D3.4 Legal recommendations on EU cloud computing services

How to protect personal data in cloud service contracts

www.cloudwatchhub.eu|info@cloudwatchhub.eu

Cloud computing technologies and services have evolved as fast as they have spread amongst client organisations. However, contracts regulating the provision of cloud computing services have not evolved at the same pace. The contracts are often offered by cloud providers in a standard and non-negotiable form, which may make it difficult for clients, whether they are private companies or public authorities, and which typically cover the role of data controllers under EU law, to discharge their duties towards data subjects and local or supranational Data Protection Authorities. This document provides some basic guidelines to cloud clients when entering a cloud computing contract. A series of recurrent contractual issues have been identified and addressed in a short and comprehensive way from the data protection law standpoint. References to other checklists and standards tackling issues critical for cloud services are also provided when relevant. In developing the document, the provisions of Regulation (EU) 2016/679 ("GDPR" or simply "Regulation"), which entered into force on 5 May 2016 and will start applying from 2018, were taken into account and incorporated, where relevant, in the text of the document.

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

CloudWATCH2 Mission

It is only when the innovation process is inclusive and open that we truly advance technology for humanity – from small businesses to public sector organisations and citizens as the new digital consumers. The use of open source software and open standards are becoming increasingly seen as enablers and levellers for public and private sectors alike, bundling skills to create new services and applications.

To support this CloudWATCH2 takes a pragmatic approach to market uptake and the exploitation of results coming from European sustainable competitiveness for wider uptake and commercial exploitation. It provides a set of services to help European R&I initiatives capture the value proposition and business case as key to boosting the European economy.

CloudWATCH2 services include:

- A cloud market structure roadmap with transparent pricing to enable R&I projects to chart exploitation paths in ways they had not previously considered, or help them avoid approaches that would not have been successful.
- Mapping the EU cloud ecosystem of products, services and solutions emerging from EU R&I projects. Identifying software champions and best practices in mitigating risks associated with open source projects, and ultimately, enable faster time-to-value and commercialization.
- Impact meetings for clustering and convergence on common themes and challenges. Re-use of technologies will also be of paramount importance.
- Promoting trusted & secure services through roadshows and deep dive training sessions. Giving R&I initiatives a route to users at major conferences or in local ICT clusters.
- A portfolio of standards for interoperability and security that can facilitate the realization of an ecosystem of interoperable services for Europe.
- Cloud interoperability testing in an international developer-oriented and hands-on environment. Findings will be transferred into guidance documents and standards.
- Risk management and legal guidelines with practical examples of cloud contracts' clauses that need to be assessed before purchasing cloud services to the cloud for private and public organisations to lower barriers and ensure a trusted European cloud market.

Disclaimer

The CloudWATCH2 (Think Cloud Services for Government, Business and Research) is funded by the European Commission's Unit on Software and Services, Cloud Computing within DG Connect under Horizon 2020.

The information, views and tips set out in this publication are those of the CloudWATCH2 Consortium and its pool of international experts and cannot be considered to reflect the views of the European Commission.

Document information Summary

Document title:	Legal Guide to the Cloud How to protect personal data in cloud service contracts
Main Author(s):	Theodora Dragan, Lucio Scudiero, Paolo Balboni, ICT Legal Consulting
Contributing author(s):	
Reviewer(s):	Nicholas Ferguson, Trust-IT Services & Damir Savanovic, Cloud Security Alliance
Target audiences:	Potential adopters of cloud services, SMEs and PAs
Keywords:	SLA, Legal issues, Cloud contract
Deliverable nature:	R
Dissemination level: (Confidentiality)	PU
Contractual delivery date:	M15
Actual delivery date:	M15
Version:	Final
Reference to related publications	

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

Executive Summary

Cloud computing technologies and services are evolving at a fast pace and new ways of delivering IT services have emerged on the market, many of which are driven by the explosion of the power and capability of mobile devices.

The legal models accompanying these developments are evolving too – though not at the same pace.

An increasing amount of attention is paid by cloud service clients (hereinafter also "CSCs") to cloud computing contracts, which are nonetheless still framed in standard forms by CSPs (hereinafter also "CSPs"). In this document CSCs are both private companies and public authorities – in practice, by CSCs, we refer to all entities that use cloud computing services (only individual users are excluded).

The contractual clauses to which CSCs usually pay the most attention pertain to:

- exclusion or limitation of liability and remedies, particularly regarding data integrity and disaster recovery;
- service levels, including availability;
- security and privacy, particularly regulatory issues under the European Union Data Protection Directive and the General Data Protection Regulation (hereinafter "GDPR"or "Regulation")[1];
- lock-in and exit, including duration, termination rights, and return of data upon exit from the contract;
- the ability of the provider to unilaterally change for service features.[2]

This document is aimed at the constituency of CloudWatch2, which breaks down as follows:

- Private entities (mainly SMEs);
- Public authorities (governments);
- Governments (public authorities);
- Research communities and academia.

Considering that it is, generally speaking, unlikely that such entities can negotiate terms and conditions of a cloud computing contract with the CSPs, the legal advice in this document is aimed at providing them with a set of guidelines to help them select, amongst different providers, the one which best suits their needs and gives the most adequate assurances regarding the protection of personal data under current European law, in particular under the GDPR.

[1] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[2] These issues have been found by a research into negotiated contracts performed by W. Kuan Hon, Christopher Millard & Ian Walden in Negotiating Cloud Contracts - Looking at Clouds from Both Sides Now, 16 STAN. TECH. L. REV. 81 (2012) - http://stlr.stanford.edu/pdf/cloudcontracts.pdf.

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

Glossary of terms

Here below it is a glossary of recurrent terms in this document with their definition. [3]

Cloud Computing - A paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

Cloud service client (CSC) - A party which is in a business relationship for the purpose of using cloud services; for the purposes of this document, consumers are excluded from this definition.

Cloud Service Provider (CSP) - A party which makes cloud services available.

Cloud SLAs – Documented agreement between the CSP and cloud service customer that identifies services and cloud service level objectives (SLOs).

Data controller – In accordance with Article 4(7) of the Regulation, data controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data location – The geographic location(s) where personal data may be stored or otherwise processed by the CSP**.**

Data portability – Ability to easily transfer data from one system to another without being required to re-enter data, in accordance with new Article 20 of the Regulation.

Data processor – In accordance with Article 4(8) of the Regulation, processor means "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

Data Protection Law – Regulation (EU) 2016/679, Directive 680/2016 and its implementing laws at national level, and Directives 95/46/EC, 2002/58/EC as far as applicable

Supervisory Authority (SA) – In accordance with the definition included in Article 4(21) of the Regulation, it means "*an independent public authority which is established by a Member State pursuant to Article 51*". Article 51(1) defines a *supervisory authority* as "*the*

[3] Some definitions are drawn from the "Standardisation guidelines for cloud computing service level agreements" elaborated by the Cloud Select Industry Group – Subgroup on Service Level Agreement (C-SIG-SLA). Available at the following address: https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines.

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

authority responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union".

Personal data – As defined in Article 4(1) of the Regulation, *personal data* means "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*"

Privacy Level Agreement (PLA) – a document to be used as an appendix to Cloud Services Agreements to describe the level of privacy protection that the CSP will maintain

Processing of personal data – This notion is defined in Article 4(2) as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

SMEs – Small and Medium Enterprises. Small and medium-sized enterprises (SMEs) are defined in the EU recommendation 2003/361. The main factors determining whether an enterprise is an SME are staff headcount (up to 250) and either turnover (up to € 50 m) or balance sheet total (up to € 43 m).

Public Authorities – The scope of the concept is much debated in EU case law and has been interpreted in different ways. However, for the purposes of these guidelines, the term "public authorities" refers to a public sector body or a legal entity governed by private law with a public service mission providing adequate financial guarantees.

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

Table of Contents

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

1 Objectives of this document

The objective of this document is to provide some basic guidelines to cloud clients when entering a cloud computing contract. Some recurring contractual issues have been identified and addressed in a short and comprehensive way, from the data protection law standpoint. References to other checklists and standards tackling issues critical for cloud services are also provided where relevant.

The guidelines are for informative purposes only. They have been drafted by ICT Legal Consulting as part of the CloudWatch2 project. The guidelines will be available on www.cloudwatchhub.eu.

These guidelines are not meant to be exhaustive and cannot replace the legal advice provided by expert lawyers when negotiating cloud service contracts. The main addressees of these guidelines are SMEs, on the one hand, and public authorities (hereinafter "PAs"), on the other hand. Whereas the main issues related to cloud computing are common to both, some aspects may be specific to SMEs or PAs and will be duly highlighted to the reader.

The guidelines contribute to CloudWATCH2's objective of offering educational services on risk management and legal issues to lower adoption barriers for SMEs and public administrations.

Figure 1 indicates CloudWATCH2 outputs highlighting WP3 activities.

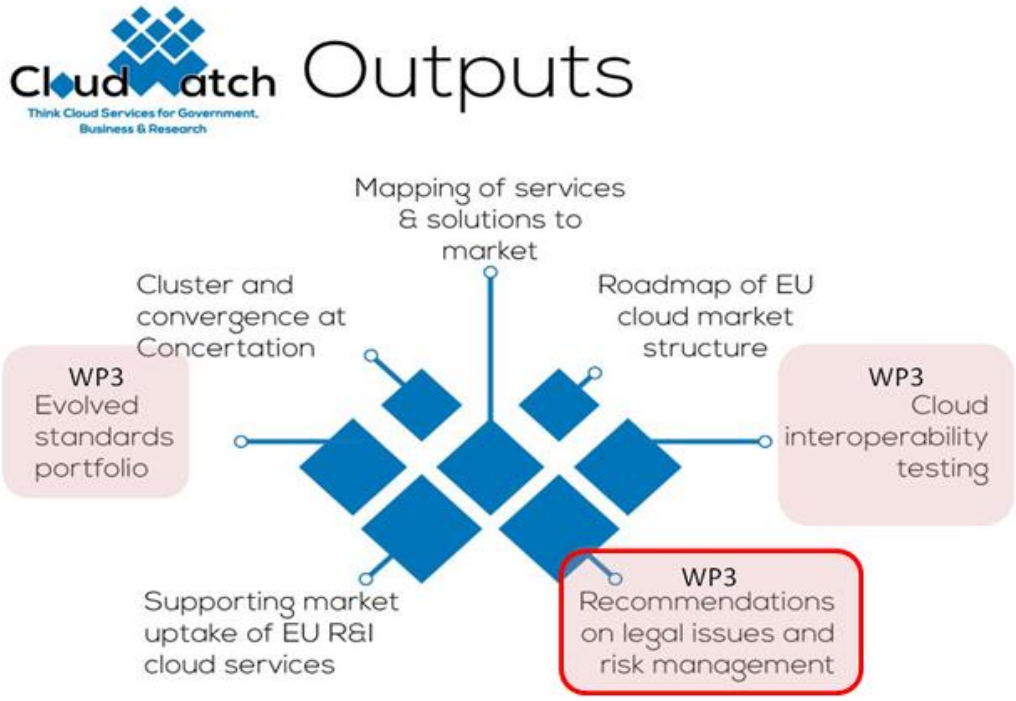

Figure 1 CloudWATCH2 outputs and WP3 activities

This activity (T3.4) focuses on contributing to making the cloud more transparent to potential adopters by addressing the legal aspects of cloud services by helping innovative companies and high-tech SMEs

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

(including providers within the ecosystem) and Public Authorities to better understand the relevant contractual and EU data protection legal framework and to make meaningful assessments of the right issues before starting to use, buy or sell cloud-based services.

In addition to this report, CloudWATCH2 has also provided a "Legal Services" section[4] on the CloudWatchHUB.eu. Indeed, content from this report will be used to further enrich this section. The section also includes the following outputs from CloudWATCH2:

- FAQs on legal terms in cloud service contracts[5]: FAQ document to answer the common questions that SMEs have with regard to cloud computing.
- Contractual clauses in cloud contracts:[6] The document provides sample clauses that consumers can expect to find in Cloud Service Agreements, in order to give readers a starting point for understanding the content of a cloud contract and the typical approach that CSPs take with regard to the various contractual aspects. The clauses have been drafted from the perspective of customer SMEs. However, they may constitute a good starting point for Public Authorities as well, save what is provided for them by specific legislation applicable to them, which needs to be carefully assessed on a case by case basis.
- Legal Tips:[7] Regular provision of articles and updates on legal matters related to cloud computing on a monthly basis.

1.1 SMEs

The main issue that SMEs are confronted with, when considering moving to the cloud, is related to the fact that they sometimes lack the necessary bargaining power needed to properly negotiate the contract with CSPs. Therefore, they are usually "stuck" with the standard terms and conditions, especially with regard to the clauses on termination or limitation of liability of the CSPs. For this specific reason, SMEs should very carefully read the cloud contracts and ensure that they choose the CSP that best fits their needs – not just from a business perspective, but also from a data protection perspective. Given the legal obligations introduced by the Regulation with regard to data controllers, perhaps the most important factor to take into account when considering a cloud provision agreement is how well the CSP is willing and able to collaborate with the SME, as client and data controller, to enable it to fulfil its legal duties, for example those related to data subjects' rights, data transfer requirements or personal data breach notification. In this regard, the GDPR gives some leverage to SMEs over CSPs, as it expands the scope of application of EU data protection law requirements, recognising the role that processors also play in protecting personal data. Unlike the EU Data Protection Directive (95/46/EC, hereinafter 'the Directive') currently in force, with the GDPR processors are no longer outside of the ambit of the rules.

[4] http://www.cloudwatchhub.eu/legal-services
[5] http://www.cloudwatchhub.eu/legal-week
[6] Http://www.cloudwatchhub.eu/sites/default/files/CloudWATCH%20Contractual%20Clauses%20in%20Cloud%20Contracts.pdf
[7] http://www.cloudwatchhub.eu/legal-tips

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

Throughout the guidelines, we point out when a specific aspect is particularly important for SMEs to take into consideration.

1.2 PAs

Public Authorities (PA) may have, compared to SMEs, more bargaining power in the light of their size and/or legal mission. However, for the same reasons, PAs may also have constraints and/or specific issues to deal with before entering a cloud contract, linked, for example, to specific rules on the provisioning of public services and on public procurement, as well as particular obligations in terms of security. This is also due to the fact that PAs process huge amounts of data in their public role, for which any sort of data breach has the potential of being very harmful, given the various links of the data subjects' data and the potentially sensitive information about the data subjects. Therefore, PAs should pay particular attention to the data security level that is provided by the CSP and ensure that threats, leaks or cyber-attacks are safeguarded against properly.

2 Pre-contractual phase

2.1 Risks and opportunities for the cloud service client

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or CSP interaction."[8]

Users are attracted to cloud services due to the features inherent to the cloud model, such as the possibility to access a broad network, the ability to pool and optimise resources, accessing services with elasticity and scalability, all the while reducing the costs and, to some extent, the regulatory risks.

The outsourcing of computational, storage and platform services to CSPs, however, does not come without risks; this is particularly relevant for the protection of personal data processed in the cloud.

The Supervisory Authorities of the Member States (SA) have divided the main risks for privacy and protection of personal data in the cloud into two categories:[9]

- Lack of control over personal data;
- Lack of information on the processing of personal data.

[8] National Institute of Standards and Technology (NIST), Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011, Page 3. Available at the following website: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[9] Article 29 Working Party, "Opinion 05/2012 on Cloud Computing", Adopted on July 1st 2012, pp. 5-6. Available at the following website: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

Pondering the trade-off between the expected advantages of outsourcing to CSPs and the risks arising for personal data in the cloud is a preliminary step that every organisation has to take before purchasing cloud services.[10]

2.2 Deciding whether or not to outsource cloud services

In view of contracting cloud services with big CSPs, CSCs are advised to perform both an internal and external due diligence check.

Legal tips and recommendations

For **internal due diligence**, **SMEs** should:

- Define their privacy, security and compliance requirements;
- Identify what data, processes or services they want to move to the cloud;
- Analyse the risks of outsourcing services to the cloud;
- Identify what security controls are needed to protect their employee data once transferred to the cloud;
- Define responsibilities and tasks for security control implementation;

For **external due diligence**, SMEs should:

- Assess whether the CSP meets their privacy and data protection requirements using the Privacy Level Agreements (PLA);
- Check whether the CSP holds any certification or attestation released by an independent third party;
- Consider whether the terms of service can be amended, how and by whom;

Understand whether and how to monitor the security controls implemented by the CSP. For **internal due diligence**, **PAs** should:[11]

- Verify whether they have a National Information Asset classification scheme which has an impact on the type of services and/or architectural models to be purchased;

[10] For a complete overview of the risks posed by cloud computing read ENISA's paper on Cloud Security Risk Assessment, available here https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

[11] See also *PICSE project*, *Guide to Cloud Procurement - Roadmap for Cloud Service Procurement for public research organisations*. Available at the following website: http://www.picse.eu/sites/default/files/Annex1_Guidetocloudprocurement_webversion_0.pdf.

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

- Ascertain whether they have an obligation to make the source code of software developed on their specific request available to other Public Administrations, together with the relevant documentation and an open license:
- Assess whether the CSP holds a formal authorisation or is part of an accreditation system, where applicable;
- Write an effective cloud tender;
- Consider the need for a pilot phase;
- Define objective eligibility criteria for CSPs;
- Identify technical requirements clearly;
- Identify legal requirements clearly, especially regarding data location;
- Analyse the risks of outsourcing services to the cloud;
- Identify what security controls are needed to protect their employee data once transferred to the cloud;
- Define responsibilities and tasks for security control implementation;

For **external due diligence**, PAs should:

- Carry out pre-procurement market consultation and engagement;
- Assess whether the CSP meets their privacy and data protection requirements using the Privacy Level Agreements (PLA);
- Assess whether the CSP relies on commercially available certifications and whether it is based on self-attestation /assessment.
- Make sure that the cloud services under consideration do not impinge on the obligations of the PAs to facilitate re-use of documents and data under Directive 2003/98/EC on the reuse of public sector information (hereinafter "PSI Directive").

3 Entering a cloud service contract: major issues

The following recurring issues have been identified with regard to the negotiation of a contract for the provision of cloud services, based on the direct and indirect experience of ICT Legal Consulting.

3.1 Jurisdiction & Applicable law

Cloud service contracts often contain clauses whereby the competent jurisdiction and the applicable law are set by the agreement between the parties involved.

A distinction has to be made between the two concepts.

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

Finding the competent jurisdiction means allocating the enforcement of the contract to a certain, competent judge, whereas finding the applicable law means finding the set of substantive rules applicable to a given contract. A possible consequence of this distinction may be that a judge of Member State "A" is called to enforce a cloud computing contract, or a part thereof, on the basis of the law of Member State "B".

From a purely contractual standpoint, the parties autonomously decide in which jurisdiction they want the contract to be enforced in. Generally speaking, the possibility to mutually set the competent jurisdiction is recognised by the principle of contractual liberty. In practice, however, the CSP is the entity that selects the jurisdiction it prefers, whereas the CSC often only has the opportunity of "taking it or leaving it". This situation may undergo exceptions when the client is a PA. In this case, it is the law regulating the public procurement that usually stipulates that the jurisdiction over the contract to which a PA is party belongs to national courts.

Regarding the applicable privacy law, Regulation (EU) 2016/679 sets out the territorial scope in Article 3. In particular, at paragraph 1, the Regulation sets out that its provisions apply to "*the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not*". Therefore, if either the data controller's (CSC) or data processor's (usually, the CSP is the data processor) establishment is in the EU, the provisions of the Regulation apply.
Moreover, paragraph 2 of Article 3 sets out that, the Regulation also applies where neither the controller, nor the processor are established in the EU, but "*the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union*." The latter case is likely to catch most of the CSPs established outside the Union in the scope of European data protection rules. The Regulation, in fact, has a wider territorial scope than its predecessor piece of legislation, the Directive 95/46/EC.

Another piece of relevant legislation is the e-privacy Directive 2002/58/EC, whose application is triggered by the provision of publicly available electronic communications services in public communications networks (telecom operators) by means of a cloud solution. When the CSP is also a provider of publicly available electronic communications services in public communications networks, this law applies.

Legal tips and recommendations applicable to both SMEs and PAs:

- Contractual arrangements regarding the jurisdiction and the applicable law are found in the Cloud Service Agreement;
- The reform of European data protection rules has widened the territorial scope of the latter; the GDPR may very likely apply to CSPs established outside the European Union, regardless of what contracts provide;
- Bear in mind that under the GDPR the data processors have now direct legal obligations which are also enforceable by the data subjects.

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

Legal tips and recommendations for PAs:

- Litigation holds and public records responsibilities are critical and should be included in contracts for cloud services. Compliance with public records laws and legal data holds should also be a core part of cloud contracts;
- Check whether the CSP is also able to carry out the activity of conservation and certification of electronic document prescribed by law (e.g. electronic health records) to public and private bodies, and is accredited as conservator with the national accrediting authority.

3.2 Privacy Roles

A correct understanding of the roles in the processing of personal data performed by means of cloud computing technologies is functional to the correct allocation of legal obligations and responsibilities between the parties of a cloud computing contract.

According to the standard allocation of responsibilities,[12] the controllership of personal data processed in the cloud belongs to the client, whereas the CSP is usually the data processor.

Departing from the rationale underpinning Directive 95/46/EC, the GDPR has substantially increased the level of accountability directly required to data processors. As a consequence, for example, CSPs can now be the direct addressees of a claim by data subjects for material or immaterial damage they have undergone as a result of an infringement of the GDPR, in particular of the obligations therein specifically directed to processors; this holds true also when the CSPs acted outside or contrary to lawful instructions of the controller. Moreover, CSPs have the obligation to keep the records of processing activities (when they have more than 250 employees), to notify the controller without undue delay after becoming aware of a personal data breach, regardless of whether the controller is a provider of publicly available communication services, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, to seek the data controllers' authorization before engaging another processor, and to impose on the latter the same data protection obligations as set out in the contract or other legal act between the controller and the processor.

Legal tips and recommendations for both SMEs and PAs:

- Clearly allocate the data protection roles between the parties;
- Choose a CSP that guarantees compliance with European data protection law;
- Define the degree of autonomy left to the CSP, acting as data processor, in the choice of methods and technical or organisational measures;

[12] This model is taken as a reference by the European DPAs in "Opinion 05/2012 on Cloud Computing", Adopted on July 1st 2012, p.7.

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

- Bind the CSP, acting as a data processor, by means of a specific data processing agreement, or at least make sure that the boundaries of the data processing are clearly defined in the cloud service agreement and that the activities outsourced to the CSP are adequately identified;
- Avoid CSPs that use complex chains of sub-contractors located outside the EU; if this is not possible, decide whether to provide CSPs with a general or specific authorization to engage further CSPs;
- Verify whether the contract contains provisions aimed at limiting the CSP's liability for breach of data protection rules;
- Verify whether the contract contains provisions aimed at avoiding that the controller is entitled to claim back from the processor involved in the same processing that part of the compensation corresponding to their part of responsibility for a damage, where a controller has paid full compensation for the damage suffered by the data subject according to European data protection rules.

3.3 Amendments to the contract

CSPs often include clauses in contracts whereby they retain the right to unilaterally change the cloud contract in their own interest, without including the need to notify the other party.

In legal terms, this is quite problematic; therefore, it is paramount to verify whether the contract requires the CSP to give an acceptable notice for any changes to the services, or establishes the client's right to terminate the contract in the event of materially detrimental changes to it.

Legal tips and recommendations for SMEs and PAs:

- Contracts should clearly regulate which services and under what conditions, including procedural ones, can be modified in the course of the provision of services;
- Changes that are materially detrimental to the level of a mission critical service or/and to the level of protection of personal data should be explicitly excluded from the contract;
- Changes should not be implemented without giving notice to the client;
- The written agreement of the client, or at least the client's right to be prior notified of any changes to the contract, may be foreseen therein;
- The clients should verify whether the contract provides for their right to terminate it upon unwanted, unnoticed and/or detrimental amendments to the contract.

3.4 Data location and transfers of data

The provision of cloud services very often entail that personal data are processed in servers and infrastructures located outside the European Union. It is unavoidable, in such cases, that personal data are transferred outside the EU. The utmost attention must be paid to the rules governing the flow of personal data from the European legal space to the outer world.

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

According to the Regulation, personal data can be transferred outside the European Union on the basis of an adequacy decision related to the country where the recipient of the transfer is located, pursuant to Article 45 thereof, or where specific safeguards have been put in place, in accordance with Article 46 thereof (one particular example of such safeguards are the Binding Corporate Rules, which are specifically addressed in Article 47) or if one of the derogations contained in Article 49 applies[13].

Therefore, for a personal data transfer to be valid, one of the provisions contained in Articles 45, 46, 47 or 49 must apply. Given that only a few countries have been awarded an adequacy decision by the European Commission (full updated list is available here: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm), and that the derogations in Article 49 apply in limited cases, most situations will require adequate safeguards to be adopted, pursuant to Articles 46-47.

Legal tips and recommendations for SMEs and PAs:

- Verify if the processing of personal data takes place in countries that have been subject to an adequacy decision; in that case the transfer can be lawfully carried out;

[13] GDPR, **Article 49 - Derogations for specific situations**

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:
(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
(d) the transfer is necessary for important reasons of public interest;
(e) the transfer is necessary for the establishment, exercise or defence of legal claims;
(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.
Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.
2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.
3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.
4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.
5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.
6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

- In case the processing takes place in countries that have not been subject to an adequacy decision, one of the following "adequate safeguards", in accordance with Article 46, must be in place:
    - The CSP has adopted binding corporate rules in accordance with Article 47;
    - SMEs and CSPs enter into standard data protection clauses adopted by the Commission (the ones adopted with Decision 2010/87/EU can still be used);
    - SMEs and CSPs enter into standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
    - The SME and/or the CSPs adhere to an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
    - The SME and/or the CSPs hold an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

Legal tips and recommendations for PAs:

- The tips recommended for SMEs above are also applicable to PAs;
- Additionally, in case the processing takes place in countries that have not been subject to an adequacy decision, an additional "adequate safeguard", in accordance with Article 46 can be put in place, ***in addition to*** the list provided above under "Legal tips and recommendations for SMEs":
    - The transfer takes place on a legally binding and enforceable instrument between public authorities or bodies.

3.5 Processing of personal data by sub-contractors

CSPs may outsource part of the processing necessary for the functioning of the cloud to sub-contractors. These sub-contractors may receive personal data from the client of cloud services, and may be located outside the EU. They can lawfully process personal data flowing from the EU only when one of the conditions mentioned in the preceding paragraph have been met.

The chain of sub-processors may be very long and scattered, which may result in loss of control over personal data, difficulties in the exercise of data subjects' rights, and lack of accountability on the side of the data processor.

Legal tips and recommendations for both SMEs and PAs:

- In Opinion 5/2012[14], the European DPAs recommended Processors/providers to inform the client about the sub-processing in place, detailing the type of service subcontracted, the

[14] See the Opinion 05/2012 on Cloud Computing, p.9, 10 and 20, cited above.

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

characteristics of current or potential sub-contractors and that these entities guarantee to the CSP to comply with the applicable EU data protection legislation;

- Under the GDPR, the CSP must ensure that its sub-contractors are contractually bound to him by the same obligations and standards he has agreed to with the controller; the model contractual clauses approved by the European Commission constitute a useful tool to this effect;
    - Under the GDPR, the Supervisory Authorities may adopt standard clauses for the purpose of regulating the relationship between data processors and sub-processors; if such a set of clause is available, the CSC should ensure it is used by the CSP with its sub-processors;
- The CSC has the possibility to decide whether to provide the CSP with a general or specific authorization to engage further providers; the CSP cannot engage sub-providers without such authorization by the controller;
- The controller should have contractual recourses against the processor in case of any breach of the contract caused by the sub-processor.

3.6 Data subjects' rights (or "Intervenability")

In the framework of the Regulation, the data subjects have the following rights:

- right of access (Article 15);
- right to rectification (Article 16);
- right to erasure (Article 17, "right to be forgotten");
- right to restriction of processing (Article 18);
- right to data portability (Article 20);
- right to object (Article 21);
- right not to be subject to a decision based solely on automated processing (Article 22); [15]
- right to compensation (Article 82).

When reading a cloud computing contract, the client should check whether the CSP guarantees full cooperation in ensuring an effective and easy exercise of rights on the part of the data subjects, including in cases when data is further processed by subcontractors.

Legal tips and recommendations for both SMEs and PAs:

[15] Chapter III of the Regulation is dedicated to the Rights of the Data Subject.

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

- The contract between the client and the CSP should stipulate that the CSP supports the client in facilitating the exercise of data subjects' rights and ensuring that the same holds true for his relation to any subcontractor;

- Verify whether the contract contains provisions aimed at avoiding that the controller is entitled to claim back from the processor involved in the same processing that part of the compensation corresponding to their part of responsibility for a damage, where a controller has paid full compensation for the damage suffered by the data subject according to European data protection rules.

3.7 Lock-in and Interoperability

The lock-in effect may be a consequence of the CSP using proprietary data formats and service interfaces, which render the interoperability and portability of data from a CSP to another difficult if not impossible. It is noteworthy that the GDPR introduces a brand new right to data portability that should enable the data subject "*to transmit those data to another controller without hindrance from the controller to which the data have been provided*".

The right to data portability Is surely enforceable against private data controllers, whereas according to Recital (68) of the GDPR "*by its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties*". Data portability however depends on the availability of standards which lead to interoperability. Therefore, SMEs should ensure that the CSP they choose uses interoperability standards that would make the data portable at the request of the data subjects; as clarified above, the latter obligation does not apply to PAs processing personal data in the cloud in the exercise of their public duties.

The lock-in effect might also hurdle the migration of services that the client developed on a platform offered by the original CSP (PaaS).

Legal tips and recommendations for both SMEs and PAs:

- Focus on whether and how the CSP ensures data portability (for moving data between systems) and interoperability (when upgrading software or when migrating between two competing systems). Ensuring the data subject's right to data portability is mandatory for SMEs when the conditions contained in Article 20 of the GDPR are met.

3.8 Service Level Agreements ("SLAs")

Service Level Agreements constitute a very important component of a cloud computing contract.

SLAs identify the services and the service level objectives that the CSP offers to the cloud client. The SLAs are expressed in terms of metrics on the performance of the services; the metrics are usually measured in numbers. Neither the terminology of SLAs nor the willingness to negotiate SLAs are the

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

same between different CSP. This has triggered initiatives aimed at standardizing Service Level Agreements between CSP and clients at the European and international levels.[16]

SLAs may define the performance of the services (e.g. the availability of the service, the response time etc.), the security (e.g. service reliability, authentication and authorization, security incident reporting and management etc.), the way data are managed (data classification, data lifecycle etc.) and sometimes also relevant provisions concerning the protection of personal data.

Legal tips and recommendations for both SMEs and PAs:

- CSCs should attentively read and analyze the SLAs;
- Check which mechanisms are put in place to guarantee continuity of operation in case of severe incidents;

  Clients should also verify whether the cloud service agreement provides for remedies to service levels breaches or if it sets out service credits for SLA breaches (such as money back rebates or monetary compensation).

For a check list of essential items that should appear in a cloud SLA, please refer to the SLA Common Reference Model and free online resources from such as the SLA-Aid[17] and related use cases[18] provided by the EC-funded project SLA-Ready.

3.9 Termination of the contract

Termination of cloud computing contracts is a critical phase which initiates a process in which the client must be able to retrieve the data transferred to the cloud, within a specified period of time, before the CSP irreversibly deletes them.

Legal tips and recommendations for both SMEs and PAs:

- The steps of the termination process must be clearly identified in the cloud service agreement between the parties;
- A good cloud service agreement should contain provisions regulating the data retrieval time i.e. the time in which clients can retrieve a copy of their data from the cloud service. The data retention period should also be included, as well as the procedures followed by the CSP in

[16] See, above all, the initiative undertaken by the DG CONNECT of the EU Commission that set up the Cloud Select Industry Group – Subgroup on Service Level Agreement (C-SIG-SLA) to work towards the development of standardisation guidelines for cloud computing service level agreements. The Group finalized its work in June 2014. The result thereof is available at the following address: https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines. See also EC-funded projects such as SLA-Ready www.sla-ready.eu/

[17] http://sla-aid.sla-ready.eu/

[18] http://www.sla-ready.eu/sla-ready-new-use-cases

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

order to transfer personal data back to the client or to allow the latter to migrate to another CSP.[19]

3.10 Privacy Level Agreements ("PLAs")

Privacy Level Agreements (PLAs) are intended to be used as an appendix to Cloud Services Agreements to describe the level of privacy protection that the CSP will maintain. An exhaustive outline of PLAs has been provided by the Privacy Level Agreement Working Group established within the Cloud Security Alliance.[20]

In the PLAs, the CSP defines the level of privacy and protection it affords to personal data hosted in the cloud.

PLAs may tackle several issues:

- Identity of the CSP (and of Representative in the EU, as applicable), its role, and the contact information for the data protection officer and information security officer;
- Categories of personal data that the customer is prohibited from sending to or processing in the cloud;
- Ways in which the data will be processed;
- Personal data location;
- Data transfer;
- Data security measures;
- Monitoring;
- Third-party audits;
- Personal data breach notification;
- Data portability, migration, and transfer-back assistance;
- Data retention, restitution, and deletion;
- Accountability;
- Cooperation;
- Law enforcement access;

[19] Also see paragraph 3.7. above for "Lock-In and Interoperability".
[20] See the "Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union" drafted by the Privacy Level Agreement Working Group set within the Cloud Security Alliance. The outline is available at the following website https://cloudsecurityalliance.org/research/pla/.

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

- Remedies;
- Complaint and dispute resolution;
- CSP insurance policy.[21]

Legal tips and recommendations for both SMEs and PAs:

- PLAs could be used as a guide to compare the privacy policies of different CSP;
- PLA checklists and guidelines may be a useful tool to get acquainted with the minimum level of data protection that a CSP must ensure.

4 Conclusion

Cloud computing solutions are offered in a wide variety of models; they change considerably from one CSP to another. As already specified above, the guidelines contained herein deal with cloud computing contracts from a general perspective, with particular emphasis on CSCs being SMEs or public authorities. The guidelines identify, at high level, some of the clauses that require great attention by the CSCs.

Solutions to the majority of issues listed in this document may significantly change according to the deployment model (private, public or hybrid cloud computing) and in consideration of the service model (SaaS, PaaS, IaaS).

Moreover, the nature and size of both the CSP and the clients has a significant influence on the way contractual clauses are drafted and viable legal solutions found.

Big clients with a considerable "countervailing buying power" are able to exert greater pressure on CSPs. Additionally, entities such as governments, or even smaller public administrations, might have specific needs in terms of data security and business continuity because of the mission critical services they provide to the public. These are all cases that often require the provision of tailored cloud services and specific legal guidance.

Some useful legal tools are now available to the large public thanks to the effort made at the EU level under the European Commission's initiative called "European strategy for Cloud computing – unleashing the power of cloud computing in Europe", such as:

- Cloud Service Level Agreement Standardisation Guidelines - http://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines ;
- Certification in the EU Cloud Strategy - https://resilience.enisa.europa.eu/cloud-computing-certification/certification-in-the-eu-cloud-strategy.

[21] Outline drawn from the CSA's Privacy Level Agreement Outline, cited above in footnote 20.

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

A further tool has been added to the ones already availablein 2015, when the Cloud Select Industry Group on Code of Conduct completed its task and delivered a code of conduct for the cloud computing providers that has been submitted to the Article 29 Working Party for approval.[22] The "Code of Conduct for CSPs" Revised v1.0 was published on 22 June 2016 and intends to "*make it easier and more transparent for cloud customers to analyse whether cloud services are appropriate for their use case*".[23] In particular, it is hoped that "the transparency created by the Code will contribute to an environment of trust and will create a high default level of data protection in the European cloud computing market, in particular for cloud customers such as Small and Medium enterprises (SMEs) and public administrations.

5 Next steps

The next steps include the publishing of the document on the CloudWATCH2 website and the dissemination and promotion via the various social media platforms of ICT Legal Consulting and CloudWATCH2.

The objective is, of course, to use the best endeavours to ensure that the target audience, consisting of SMEs and PAs, have access to this informative document and can use it as a starting point when considering which CSP best fits their specific needs. Given that there is usually little room for negotiation, it is important to understand the various stages of cloud computing contracts, from selecting the right provider to successfully migrating the data to a different system following termination of the contract for whatever reason. By using a mix of marketing and communications strategies, it is hoped that the target audience will have access to the document and will be able to make more informed choices as a result.

[22] See here for more information: https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-code-conduct

[23] The Code of Conduct is available here: https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers.

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748

6 Annex 1 - Document Log

DOCUMENT ITERATIONS		
V0.1	First Version	Paolo Balboni, , Lucio Scudiero, Theodora Dragan, ICT Legal Consulting
V0.2	Partner internal review	Damir Savanovic, CSA
V0.3	Partner internal review	Nicholas Ferguson, Trust-IT
V0.4	Pre-final review	Theodora Dragan, ICT Legal Consulting
V0.5	Pre-final review	Lucio Scudiero, ICT Legal Consulting
V0.Final	Final version	Lucio Scudiero, ICT Legal Consulting

CloudWATCH2 is funded by the EC Horizon2020 - DG Connect Software & Services, Cloud. Contract No.644748