1. Background

1.1. What is the 'Cloud Computing' model?

'Cloud computing' or in short 'Cloud' can be simply defined as the service of providing computational capacity over the internet. The Cloud users "rent" capabilities such as data storage, computer processing and software applications, from cloud providers utilising "clouds" of on-line resources (networks, servers, storage, applications and services).

1.2. Is there a categorization of the different cloud services?

There are generally three distinct service models of cloud computing[1]:

a) Software as a Service (SaaS) - the client uses provider's applications (mainly industry –standard software packages) running on cloud infrastructure
b) Platform as a Service (PaaS) - the client deploys onto the cloud infrastructure, applications created using programming languages and tools supported by the provider
c) Infrastructure as a Service (IaaS) – the client deploys and runs arbitrary software including operating systems and applications with the support of fundamental computing resources provided by the cloud such as processing, storage and networks

1.3. What is the novelty of Cloud Computing?

Outsourcing IT services and transferring data and software across borders through internet is not a new idea, especially for multi-national and large companies. However, Cloud Computing is an innovative IT paradigm in that it enables the rapid and elastic provision of computing services on a 'pay-as-you-go' mode, in a highly distributed environment.

This possibility for provision of elastic computing capabilities on large scale encapsulates the main thrust and source of risks associated with the cloud services. On the one hand, private and public organisations could benefit from the agile usage of advanced IT services reducing at the same time the IT infrastructure cost. On the other hand, a number of security, privacy and trust challenges such as the secure management of virtual resources and limitations in providing granular access controls and audit trails for regulatory and forensic purposes are yet to be addressed[2]. Apart from security, privacy and

[1] Classification provided by Mell, P., Grance, T., The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology, Special Publication 800-145, 2011, in: https://www.google.com/search?sourceid=ie7&q=outlook&rls=com.microsoft:el:IE-SearchBox&ie=UTF-8&oe=UTF-8&rlz=1I7ACAW_elIT432IT432

[2] For a comprehensive analysis of the security, privacy and trust challenges inherent to the cloud see:
Robinson, N., Valeri, L., Cave, J., Starkey, T., *The Cloud: Understanding the Security, Privacy and Trust Challenges*, Final Report prepared by RAND Europe, time.lex and the University of Warwick for Unit F.5 ,Directorate General Information Society and Media, European Commission, 2010 in:

operational concerns, the cloud relates also to regulatory problems encountered already in the area of traditional IT outsourcing such as uncertainties over the applicable law when different jurisdictions are entangled.

1.4. Is there a regulatory framework in the EU context?

Cloud computing is considered as "a fundamental change in the way computing power is generated and distributed" and a revolutionary service whose further development "could deliver a net gain of 2.5 million new European jobs, and an annual boost of EUR 160 billion to EU GDP by 2020"[3]. With a view to reaping the benefits and responding to challenges related to the Cloud Computing, the European Commission has established a specific strategy aiming at furthering wide-spread cloud use and cloud provision[4]. The Commission's Communication 'for unleashing the potential of cloud computing in Europe' refers to all these policy initiatives undertaken in the framework of the Digital Agenda for Europe and touching upon cloud computing issues such as the e-commerce directive, the Commission's proposal on e-identification and authentication and the review of the data protection directive. Furthermore, key actions needed for the development and uptake of cloud are laid down: standardisation of the rules applying to cloud provision, adoption of certification requirements to guarantee compliance with these rules and development of model contacts for safe and fair terms along with the establishment of a European Cloud Partnership to function as a reference model originated from the public sector are the main priorities set.

Given the diffusion of cloud computing services and the necessity for its seamless further development, it is considered useful to clarify the role of export controls with regard to the cloud phenomenon.

2. Dual-use exports controls and cloud computing

2.1. Objectives

Articles 2.2 (iii) and 2.3(ii) of the Regulation stipulate that the transmission of controlled technology or software by electronic mail or any other electronic means to a destination outside the EU, as well as the act of making available in an electronic form such software and technology to persons or partnerships outside the EU is subject to authorisation.

The very nature of cloud computing relates to the transfer of technology/software over the internet and thus, it should be treated as an Intangible Transfer of Technology (ITT) practice. Whenever controlled

---

http://cordis.europa.eu/fp7/ict/security/docs/the-cloud-understanding-security-privacy-trust-challenges-2010_en.pdf

[3] Bradshaw,D., Folco,G., Cattaneo, G., Kolding, M., *Quantitative Estimates of the demand for Cloud Computing in Europe and the Likely Barriers to Take-up*, International Data Corporation (IDC), 2012 in: http://ec.europa.eu/information_society/activities/cloudcomputing/docs/quantitative_estimates.pdf

[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Unleashing the Potential of Cloud Computing in Europe, COM(2012) 529 final, in: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM%3A2012%3A0529%3AFIN%3AEN%3APDF

data and technology -originated from the EU- are transmitted or made available to persons located in third countries, either through traditional IT services or via cloud computing services, an export control authorisation shall be required.

2.2. Export control implications relating to the usage of cloud computing

From an export control perspective, the determining factor for imposing an authorisation requirement should be the location of the intended final recipient(s). However, the usage of cloud services may entail a multiplicity of locations from where sensitive data may be accessed. This happens because cloud providers utilise distributed networks of servers programmed to search for the fastest and cheapest transmission routing or processing time, and located anywhere an internet connection is available.

This constant shifting of data locations poses two main problems: first, data allocations occur without the knowledge of cloud users and thus, cloud users are not aware of all different locations from which their sensitive information might be accessed; second, and interrelated to the previous, there is much uncertainty as regards who could access the controlled data during the interval phase of continuing data allocations. For instance, IT administrators might be able to access the sensitive information from different locations violating inadvertently or even intentionally export control provisions. In this case an export authorisation shall be sought irrespective of the final recipient.

With a view to reducing the uncertainties and overcome the problems described above three options are available:

a. The cloud user should ask assurances from the cloud provider that the latter will rely solely on servers within the EU and thus, an export authorisation would not be normally required.

b. In case that controlled data will be uploaded to and processed over servers located outside the EU, the cloud users should ask guarantees from the cloud providers that the local IT administrators are prevented by technical or contractual means to access the data. In the event of failure to furnish such guarantees, cloud users shall ask export authorisations for the transfer of data to any IT administrator located outside the EU.

c. In order to avoid such an administrative burden cloud users may opt for encrypting those controlled data entrusted to cloud services. The competent licensing authorities should pursue national legislation clarifying the types of technologies for which such a possibility will be applicable.

Adopting such a straightforward approach vis-à-vis cloud computing, presupposes that certain security guarantees, referred below in paragraph 3.4, are satisfied.

3. Dealing with cloud computing cases

3.1. Role of the cloud user

Article 3(ii) of the regulation clarifies that any natural or legal person or partnership who decides to transmit or make available software and technology by any electronic means to a destination outside the EU must be considered as exporter. The power of such a decision lies with the cloud users, who shall apply if necessary, for an export authorisation in the Member State where they are located and the data uploaded[5]. In addition, the cloud users, i.e. the exporters should be in position to furnish the certification mentioned in paragraph 3.4., if the competent authorities require so.

3.2. Object of the transaction and applicability of exemptions

The Dual-use regulation in Annex I (categories from 0 to 9) determines which technologies and software programmes are controlled as a result of their possible contribution to the development, production or use of controlled tangible items. It is reminded that listed technologies "*remain under control even when applicable to non-controlled goods*", meaning regardless of whether their export involves a controlled item or not. The Nuclear Technology Note (NTN) and the General Technology Note (GTN) in Annex I of the regulation, provide the particular instances where technology is not controlled:

- technology which is the minimum required for the installation, operation, maintenance and repair of authorised goods
- technology which is the minimum necessary for patent applications (only for categories 1 to 9), falls "in the public domain" or constitutes "basic scientific research"

The General Software Note (GSN) decontrols software available in large commercial distribution or falling "in the public domain".

Whenever the transfer of information through cloud services concerns software and technology falling within the scope of these exemptions an export authorisation shall not be required.

3.3. Intended end-users and destinations

There are generally two possibilities:

- the final recipient(s) is either an EU or non-EU citizen located in a third country.

  The transaction would require an export license, unless the export concerns technologies and destinations for which a Union General Export Authorisation is applicable or it is covered by a Global Export Authorisation or National General Export Authorization issued by the Member State where the exporter is located and the data uploaded.

- the final recipient(s) could be a person either an EU or non-EU citizen located within the EU.

[5] Article 9 (2) spells out that export authorisations shall be granted by the competent authorities of the Member State where the exporter is established.

An export licence would not normally be required, unless the export concerns the technologies listed in Annex IV and hence controlled also within the EU.

3.4. Security and data protection issues

As consequence of illegal access and data hacking, the final recipient might also be an unauthorized person located either within or beyond the EU borders. Hence, data hacking could involve also unwanted transfer of proliferation sensitive technology.

Even if not in the scope of export controls, the competent authorities should pay due consideration and explore such a likelihood.

Important indicators to take into consideration are the level of security and the assurances provided by the cloud providers.

Cloud providers relying only on EU servers and complying with EU-data protection procedures could be reasonably considered reliable. In any case, the competent national authorities should remain vigilant and may ask from the cloud users to furnish appropriate guarantees. These may include cloud providers' statements ensuring that only authorised persons can access sensitive data, or the non-reliance on third-country servers. Pending the establishment of certifications to prove compliance with the EU legislation in the area of cyber security and data protection, the provision of the contract itself (service level agreement, SLA) could be an alternative option. Common guidelines for EU harmonized approaches to data protection are needed.

3.5. Role of the cloud provider

Cloud providers established in the EU might also have export control liabilities in case they act as exporters and make available the capabilities of controlled software and applications to cloud users outside the EU (see above PaaS, IaaS, SaaS).

The competent authorities shall in all cases examine the lawfulness of cloud providers vis-à-vis both export control and cyber security imperatives when assessing an export application.

3.6. Types of transaction

Verifying where the sensitive information is uploaded and from where it is accessed is of utmost importance in order to answer if an authorisation requirement is applicable.

It is reminded that the focus should not only be on the final recipient, who might be identical with the exporter, but on the potential intermediate recipients of the sensitive information either intended or unintended.

A summary of the scenarios is provided in the table below.

Possibilities		Action
Upload inside the EU	Access only inside the EU	No licence needed unless the transaction concerns the most sensitive technologies mentioned in Annex IV
	Access outside the EU	A licence is required unless an EUGEA ,GEA or NGEA is applicable
Upload outside the EU	Access outside the EU	A licence should be sought in the event of an EU cloud provider making available controlled technology and software to third countries for which no EUGEA or NGEA applies
	Access inside the EU	No licence is required from the EU authorities. EU cyber security or other related regulations may apply.

3.6.1. Upload inside the EU, access inside the EU

More particularly, If both actions the upload and access of controlled data takes place within the EU, no license would be needed. However, if the transfer in question refers to technologies and software listed in Annex IV, a license for intra-EU access shall be required.

3.6.2 Upload inside the EU, access outside the EU

Whenever controlled information originated from the EU is accessed outside the EU's territory a licence obligation is relevant, regardless of the nationality of the person accessing the controlled data. However, the exporter to the "cloud" might also benefit from the EU General Export Authorisations reported in Annex II of the Dual-use regulation, as well as Global Export Authorisations and National General Authorisations, for certain items and destinations specified in the regulation and national law.

3.6.3 Providing EU cloud services outside the EU

This particular situation (see par. 3.5) would see an EU cloud provider acting as exporter by providing "Software as a Service" (SaaS), or when providing a Platform (PaaS) or Infrastructure (IaaS) to a third country national/ company outsources all or a part of its ICT activities. The data stored in the EU cloud

provider's servers could be accessed both from inside or outside the EU. Dealing with such a scenario brings to the forefront the role and responsibilities of cloud providers in the EU, who should act to guarantee data protection and security, being at the same time aware of any export control responsibilities from their part. To that effect, the EU cloud provider should ask for an export control authorisation when providing controlled software/technology to recipients outside the EU, according to the Dual-use regulation requirements.

.