exclusive right to collect, whether individually or via a performance-rights society (e.g. SoundExchange), royalties for the public digital performance (e.g. webcast) of the Work, subject to the compulsory license created by 17 USC Section 114 of the US Copyright Act (or the equivalent in other jurisdictions).

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats, but otherwise you have no rights to make Derivative Works. All rights not expressly granted by Licensor are hereby reserved.

4. Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy or phonorecord of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this License Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this License. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any credit as required by clause 4(b), as requested.

If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or Collective Works, You must keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilising: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or (ii) if the Original Author and/or Licensor designate another party or parties (e.g. a sponsor institute, publishing entity, journal) for attribution in Licensor's copyright notice, terms of service or by other reasonable means, the name of such party or parties; the title of the Work if supplied; and to the extent reasonably practicable, the Uniform Resource Identifier, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5. Representations, Warranties and Disclaimer. UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE MATERIALS, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Termination

This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Collective Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. Miscellaneous

Each time You distribute or publicly digitally perform the Work, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Licensor and You.