EUROPEAN DATA PROTECTION SUPERVISOR

Guidelines on the use of cloud computing services by the European institutions and bodies

EDPS

16 March 2018

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Purpose and scope

The EU institutions, bodies and agencies ("the EU institutions") have been considering the use of cloud computing services because of advantages such as costs savings and flexibility gains. They are nevertheless faced with the specific risks that the cloud computing paradigm involves and remain fully responsible regarding their data protection obligations. For cloud services, the EU institutions should ensure an equivalent level of protection of personal data as for any other type of IT infrastructure model.

These Guidelines aim at providing **practical advice and instructions** to the EU institutions to comply with Regulation (EC) No. 45/2001. As a legislative process is currently underway to integrate the principles of the General Data Protection Regulation (Regulation (EU) 2016/679, hereafter "GDPR") into the data protection rules for EU institutions, the new concepts are taken into account in these guidelines, referring to the relevant GDPR provisions. After adoption of the new data protection Regulation for EU institutions, an updated version will be published.

The Guidelines provide recommendations and indicate best practices to implement accountability for personal data protection by **helping to assess and manage the risks for data protection, privacy and other fundamental rights of individuals whose personal data are processed by cloud-based services**. They collect and consolidate the advice the European Data Protection Supervisor (EDPS) has been giving the EU institutions in the last years, e.g. regarding the first inter-institutional tenders.

These Guidelines outline the approach that EU institutions should take to adequately protect personal data when assessing the option of using cloud computing services for their IT systems. The specific risks brought about by the cloud computing model, which includes and often magnifies those entailed in service outsourcing, must be identified and managed and relevant safeguards put in place.

The EDPS considers the best practices listed hereafter as **a reference** when assessing compliance with the Regulation. EU institutions may choose alternative, equally effective, measures other than the ones presented in this paper taking into account their specific needs. In this case they will need to demonstrate how these measures lead to an equivalent protection of personal data.

While these Guidelines are aimed at the DPOs, DPCs, IT and IT security staff and other administrative services of EU institutions involved in designing, planning and procuring cloud computing services, other organisation interested in data protection and cloud computing might find them useful, too.

EU institutions should perform an assessment of the data protection impact of the planned cloud services on the data they will process. If the assessment shows that the EU institution can in principle adopt safeguards to mitigate the risk to an acceptable level, then the EU institution should consider the resulting requirements and use them as input for the procurement specifications. In case of a negative outcome of the assessment, the EU institutions should change plans and either consider less risky cloud computing services or overall abandon the cloud option.

The Guidelines focus on:

- the assessment of the appropriateness of the cloud computing option;

- how data protection requirements should be taken into account in the identification and choice of the cloud computing option in the procurement process;

- a baseline of relevant organisational and technical safeguards, with a stress on contractual terms.

The identification and assessment of general cloud specific risks is presented in an annex.

Particular emphasis is given to contracts for the provision of cloud computing services. Guidance is also given on the operation of cloud services and Service Level Agreements, which can also be used to detail the IT security requirements. The contractual agreements should also integrate requirements for service terminations, including safe return of the data or portability to another service provider.

1. Introduction

1 The European Union institutions, bodies and agencies ("the EU institutions") are considering the use of cloud computing services because of advantages such as costs savings in up-front and management resources, and partial or complete outsourcing of software applications, IT[1] infrastructure and data storage. This would allow to reduce or avoid internal IT management tasks and efforts, as well as for new capabilities offered and, under some circumstances, a number of possible advantages such as a higher level of IT security assurance. They are nevertheless faced with the specific risks that the cloud computing paradigm involves and remain fully responsible regarding their data protection obligations.

2 These Guidelines aim at providing practical advice and instruction to the EU institutions to comply with Regulation (EC) No. 45/2001[2] and with its proposed reformed rules ("the proposed Regulation")[3], by helping them assess and manage the risks for data protection, privacy and other fundamental rights of individuals whose personal data are processed by cloud-based services. They collect and consolidate the advice the European Data Protection Supervisor (EDPS) has given the EU institutions in the last years.

3 The principles of the proposed Regulation are planned to be the same as in the new General Data Protection Regulation (Regulation (EU) 2016/679, hereafter "GDPR")[4] applicable in EU and EEA member states. While waiting for the approval of the proposed Regulation, **in these Guidelines we refer to the GDPR provisions when specific Articles are mentioned. We will update the text once the proposed Regulation is adopted and published**.

4 As the independent supervisory authority competent for the processing of personal data by the EU institutions, the EDPS may among other tasks issue guidelines on specific aspects related to the processing of personal data. The present Guidelines are the result of a process where the EU institutions have been consulted and provided their feedback to the EDPS[5].

[1] The term IT refers to information and communication technologies.

[2] Regulation (EC) No. 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.01.2001, p. 1.

[3] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No. 45/2001 and Decision No 1247/2002/EC, COM(2017) 8 final, of 10.1.2017, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0008:FIN.

[4] 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); OJ L 119, 04.05.2016, p.1, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL.

[5] In 2017, the EDPS distributed a draft of these guidelines to the Data Protection Officers, IT managers and IT security officers of the European Institutions, Bodies and Agencies. About 400 comments were received and taken into account for the final version.

5 These Guidelines are targeted at Data Protection Officers ("DPOs") and Data Protection Coordinators ("DPCs") within each EU institution, as well as IT and IT security staff and other administrative services involved in designing, planning and procuring cloud computing services.

6 The purpose of the Guidelines is to make it easier for EU institutions to fulfill their obligations. The latter remain however responsible for compliance with such obligations pursuant to the accountability principle. The measures recommended in these Guidelines allow the EU institutions to start the expected process on accountability and are future oriented since they take into account the expected legislative changes. EU institutions may choose alternative, equally effective, measures other than the ones presented in this paper taking into account their specific needs. In this case they will need to demonstrate how they have planned to obtain equivalent protection via these alternative measures.

2. Scope and structure of the Guidelines

7 This document provides the EU institutions with guidance on how to protect personal data and privacy and comply with the proposed Regulation when planning and using cloud computing services to support their institutional tasks responding to their operational needs as also evidenced by requests for consultations and prior checks handled by the EDPS.

8 This document focuses on the use of cloud computing services provided by commercial entities. As such it also addresses, as a natural consequence, the issues raised by the outsourcing of IT services that process personal data.

9 The Guidelines do address, in particular:

- **Data protection roles and responsibilities** of the EU institutions and of the Cloud Service Provider ("the CSP") and their accountability aspects (section 3).
- Factors to be considered when **assessing** and **selecting** a cloud computing service through public procurement, including the **approach** to be taken and the relevant **safeguards** (sections 4.1 and 4.2).
- Operation of cloud computing services and provisions/safeguards to be ensured for the 'end of contract' (section 4.3).
- Examples of **security controls** mitigating cloud specific risks (section 4.4) and references to some external sources (see Annex 5) for further coverage.

10 The following information is provided in an annex to support the guidance:

- Further legal guidance on specific issues (Annex 2).
- Basic concepts of cloud computing, specific aspects for service model (IaaS/ PaaS/ SaaS) and deployment model (public, private, community or hybrid) cloud environments (Annex 3).
- A description of specific data protection risks introduced or magnified by the use of cloud computing services (Annex 4).
- Reference to other useful documents (opinions, technical standards, best practices etc.) (Annex 5).

11 This document does not consider/focus on:

- Risks for the EU institutions posed by cloud computing which do not relate to compliance with the proposed Regulation, such as any financial risks linked to the procurement of cloud services or those related to classified information.
- IT security risks not specifically raised or magnified by cloud computing services.
- An exhaustive coverage of relevant IT security measures.
- The technical and functional features of the IT infrastructure provided, such as type of servers, software platforms and applications, network devices, etc.
- The basic data protection principles and obligations, unless specifically impacted by the use of cloud computing services. Adequate guidance on them is provided by other existing or planned EDPS deliverables.

3. Approach to the cloud computing option

3.1. Ensuring an equivalent level of protection of personal data as for any other type of computing model

12 The use of cloud computing services can bring benefits, under some circumstances, including increasing the level of protection for the information processed. However, the cloud computing model also entails new risks[6] for personal data, and changes the level of existing ones. Just to mention a few main relevant issues: in the cloud computing paradigm organisations and individuals have in general less control on the way data are processed and exploited; many third parties may contribute to the service offer thus producing uncertainty as to who is accountable for what; the use of the public internet adds an element of risk and the dynamic interplay of many data centres gives less assurance on the physical location of the data.

13 The essential underpinning principle in these Guidelines is that cloud computing should not lower the level of protection of personal data as compared to data processing via any other type of IT infrastructure model[7].

For example, the processing of personal data via a cloud service should not trigger data retention periods different than those set out for 'non-cloud' processing by the relevant EDPS thematic guidelines[8].

14 As a result, **specific safeguards[9] are needed to cope with the new risk landscape** so that the level of protection can be equivalent. If adequate safeguards are not available, the institutions should change plans and consider less risky cloud computing services or overall abandon the cloud option.

[6] Please refer to Annex 4 where data protection related high level risks that the use of cloud computing services entails are identified.

[7] "Sopot Memorandum", adopted in April 2012 by the Berlin International Working Group on Data Protection in Telecommunications (IWGDPT), available at:

https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=3065.

See European Parliament Resolution of 10 December 2013 on cloud computing, Recommendation, "63. As a general rule, **the level of data protection in a cloud computing environment must not be inferior to that required in any other data-processing context**". In the same line, European Parliament Resolution of 12 March 2014: "Whereas the level of data protection in a cloud computing environment must not be inferior to that required in any other data-processing context; whereas Union data protection law, since it is technologically neutral, already applies fully to cloud computing services operating in the EU.".

[8] For instance, the EDPS guidelines concerning the processing of personal data in the area of leave and flexitime, available on the EDPS website, at:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/12-12-20_Guidelines_Leave_Flexitime_EN.pdf; data retention periods are specified at pages 9-11.

[9] The terms "safeguard", more used in the data protection domain, and "control", more used in the IT security domain, both refer to measures used to treat risks.

15 Policy advice previously given by the EDPS and the Article 29 Working Party (WP29)[10] can be useful to analyse the challenges of cloud computing and plan for the appropriate safeguards.

3.2. Governance and responsibility: keeping control on the data processing in the cloud context

16 Even if the EU institution is the **controller** and the CSP is usually only **the processor**[11]**,** respective **roles and responsibilities** of all parties must be clearly defined. For many cloud computing services on the market the role of the service provider is not always clear. Sometimes CSPs keep a level of control over the processing that exceeds the role of the processor by carrying out operations on personal data that have not been requested by the customer or not leaving the customer enough choice on the processing means or procedures. EU institutions must avoid that by negotiating adequate contracts and safeguards or choosing another CSP.

17 The EU institution, due to the legal obligations to which it is subject[12], must **retain control** (determining the **purposes** and the **means**) over the processing of personal data performed via the cloud service. Specific provisions must be inserted in the contractual legal framework between the EU institution and the CSP ("the Contract") to that aim.

18 In a nutshell, to **keep controllership** in order to ensure full compliance with the proposed Regulation[13] and be accountable, the EU institution shall:

- **Select a CSP providing sufficient guarantees** in respect of the technical and non-technical measures it is capable to implement to assist the EU institution in complying and ensure the data protection rights of the individuals whose data are processed.

[10] On the challenges that cloud computing poses for data protection, see the Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at:

https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf.

and the Opinion of the Article 29 Working Party 05/2012 on Cloud Computing, available at:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

[11] As defined under Article 2 of the Regulation (EC) No. 45/2001 and under Article 4 (no. 8) of the GDPR.

[12] For instance, according to Article 14 of the Regulation (EC) No. 45/2001, the data subject has the right to obtain *from the controller* [which is defined under Article 2, letter (d) of the Regulation as "the Community institution or body, the Directorate-general, Unit or any other organizational entity"] the rectification of inaccurate or incomplete data.

See also, under Article 23.2, letter (b) of the Regulation, the specification that "the processor shall act only on instructions from the controller".

Under the GDPR, Article 16, also states that: "The data subject shall have the right to obtain *from the controller* without undue delay the rectification of inaccurate personal data concerning him or her." Similarly to Regulation (EC) No. 45/2001, the GDPR, under Article 28(3), lays down "the processor processes the personal data only on documented instructions from the controller".

[13] We recall that specific provisions of the GDPR on processing of personal data on behalf of EU institutions and bodies (under Article 28) apply to this case.

- **Enter into a legally binding contract**[14] **("the Contract") between the CSP and the EU institution** and laying down, among other terms and conditions that the 'cloud-customer' (the EU institution) shall be **the sole controller** and the processor shall not process data except on the basis of instructions of the controller.
- When the Contract is operational, actively **ensure and monitor the implementation** of the required safeguards and other contractual provisions.

19 We recall that, as a **processor**, the CSP is legally subject to and accountable for **specific obligations** (Articles 28, 29 and 30 of the GDPR[15]).

20 The CSP **shall assist** the EU institution in ensuring compliance with its data protection obligations, in particular regarding the latter's prompt response to requests for access, blocking, rectification and deletion from the data subjects exercising their **data protection rights**[16]. It must be specified in the Contract either that the controller shall have direct control to perform processing operations that are necessary to implement data subjects' rights or that the CSP shall react without delay to any instructions from the EU institution to implement a request from a data subject (to access, to rectify, to block, to erase personal data). In any case, it must be clearly stated that the final reply to the data subject shall be given by the EU institution or under its instructions.

3.3. Planning for procurement of cloud computing services

21 With the above considerations in mind, and considering the legal nature, institutional tasks and responsibilities (the exercise of a public function, triggering special precautions) of the EU institutions[17], the latter should go through the following process while planning for cloud computing services:

[14] With this term "Contract" we refer to **both** the contract *and* the "Service Level Agreement" (SLA), as well as all annexes, which form together the contractual framework stipulated by the EU institution with the CSP.

What the CSP needs to do to support the controller in performing its tasks is defined in written contracts. These contracts are usually structured in such a way that the operational terms of the service rendered by the CSP are defined and agreed upon in a contractual section or different document, still an extension of the contract, called Service Level Agreement (SLA). Even if we assume a differentiation of the two documents in these Guidelines following a typical approach, the EU institutions are free to structure the contract as they prefer.

[15] Please refer to Articles 28-30 of the GDPR

[16] As set out under Articles 12-23 of the GDPR.

[17] EU institutions and bodies are a special kind of public administration, that is of supranational level, whose data protection legal framework is represented by the Regulation (EC) No. 45/2001 and, in the next future, by the proposed Regulation. In legal terms, it is important to note that the aforementioned data protection law is applied **in conjunction with** other pieces of legislation governing the activities of EU institutions and bodies, such as the **Protocol on the privileges and immunities of the European Union.**

Protocol (No 36) on the Privileges and Immunities of the European Communities (1965), Official Journal No C 321 E, 29/12/2006 p. 0318 - 0324, available at:

http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012E/PRO/07&from=EN.

The Protocol on Privileges and Immunities is referred to also under **Regulations establishing EU Agencies**, for example, Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), lays down: "Article 67 - Privileges and immunities: The Protocol (No 7) on the privileges and immunities of the European Union annexed to the Treaty on European Union and to the TFEU shall apply to the Authority and its staff.".

- Get **expert advice** and seek and adopt relevant **best practices**. Liaise with the other EU institutions, for example to get expertise on relevant former procurement experiences.

- **Train** decision makers, business owners, contract managers and IT staff on the data protection risks stemming from the use of cloud computing services, and request contractors to be trained.

- Perform an **assessment of data protection risks** to verify whether it is possible to procure cloud services to support the data processing operations under the envisaged scope of application and select a suitable CSP that can offer an adequate level of protection of personal data with a view to reduce the impact on the fundamental rights and freedoms of individuals and compliance with the proposed Regulation.

  The level of formalism and insight of the assessment may vary depending on factors detailed in Section 4.1.

22 We recommend that the EU institutions start developing expertise and gaining experience on processing personal data via cloud services with operations implying **lower data protection risks**[18], if possible, and only consider more sensitive operations once it is reassured about its capability to exercise effective control over those services.

23 In case the planned cloud option is feasible (on the basis of the assessment), the EU institution shall, in particular:

- Identify necessary roles, allocate relevant tasks and resources and set up internal policies, processes and procedures to manage the prospective cloud services.
- Ensure that contracts and Service Level Agreements (“SLAs”) with the CSP contain all needed safeguards, including, in particular:
  - The clear indication that the CSP shall process personal data entrusted by the EU institution **solely on documented instructions of the EU institution**.
  - Ensuring that persons authorised to process the personal data have committed themselves to **confidentiality** or are under an appropriate statutory obligation of confidentiality.
  - The clear indication and definition of the **responsibilities and liabilities** of the different parties (including sub-processors, if any).
  - The clear definition and indication in particular of how the CSP shall support the EU institution in effectively fulfilling its obligations as controller towards the data subjects and the EDPS.
  - Provisions granting the EU institution the faculty to perform **audits** of the CSP on its own or via an external (third party) auditor mandated by the EU institution.
  - The clear indication of the **location** of the CSP and any other processors engaged by the CSP (sub-processors), if any, and of their data processing operations including backups.

[18] Excluding, in principle, the special categories of personal data under Article 9 of the GDPR.

  - The clear indication that the processor will not engage **another processor** without the prior written authorization of the EU institution. This authorization can be a specific one (for a specific sub-processor) or a general one. In case of general authorization, the CSP will inform the controller of any addition or replacement of sub-processors, and the EU institution will be entitled to object to the changes.
  - **No disclosure** to EU member states or non-EU country law enforcement authorities ("LEAs") of personal data entrusted to the CSP (as well to the sub-processors, if any) by the EU institution, *unless this is expressly authorized by EU law*. As an EU body, the EU institution is subject to the **Privileges and Immunities of the European Communities**[19], particularly as regards the inviolability of archives (including the physical location of services) and information security.
  - Data portability/ recovery/ disposal procedures.
  - **Deletion or return**, at the choice of the EU institution, of all the personal data entrusted by the latter to the CSP after the end of the provision of services.
  - Clear indication of the **IT security measures** to be provided by the CSP and by any sub-processors.
- Manage the contract, its execution and termination, and keep control of the operations performed by the CSP on the personal data 'entrusted' by the EU institution to the latter.

24 The outcome of the assessment of data protection risks could also show that the planned cloud service poses **data protection risks that cannot be sufficiently managed in a way to appropriately reduce their impact.** As a result the EU institution should **consider procuring other cloud service(s) involving risks that can be properly managed** or even **'giving up' the overall 'cloud option'**.

25 The overall recommended **process** for the procurement of cloud computing service is described in more detail in chapter 4.

[19] See footnote 17.

4. How to assess the cloud computing option, procure and operate cloud services

4.1. Assessing the data protection appropriateness of a cloud service

26 Procurement of cloud computing services to process personal data can be somehow different depending on whether the EU institution:

- (Scenario I) wishes to procure cloud services to support ***specific* processes** (e.g. to manage the organisation of meetings of groups of experts), or
- (Scenario II) the portfolio of prospective processes to be supported is relatively wide and **a range of services** and deployment models is needed.

The two scenarios, while sharing many common features, are described separately.

Assessment of data protection risks of the cloud service option

27 The EU institution must assess whether **requirements for compliance** with the proposed Regulation can be met.

28 The EU institution shall also perform an assessment of the data protection risks for the individuals' fundamental rights and freedoms taking into account the information at their disposal at this stage:

- The **nature of the personal data** to be processed.

  Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms[20] merit specific protection.

- The **type of operations** to be performed.

  For example "profiling" is a type of operation entailing possible high risks for individuals[21].

- The **scope** of the processing operations and their **context.**

  Performing operations on data referring to a large number of individuals is a factor that can increase the risk.

  The context of processing operations, such as: category of data subjects (e.g. whether EU staff or not; individuals' working place, role and tasks; involvement of children); the possible impact of the environment (e.g. possible prejudice to individuals due to their specific culture), etc.

[20] These are in particular data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation or data relating to criminal convictions and offences. Nevertheless, this is not the only factor determining the level of risk. Personal data that do not fall under the mentioned categories might lead to high levels of risk for the rights and freedoms of natural persons under certain circumstances, in particular when the processing operation includes the scoring or evaluation of individuals with an impact on their life such as in a work or financial context, automated decision making with legal effect, or systematic monitoring, e.g. through CCTV. (See also Working Party 29 "*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679"*, WP 248 rev.01, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236*)*.

[21] See also Working Party 29 "*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)*": http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

- The **purpose** of the operations.

  Examples are: managing e-mail communications, assessing staff performance, storing and processing pictures and videos of CCTV footage etc.

29 In performing the assessment they shall take into account:

- The **generic cloud computing related risks** (as described in Annex 4) and **risks linked to the specific cloud service option** and the specific personal data and to the processing operations falling under the scope of the procurement.
- The **current market reality** and **the maturity of the prospective CSPs** with respect to their capability of fulfilling the requirements for compliance with the proposed Regulation and of reducing the risks to an acceptable magnitude. This can be done by obtaining some preliminary information (publicly available or on request), including on possible assurance means such as those listed in section 4.2.1.

30 The GDPR identifies conditions under which the assessment of the risks for individuals is mandatory and the minimum content of such assessment, which is called **Data Protection Impact Assessment (DPIA)**[22]. The Article 29 Working Party has provided guidance on the conditions, modalities and content of the DPIA[23].

31 The present Guidelines do not provide further advice on how to perform a DPIA. The EDPS is currently drafting relevant guidance for the EU institutions to which reference can be made in this regard. The DPO of the EU institution will play a key role advising the latter on whether a DPIA is mandatory or not and on how to perform it.

32 If a DPIA is required, as specified by the forthcoming EDPS guidance, then its results shall be considered also having regard to the possible use of the cloud computing service by the EU institution. If a DPIA is **not** required, the EU institution might find useful to nonetheless use the relevant DPIA methodology to perform the assessment of the data protection risks.

33 Possible measures to comply with the proposed Regulation and mitigate these risks are part of these Guidelines and are described in sections 4.2, 4.3 and 4.4. These obligations and recommendations can be considered as a **baseline of safeguards to be implemented for all cloud computing services.**

34 The existence of a baseline does not exclude the obligation:

- to assess the residual risks and the risks linked to the specific context and operations the cloud service is planned to support (see also Annex 4);
- and to eventually identify possible necessary measures to treat those risks.

Therefore, a **documented risk management** by the EU institution remains in all cases mandatory[24]**.**

[22] See Article 35 of the GDPR.

[23] Available at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[24] See Article 24(1) of the GDPR: “Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary”.

35 Should the EU institution, based on its risk assessment, decide not to implement some of the measures proposed in this document as a baseline, it shall do it in an accountable way and thus document the rationale behind its choice.

36 The EU institution shall in any case implement measures necessary to comply with the obligations provided for in the proposed Regulation.

The EU institution shall eventually assess whether the identified risks can be managed as to appropriately reduce their impact and comply with the Regulation, and decide **whether a cloud service is a suitable option or not**.

Scenario I: Public procurement of cloud computing services for specific operations processing personal data

37 If the conclusion of the assessment implies that the EU institution is in principle able to adopt safeguards to mitigate the cloud computing risks for the specific processing operation or anyhow appropriately manage the risks, and thus a positive decision is taken, the data protection requirements (which include the security ones) identified during the risk assessment need to be translated into criteria in the procurement specifications.

38 If the requirements **cannot** be met by available cloud services, the processing must **not** be operated in the targeted cloud service environment (**negative decision**).

39 In this case, the requirements may be changed by limiting the processing operations to be supported by cloud services to those that are less risky or, if applicable and still useful, by limiting data processed to less sensitive categories or to non-personal data. Alternatively, another deployment/service model bearing lower risks could be assessed. In case the EU institution still plans to process personal data, it will perform a new assessment of requirements and risks.

Scenario II Public procurement of framework contracts for cloud computing services planned to process personal data in a large portfolio of use cases

40 A process for public procurement of framework contracts for cloud services planned to process personal data in a large portfolio of use cases (e.g. complete EU institutions IT infrastructure, IT resources to develop and operate institutional websites, IT environments for developers, etc.), often targeting IaaS and PaaS services, could take into account the data protection requirements along the following three main phases.

Phase 1: service groups for a framework contract

41 The assessment described above has to be performed on **a group of candidate processing operations/applications** for which the cloud services procured under a framework contract may be used.

42 The data protection compliance requirements and the safeguards identified during the risk assessment need to be **translated into criteria** in the procurement specifications.

43 The EU institutions will evaluate which cloud service offerings are adequate and select only service providers that are able to satisfy these requirements. If no suitable offer exist, no contract may be awarded.

Phase 2: suitability of a specific processing operation for cloud services

44 Once a framework contract exists, the EU institution might want to consider whether a specific operation/application can be supported by one of the cloud services offered by the awarded contractor(s).

45 For a specific application that is planned to be used as a cloud service:

The EU institution should **assess whether any of the cloud services available under a framework contract** are **compatible** with the data protection requirements of the specific processing operation it is meant to support.

46 If the requirements **cannot** be met by available cloud services, the processing must **not** be operated in the targeted cloud service environment (**negative decision**).

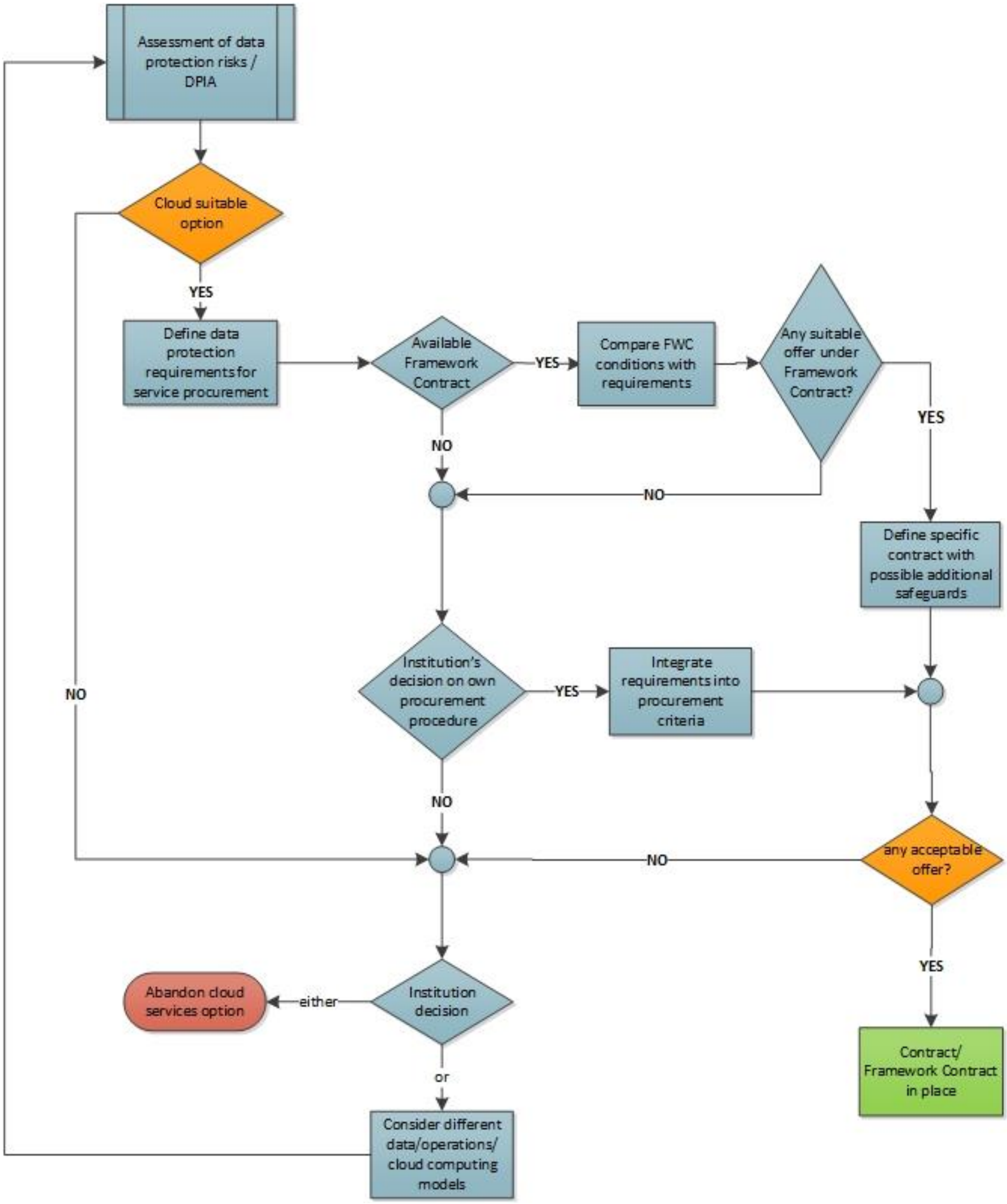
47 In this case, the requirements may be changed by limiting the processing operations to be supported by cloud services to those that are less risky or, if applicable and still useful, by limiting data processed to less sensitive categories or to non-personal data. Alternatively, another deployment/service model bearing lower risks could be assessed. In case the EU institution still plans to process personal data, it will perform a new assessment of requirements and risks.

Phase 3: contracting for specific processing operations

48 In case the outcome of phase 2 indicates that one or more processing operations are in principle suitable for the available cloud services, the EU institution may be required to negotiate, as far as legally allowed, possible new requirements in the specific contract to be signed to ensure that all necessary safeguards and measures are in place.

49 In any case, since further integration may not be possible due to public procurement constraints, it is of the utmost importance that the EU institution considers and defines as precisely as possible all envisaged uses of the planned services since the initial assessment in phase 1.

The overall process can be summarised by the following flowchart:



Assessment of data protection risks / DPIA
Cloud suitable option
YES
NO
Define data protection requirements for service procurement
Available Framework Contract
YES
NO
Compare FWC conditions with requirements
Any suitable offer under Framework Contract?
YES
NO
Define specific contract with possible additional safeguards
Institution's decision on own procurement procedure
YES
NO
Integrate requirements into procurement criteria
any acceptable offer?
NO
YES
Contract/ Framework Contract in place
Institution decision
either
or
Abandon cloud services option
Consider different data/operations/ cloud computing models

4.2. Criteria and requirements for cloud service procurement

50 Once the option for cloud based services is chosen, **criteria and requirements** need to be set for public procurement and consequent service management (operation, maintenance, termination).

51 As for **the tendering procedure in general**, we strongly suggest that the EU institutions take measures to establish a **common strategy**[25] regarding cloud computing. This should include **the planning** of the procurement of cloud services, also in order to increase their bargaining powers towards CSPs, and other common elements such as e.g. a framework for SLAs that include the data protection requirements, including notably contract management and brokerage[26].

52 This could partly overcome the potential difficulties of small EU institutions having their own tendering procedure when it comes to the definition of the contractual requirements and the integration of specific safeguards in the Framework contract/tendering contract.

4.2.1. Due diligence on choosing a prospective CSP

53 The EU institution must choose a CSP **providing sufficient assurance to act on behalf of the EU institution and to implement the necessary technical and organisational data protection measures**, and must verify the effectiveness of those measures.

54 The evidence an EU institution can use to contribute to such assurance include:

- Data protection and IT security **certifications by accredited third parties** in the context of relevant certification schemes[27]. These should include cloud-related data protection and IT security certifications schemes tackling the risks identified[28]. In general, self-assessments are not to be considered as providing sufficient assurance.
- Adherence to **cloud-specific codes of conduct** that provide added value in terms of measures to protect personal data and contribute to demonstrating compliance with the Regulation in a cloud-specific environment[29].

[25] See Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", at page 27: "118. (...) in the context of the European Cloud Partnership, the Commission will work on developing specific procurement terms for the public sector by defining **common procurement requirements for their use of cloud computing services**. The EDPS underlines that these common procurement requirements **should include** data protection requirements, including appropriate security measures, which should be defined in a manner appropriate to the specific risks of processing public sector data in a cloud computing environment. This should be done on the basis of a careful **data protection impact assessment** according to the type and sensitivity of the processing carried out (e.g. differentiate between public sector processing of health data, criminal offences, confidential data, etc.). As a result, the requirements contained in procurement terms will need to be differentiated according to the sensitivity of the data processed, which should lead to defining several sets of common requirements." In this regard, see also, European Parliament, Resolution of 12 March 2014.

[26] Carried out by the European Commission on behalf of other EU institutions in the context of the inter-institutional framework contract Cloud I. A similar approach is used by EU Agencies in the context of a framework contract managed by the European Food Safety Authority (EFSA).

[27] The Article 29 Working Party provides guidance on establishing **certification schemes** that can contribute to demonstrating compliance according to the terms of the GDPR. A list of those schemes will be available by the national data protection authorities or by the future European Data Protection Board.

[28] The GDPR, under Article 28(5) lays down that processors (in this case, CSPs) may rely on the **certification schemes** (referred to in Article 42 of the GDPR) as element which can guarantee the implementation of appropriate technical and organizational measures.

[29] The Article 29 Working Party will provide guidance on **codes of conduct** that can contribute to demonstrating compliance according to the terms of the GDPR. A list of those codes of conduct will be made available by the national data protection authorities or by the future European Data Protection Board.

- **Previous experience on projects** sharing similar (or higher) risks for analogue categories of personal data. Further reassurance can be demonstrated by proven experience with EU and national public administrations.
- **Accountability practices already in place** such as: a Data Protection Officer within the company; privacy policies and procedures in place; having contributed to perform DPIAs or anyhow having a methodology to assess data protection risks; use of standard contractual clauses[30] (if applicable); use of Binding Corporate Rules (if applicable); an established IT risk management framework; IT security policies, procedures and safeguards already in place.

4.2.2. Contracting: getting the right terms and conditions for the prospective CSP[31]

(i) Introduction and general remarks

55 In order to ensure that the EU institution keeps control on how the CSP delivers the requested services it is essential to **negotiate and obtain appropriate terms and conditions in the Contract with the CSP**. Some of these terms and conditions are specified below (as ‘model clauses’).

56 It is important to stress that such terms and conditions should be **adapted** taking account of the legal constraints applicable to EU institutions (in particular, of the applicability of the Protocol on Privileges and Immunities of the European Communities[32]) and **customised** according to the need to address the risks posed by the data processing (according to a ‘risk-based’ approach).

(ii) Overall assessment of the contractual arrangement

57 Controllers should be aware of the importance of **the overall assessment of the contractual framework** applicable to the provision of the cloud service[33].

[30] Reference to standard contractual clauses is made in particular under Article 29(6-8) of the GDPR.

[31] As reference to this issue in general, see the Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", at pages 26-27, paragraph 117.

[32] See footnote 17.

[33] For a **quick check list**, see Opinion 5/2012 on Cloud Computing, section 3.4.2 **Contractual safeguards of the “controller”-“processor” relationship(s)**, pages 12-14, laying down 14 points, among which we draw attention on:

Point 5 – “Inclusion of a **confidentiality clause**, binding both upon the cloud provider and any of its employees who may be able to access the data. Only authorized persons can have access to data;”.

Point 7 – “The contract should expressly establish that **the cloud provider may not communicate the data to third parties**, even for preservation purposes unless it is provided for in the contract that there will be subcontractors. The contract should specify that sub-processors may only be commissioned on the basis of a consent that can be generally given by the controller in line with a clear duty for the processor to inform the controller of any intended changes in this regard with the controller retaining at all times the possibility to object to such changes or to terminate the contract. There should be a clear obligation of the cloud provider to **name all the subcontractors commissioned** (e.g., in a public digital register). It must be ensured that contracts between cloud provider and subcontractor reflect the stipulations of the contract between cloud client and cloud provider (i.e. that sub-processors are subject to the same contractual duties than the cloud provider). In particular, it must be guaranteed that both cloud provider and all subcontractors shall act only on instructions from the cloud client. (…) the **chain of liability** should be clearly set in the contract. It should set out the obligation on the part of the

(*continued on next page*)

- This means that the EU institution should assess **all components** (including e.g. annexes) to the CSP's contractual documents that specifically describe the processing operation covered by the agreement (e.g. categories of data processed, security and confidentiality measures implemented by the CSP, etc.). The EU institution needs to assess on a **case-by-case basis** how the Contract, the SLA and their annexes (that is, the overall contractual framework) meet its specific data protection needs and legal requirements.
- In particular, it is essential to check the so-called "**other** contractual clauses" (meaning clauses **not directly-related to data protection, but still important to ensure accountability**), including clauses on the **law applicable to the contract itself** ("governing law") and on the **applicable jurisdiction**; on **the right of the parties to introduce variations of the Contract**; on CSP's **obligations after the termination of the data processing service 'outsourced' by the EU institution**.

58 Other clauses to be established in the cloud services Contract are the ones related to the **availability and quality of the service** (establishing the timeframe in which the service is available as well as technical characteristics, effectiveness and efficiency, and defining relevant metrics). Very often such provisions are grouped within a SLA.

59 As a general rule, we would recall that all CSPs offering services to clients subject to EU laws have a duty to assess the compliance of their contractual arrangements with EU data protection requirements based on the proposed Regulation, taking into consideration the challenges that cloud computing poses for data protection as described in WP29 Opinion 05/2012 on cloud computing as well as in the EDPS relevant Opinion[34].

(iii) On certain 'core' data protection issues to be addressed under the contractual terms and conditions

60 It is of the utmost importance to add to the terms of the Contract that cloud service providers are **prohibited from disclosing** to an EU Member State or Third Country **law enforcement authorities ("LEAs")** personal data entrusted to the CSP by the EU institution, *unless this is expressly authorized by EU law, or by Member State law to the extent that the conditions laid down in EU law for such disclosure are fulfilled*[35].

processor to frame international transfers, for instance by signing contracts with sub-processors, based on the 2010/87/EU standard contractual clauses;".

Point 11 – "It should be contractually fixed that the cloud provider must **inform the client** about relevant changes concerning the respective cloud service such as the implementation of additional functions.".

Point 12 – "The contract should provide for **logging and auditing** of relevant processing operations on personal data that are performed by the cloud provider or the subcontractors.".

[34] See footnote 10.

[35] This prohibition stems - as a mandatory legal obligation - from the **Protocol on the Privileges and Immunities of the European Communities**. Nonetheless recalling it under the terms and conditions of the cloud contract would represent a useful reminder for the cloud provider. Pursuant to Article 1 of aforesaid Protocol: (...) "*The property and assets of the Communities shall not be the subject of any administrative or legal measure of constraint without the authorization of the Court of Justice*". Regarding this provision, we observe that it could also cover the cloud computing services for which a licence of use has been granted to EU institutions and bodies; Article 2 lays down: "*The archives of the Communities shall be inviolable*". Article 6 states that: "*For their official communications and the transmission of all their documents, the institutions of the Communities shall enjoy in the territory of each Member State the treatment accorded by that State to diplomatic missions.*

61 **Transparency** is important in the relationship between the EU institution and the CSP, because **it has direct impact on compliance with the obligations of the EU institution under the proposed Regulation**. Therefore, relevant changes in the underlying infrastructure, procedures, and results of relevant security audits should be **communicated** by the CSP to the EU institution without delay, under guarantee of confidentiality. This could also include information regarding activation of business continuity measures, tests or any operation with potential impact on customer service.

62 Since the EU institution is responsible for the lawfulness of the data processing, it has the right to require the CSP to **immediately inform** it if the CSP cannot ensure compliance with any obligations under the Contract. For transparency, it is important to mention - in the SLA or the contract - **all sub-processors** contributing to the provision of the cloud service, as well as of **the locations where** personal data may be processed.

63 The **location** of the company providing the cloud service, of its data centres holding the servers and other equipment in which data are stored or operated upon (including for backup, business continuity purposes and transit, as well as locations from where remote operations are performed) is also a key factor to be considered.

- In **this regard, the EDPS recommends that the processing of personal data entrusted by EU institutions to CSPs, and any sub-processing, *as a rule*, take place within the EU[36]**.

  The reason for this recommendation is to ensure the applicability – also in the 'cloud environment' – of the privileges and immunities enjoyed by the EU institutions in the territory of its Member States pursuant to the **Protocol on the Privileges and Immunities of the European Communities**[37]**.**

  According to Article 1 of the Protocol "The premises and buildings of the Union shall be inviolable. They shall be exempt from search, requisition, confiscation or expropriation. The property and assets of the Union shall not be the subject of any administrative or legal measure of constraint without the authorisation of the Court of Justice." Article 2 lays down that "The archives of the Union shall be inviolable." Finally, according to Article 5, "For their official communications and the transmission of all their documents, the institutions of the Union shall enjoy in the territory of each Member State the treatment accorded by that State to diplomatic missions."

  In addition to the above, we take into consideration that when data is stored in the territory of a non-EU country, a law enforcement body competent in that territory may request access to that data in the context of an enforcement action **applying its public law** (e.g. criminal law, procedural law, data retention legislation, *etc.*). This risk must be carefully assessed by the EU institution.

[36] For instance, EFSA has ensured that the following clause is inserted in the cloud computing service contract to be entered into by the EU Agency : « *the cloud computing services shall be hosted solely in the territory of the European Economic Area. The cloud service provider, its affiliates and any sub-processor will host the (EU Agency's) data, including back up data, on storage media and datacentres located in the following **EU Member State*** ».

[37] On the protections recognised by EU Member States to EU institutions according to the Protocol, see, in particular, Articles 1, 2, and 5 of the Protocol, available, in its consolidated version, at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012E/PRO/07&from=EN.

It also has to be noted that in case of hosting location of the cloud infrastructure in **non-EU** Member States, it will be **more problematic for the EDPS to cooperate and coordinate inspections** with competent supervisory authorities and thus ensure the overall enforcement of the rules of the Regulation[38].

(iv) Model- clauses (what to check for, what shall be defined/included in the Contract)

64 Some content of this section could also be found in the form of an SLA (see section 4.3.2), such as the security provisions. The SLA should be part of the binding contractual agreement (it is nonetheless up to the EU institution how to organise the contractual provisions, allocating terms and conditions in the Contract and/or in the SLA).

65 As based on the most relevant and frequently used contractual clauses[39], we are providing some model clauses to be included in the Contract. Such **model clauses** are laid down **to facilitate a quick control by the EU institution of whether the contract for the provision of cloud services offers adequate data protection safeguards**. Such clauses should be **adapted** to the specific cloud service offered (for example, taking into account whether the CSP uses sub-processors or not).

66 The model clauses are as follows:

[38] We remark that the GDPR provides for an obligation of **cooperation between national supervisory authorities** under Chapter VII.

It is also noteworthy referring to Article 58.1(f) of the GDPR, according to which the supervisory authority shall have the investigative power “to obtain access to any premises of the controller **and the processor**, including to any processing equipment and means, **in accordance with Union or Member States procedural law**” (*emphasis added).*

We point out that, *if* personal data are processed **outside the EU**, the relevant provisions of the GDPR are applicable (namely Chapter V, articles 44-50).

For EDPS guidance, based on the provisions of the current Regulation (EC) No. 45/2001, see the EDPS position paper "Guidance on International Transfers: Article 9", available at:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf. This paper will be updated in the light of the provisions of the proposed Regulation.

[39] Notably, the clauses contained in Commission Decision C(2010)593, available at:

http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

It has to be noted that the possibility for the controller to use standard data protection clauses should neither prevent the possibility for the CSP to include the standard data protection clauses in a wider contract nor to add other clauses as long as they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects.

Account shall also be taken of the recent update (29 November 2017) to the "Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules", WP 256, (http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109) and to the "Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules", WP 257, (http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110). These documents set up a table with the elements and principles to be found in Binding Corporate Rules (BCR) in order to reflect the requirements referring to BCRs now expressly set out in the GDPR (Article 47). A provision similar to Article 47(2) GDPR, describing the content of standard contractual clauses, is not laid down under the GDPR. Nonetheless, it could be argued that some of the safeguards under Article 47(2) may also apply to the standard data protection clauses mentioned under Article 46 GDPR.

A - Description of the processing supported

The description of the processing and, in particular, of the categories of personal data which are the object of processing by the CSP are specified, as applicable, in this Contract and in the SLA and its annexes, which forms an integral part of the Contract[40].

B - Applicable data protection law

67 The processing of the personal data shall be carried out in accordance with the relevant provisions of [the proposed Regulation], providing, among others, data subjects with specific rights (under Chapter III, Articles 14-25) and as determined in the Contract, the SLA and its annexes.

68 Any change in legislation applicable to the CSP preventing it from fulfilling the instructions received from the EU institution and the obligations provided under the Contract which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, shall promptly be notified by the CSP to the EU institution as soon as the CSP is aware of the legislative change, even before its entry into force. In this case the EU institution is entitled to suspend and/or terminate the Contract..

69 The CSP shall provide the EU institution with **comprehensive information on the physical location** of the servers used by the CSP and its sub-processors for the provided cloud services (including for backup, business continuity purposes and transit) as well as locations from where remote operations are performed. Any plans for change of location shall be provided by the CSP to the EU institution before data are processed in the new location with a pre-notice necessary for the EU institution to check in particular if this change complies with the Contract and the applicable law[41]. The EU institution shall have the right to object to the change.

C - Applicable contract law

70 The Clauses/Contract shall be governed by EU law and, where applicable in accordance with EU law, by the law of the EU Country where the EU institution is established or any other applicable law of an EU Country.

D - Variation of the Contract

71 The CSP and the EU institution undertake not to vary or modify the Clauses. This does not preclude the CSP and the EU institution from adding other contractual provisions on business related issues where agreed and insofar as they do not deviate from the applicable data protection law.

E - Obligation after the termination of personal data processing services

[40] Pursuant to Article 28(3) and Article 28(9) of the GDPR, the following elements describing the processing shall in any case be set out in the contract, which shall be in writing, including in electronic form: the subject matter and the duration of the processing; the nature and purpose of the processing; the type of personal data and categories of data subjects; the obligations and rights of the controller.

[41] This could also be more precisely defined according to the EU institution's needs.

72 On the termination of the provision of data **processing services**, the CSP and the sub-processors shall, at the choice of the EU institution:

- without any delay, in a commonly agreed format, either **return all the personal data and the copies thereof to the EU institution** or **transfer them to a destination designated** by the EU institution itself, or
- **effectively delete all the personal data and certify to the EU institution that it has done so,** once it has been verified and confirmed that the data have been successfully and completely transnferred to the new processor or the EU institution.

F – 'Portability' of the data transferred to the CSP (as a right for the EU institution to receive and trasmit these data to another CSP)

73 The CSP shall ensure and be able to demonstrate the '**portability' of the EU institution data from its systems, and any sub-processor system, to other providers** of the EU institution's choice, within *[..]* hours in the format specified *[in the SLA, and/or..]* after having been notified in writing by the EU institution. The CSP must ensure that the EU institution is provided fully with the service and access to the data during this period.

74 The CSP and any sub-processor shall keep the EU institution's data safe and secure until transferred to another site under the control of the EU institution.

G - Sole controllership

75 The CSP shall process the personal data **only on behalf of the EU institution** and **in compliance with its documented instructions and the Clauses**. If it cannot provide such compliance, it shall promptly inform the EU institution of its inability to comply. In this case the EU institution is entitled to suspend or terminate the Contract.

H - Sub-processing

76 The CSP shall ensure, monitor and control that in the event of sub-processing, the activity is carried out by a sub-processor providing at least the same level of protection for the personal data and the fundamental rights and freedoms of data subject as the CSP under the Clauses.

77 The CSP shall ensure that, in the event of sub-processing, it has **previously informed the EU institution** of its plans; given **comprehensive information** on the prospective sub-processors (as to their capacity of providing sufficient assurance - as described in section 4.2.1) and their future role in the cloud service; and it has obtained the EU institution's **prior written consent (specific or general written authorization)**. The CSP shall promtly **send a copy of any sub-processor agreement** it concludes to the EU institution.

78 Where the CSP subcontracts its obligations under the Clauses, with the prior approval of the EU institution **(specific or general written authorization)**, it shall do so only by way of a **written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the CSP under the Clauses**.

[This requirement may be satisfied by **the sub-processor annexing** the relevant parts of the framework contract between the EU institution and the CSP to the Contract between CSP and sub-processor.]

When the sub-processor fails to fulfil its data protection obligations under such written agreement, the CSP shall remain fully liable to the EU institution for the performance of the sub-processor's obligations.

The data protection aspects of the sub-processing shall be governed by [the proposed Regulation].

I - Obligation of the CSP to cooperate with and inform the EU institution

79 The CSP shall deal promptly and properly with all inquiries from the EU institution relating to the processing of the personal data by the CSP.

80 The CSP shall promptly inform the EU institution about the existence of legislation applicable to it or any sub-processor preventing it from processing personal data only on instructions from the EU institution or preventing the conduct of an audit of the CSP or of any sub-processor.

81 In such case, the EU institution shall be entitled to ask for the suspension of the processing of data by the CSP and/or the termination of the Contract.

82 The CSP shall inform the EU institution about:

(i) Future changes concerning the cloud service such as the implementation of additional functions, in due time.

(ii) Future changes in the infrastructure and procedures with a potential impact on the service, and, in due time, about the results of relevant security audits, under guarantee of confidentiality.

(iii) Legally binding requests for disclosure of the personal data by a law enforcement authority within the terms defined in the Clauses in accordance with the applicable law.

(iv) Security incidents (and provide adequate support to appropriately manage the possible data protection risks posed by such incidents), within the terms defined in the Clauses in accordance with the applicable law.

(v) Without undue delay, any request relating to the exercise of data subject’s rights received directly from the data subjects. In such cases, the CSP shall not reply to such a request unless otherwise instructed by the EU institution, and shall provide the EU institution with the necessary information and tools to manage data subjects’ personal data in terms of access, deletion, correction, blocking, etc.

J - Obligation to inform and cooperate with the EDPS

83 The CSP is aware that the EDPS has the right to conduct a visit, an audit or an inspection of the CSP[42], and of any sub-processor, under the same conditions applicable to an audit of

[42] It is essential to the auditability of the processing operations of the CSP by both the EU institution and the EDPS, the obligation, under Article 30 of the GDPR, for the CSP (as processor), to “maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(continued on next page)

the EU institution itself under [the proposed Regulation]. The audit shall aim at checking compliance of the processing of data entrusted by the EU institution to the CSP with the contractual obligations and with the applicable data protection rules and principles.

84 The CSP shall duly co-operate in those inspections, free of cost.

K - Security measures

85 The CSP shall ensure that it has **a proper IT Security Risk Management framework**[43] **in place** and has implemented the relevant technical and security measures set out under the relevant framework as well as those measures specified in the Contract and/or in the SLA before processing the data on behalf of the EU institution and that it will properly maintain the framework and manage the risks for the duration of the Contract.

86 In assessing the appropriate level of security the CSP shall take account in particular of the risks that are presented by the processing, in particular those deriving from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

87 The CSP shall maintain a documentation regarding the framework and the security and technical measures in place and shall provide the EU institution with adequate access to it, to enable it to comply with the requirements of [the proposed Regulation].

L - Data breach notification.

88 The CSP shall implement appropriate mechanisms to deal promptly and effectively with security incidents and personal data breaches. These shall include reporting mechanisms ensuring that the **EU institution is notified of any possible personal data breaches**[44] (security incidents affecting personal data processed on behalf of the EU institution).

89 The CSP shall notify relevant personal data breaches to the EU institution without undue delay and, where feasible, in due time for the EU institution to be able to notify, if needed based on the requirements of [the proposed Regulation], the impacted data subjects without undue delay and the EDPS within 72 hours after the CSP becomes aware of the breach.

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and of the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third Country or an international organisation, including the identification of that third Country or international organisation and the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 33.

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.”

[43] See also EDPS guidance referred to in footnote 51

[44] Some guidance on personal data breaches can be found in current WP29 draft Opinion, available at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

The GDPR contains specific provisions on the notification of personal data breaches to the supervisory authority and to the data subject under Articles 33 and 34.

90 The CSP shall provide the EU institutions with at least the following information:

- Nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.
- Likely consequences of the personal data breach.
- Measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

91 The CSP shall collaborate with the EU institutions to enable it to comply with all relevant obligations set out in [the proposed Regulation] on personal data breaches.

92 Further detail on the content and the form of the notification shall be defined in the SLA.

M - Audit (during and upon termination of the data processing activity)

93 The CSP and the sub-processor shall implement mechanisms for secure **logging of processing operations** on personal data performed on behalf of the EU institution.

94 The CSP shall allow and contribute to possible **audits** of its processing activities carried out by the EU institution, based on the relevant provisions of [the proposed Regulation][45]. The audit may be carried out **by a third party** selected by the EU institution, in possession of the required professional qualifications and bound by a duty of confidentiality.

95 The CSP and the sub-processor shall allow and contribute to audits of their data processing facilities, upon request of the EU institution and/or of the EDPS, as to the measures taken by the CSP to comply with their obligations upon termination of the personal data processing services.

N - Access by law enforcement bodies

96 Under Article 2 of the Protocol on the Privileges and Immunities of the European Communities, “The archives of the Communities shall be inviolable.” As an EU body, the EU institution is subject to the Privileges and Immunities of the European Communities, particularly as regards the inviolability of archives (including the physical location of data and services) and data security.

97 The CSP shall notify the EU institution of any legally binding request for disclosure of the personal data processed on behalf of the EU institution made by any public authority (e.g. a Member State national Prosecutor), including from non-EU countries, without delay[46]. The CSP shall not give access to the personal data unless authorised by the AIPN (*Autorité investie du pouvoir de nomination*) of the concerned EU Institution.

O - Service level

98 The CSP shall operate the service according to a Service Level Agreement, which forms an integral part of this Contract.

[45] Article 28(3) (h) of the GDPR.

[46] Access to Member State’s recipient (as the abovementioned State Prosecutor) will be provided by the EU institution only if the conditions laid down in EU law for such disclosure are fulfilled.

P - Contractual remedy

99 Any deviation from or infringement of the above points may be a ground for the EU institution to terminate the Contract with immediate effect, without prejudice to possible damages.

4.3. Operating the cloud service

100 Safeguards are needed during the operation of cloud services to protect personal data and comply with the applicable data protection principles and obligations[47].

101 The matters delegated to the CSP acting as processor should be described in the Contract (see section 4.2), where some of the operational aspects are usually defined within an SLA (see section 4.3.2) and need to be managed. What needs to be performed directly by the EU institution (see section 4.3.1) depends much on the cloud service and deployment model (see Annex 3 for their definition).

4.3.1. Tasks under the direct control of the EU institution

102 The EU institution shall set up the in-house organisational infrastructure that is necessary for ensuring that cloud computing services are operated in compliance with data protection rules[48].

103 Tasks that usually stay within the EU institution's direct control include:

- Data protection compliance as a controller, including:
  - Data protection risk (re)assessment and management.
  - Data protection safeguards and IT security controls and objectives definition, and management.
  - Handling data subjects' requests.
  - Notification of personal data breaches to the EDPS and to data subjects.
  - Data protection audits of the CSP.
  - The DPO and their role.
- IT governance and management
- Contract management.
- Service Level definition and management.

[47] The EU institution retains all its responsibilities for compliance issues as controller even if operations are carried out through a CSP. These include: lawfulness, necessity and proportionality; purpose specification and limitation; data quality, including retention periods; information to data subjects and data subjects' rights (access, rectification, erasure, blocking); possible transfers; provisions on internal telecommunications networks, where applicable; access by the supervisory authority along with any other applicable provisions.

[48] In this regard, as a source of best practices and as a check list, also including **training, monitoring and audit programmes**, see the WP29 Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents, of 27 February 2014, available at:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf.

- Data control and management (policies and plans for e.g. data access, storage, deletion, repatriation from the CSP).
- Audits (in general) of the CSP.

These tasks need adequate expert resources, mainly in contract, financial, IT, IT security and data protection management.

104 **Adequate resources in the IT field** may still be needed even in the SaaS service model in public cloud services, which features the highest level of delegation. In this case, if staff implementing the IT infrastructure and the specific service are no longer needed, staff able to understand and assess the appropriateness of IT architecture and design aspects and IT security policies and measures are still necessary to verify whether the solution is adequate under the data protection requirements.

105 **Policies** and **procedures** to carry out those tasks should be **described and available** for possible audits.

106 As to contract management, for example, the EU institution should **keep a list of sub-processing agreements notified by the CSP**, which should be **updated at least once a year**. The list shall be available to the EDPS upon request.

107 The **DPO** of the EU institution is the staff advising the EU institution on how to comply with the data protection law and principles and shall provide assistance according to the law[49]. They should always be **adequately involved,** from the very beginning of the process and throughout all the various steps, when designing and operating the cloud service, including:

- when assessing data protection risks, defining compliance requirements and relevant safeguards;
- if a DPIA needs to be performed as a mandatory requirement;
- when setting out the contractual clauses as well as the content of the SLA;
- when dealing with personal data breaches;
- when carrying out data protection audits.

108 The EU institution should also provide appropriate **training** on personal data protection rules for its personnel in relation to the use of the cloud service and for the monitoring of compliance of the service with data protection terms and conditions as stipulated in the Contract. Staff members concerned by this include: decision makers, process owners, contract managers, those who have permanent or regular access to personal data, who are involved in the collection and processing of personal data and IT staff involved in the development and operation of tools used to process personal data.

109 The EU institution should plan for possible **audits**, as appropriate considering the risks of the processing operation, on a regular basis or under specific circumstances requiring

[49] On the (enhanced) role of the DPO according to the GDPR, see in particular Articles 38 and 39.

them. It can perform them also through **third parties** accredited for appropriate cloud related certifications and standards. It is essential that:

- The audit program includes all aspects of personal data protection requirements and provides methods for ensuring that corrective actions will take place.
- The results of all audits should be communicated to the DPO and to the EU institution's management (for example, the Director of the EU Agency). The EDPS shall receive a copy of such audits upon request.
- The audit plan should enable the EDPS to be informed in advance, to join the audit, if it so decides, and to receive the results of the audit.

4.3.2. The Service Level Agreement (SLA)

110 **The SLA must be part and parcel of the contract and further define expected services and their level.** It is up to the EU institution to have these provisions either in the main body of the contract or in the SLA.

111 The content of an SLA depends clearly also on the service and deployment model, which impacts **on the respective allocation of direct control and the relevant responsibilities** on the EU institution and of the CSP.

112 The SLA should target and define at least the following elements and domains[50]:

- Detailed **description of the service provided**.

  This will integrate and detail what is missing in the Contract. Among others, the purposes of the operations processing personal data should be clearly defined.
- Clear **allocation of responsibilities** (as to the service operations levels - who does what, including as to the security measures) between the EU institution and the CSP, based on who has "de facto" control on the issue.
- **Communication channels** between the EU institution and the CSP, including the latter's Service Desk.
- **Service performance/quality and reporting:**

  Clear definitions of service performance, monitoring and reporting need to be agreed upon through measurable indicators and monitoring and reporting tools.
- Requested **capacity**.

  This refers, for example in case of a SaaS or PaaS, to instances and environments (development, testing, production, etc.), storage space, number of user and administrative accounts, etc.
- **Availability**

[50] Some further guidance on Cloud SLAs can also be found in deliverables issued by a consortium of industries under the EC's coordination: "Cloud Service Level Agreement Standardisation Guidelines" - Cloud Select Industry Group - Brussels, 24 June 2014, available at:

https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines.

This industry guidance should not be considered as an authoritative source and does not necessarily reflect the EDPS' point of view.

Availability targets, in different time bands and periods of the year or use typology, availability metrics, mean time between service incidents, maintenance windows, etc. Availability should be defined for the all requested environments. Specific care is needed for a common definition to avoid misunderstandings.

- **Backup policy, contingency management, disaster recovery and business continuity**.

Among others, retention times must be defined together with the actions to be performed on data when the retention time expires. Clear procedures to repatriate data at any moment, including data format and schedule, should be agreed and tested.

- **Change management**

Change management procedure that are relevant to the cloud service (those requested by the EU institution, such as new functionalities, changes in the SLA, and those changes that the CSP might propose, e.g. in a IaaS offer) must be defined and agreed so that the EU institution is in control of the data processing means and procedures.

- **Security measures and assurance levels**

The EU institution shall specify what security safeguards the CSP must put in place and verify the adequacy of those offered by the CSP. This should be part of the outcome of the assessment of data protection risks performed and includes:

  - Defining security objectives/assurance criteria/levels, possibly referring to existing best practices and standards.
  - Defining specific security measures/controls.

Effective encryption of personal data as necessary should be part of the measures.

See section 4.4 for more details on possible security controls.

- **Data protection safeguards**

The EU institution shall define in the SLA possible specific provisions, in addition to the security measures, on data protection, further specifying or adding safeguards not referred to in the Clauses, where appropriate.

- **Security incidents and personal data breaches**

More detail (including agreed notification channels and forms) should be provided further to what already stipulated in the Clauses. See also footnote n°44.

- **Monitoring and auditing, including forensics**

The CSP must log operations on personal data and put them at disposal, as needed, of the EU institution.

Features and reports enabling the EU institution to be in control should be defined as well as modalities and terms of audits/inspections of the CSP premises and its data centres by the EU institutions and the EDPS.

In case of need for forensics analysis by the EU institution or the EDPS, the CSP should have capabilities to cooperate in an efficient and effective way.

- **Service termination and hand-over**

Schedule and support for service termination and hand over, including data repatriation or export to a new CSP, should be defined. Support should include data repatriation or hand over to a new service provider. Procedures for permanent deletion at the end of the hand-over shall be included. Possible provisions for relevant verification through logs and premises inspection should also be included.

- **Secure deletion and disposal**

  The CSP must technically guarantee secure erasure mechanisms, such as destruction, demagnetisation or overwriting and provide the EU institution with an evidence of the conducted destruction, including on backup copies.

- **Penalties** for failing to comply with the SLA.

  Besides the right to compensation for any damage incurred as a consequence of a breach of Contract or of the SLA by the CSP, the EU institution should be entitled to suspend and/or terminate the Contract.

- Procedure for **SLA review**

  There should be a procedure for the review of the SLA. In no case, though, the CSP shall be allowed to change it unilaterally.

4.4. IT security measures

113 The security measures and relevant accountability should be reflected in:

- The Contract (including the SLA), for those measures that are under the control and operation of the CSP, or
- Internal policy/procedures as far as they are under the direct control of the EU institution.

114 A non-exhaustive **list of possible IT security measures** mitigating the specific risks of cloud computing services follows in recommendation **R2** as related to those risks. The risks are labelled according to the list of risks in Annex 4. Other non-IT safeguards are also described, to exemplify the risk based methodology, which mitigate the same risks with different impacts.

115 The value of their mitigating strength, where present, is not absolute but just aims at ranking the effectiveness of the different safeguards in the "average" situation.

116 The complete list of safeguards should be the outcome of the assessment of data protection risks, including an information security risk assessment[51] (which will, of course, also take into account the risks for outsourced information systems).

117 In any case it is recommended to refer to existing internal IT security policies and practices in the EU institutions and available IT security standards and best practices issued by industry and other organisations, such as the International Standards Organisation and the European Union Agency for Network and Information Security (ENISA). See also Annex 5 for a number of references.

[51] For further detail refer to the EDPS Guidance on "Security Measures for Personal Data Processing": https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/16-03-21_Guidance_ISRM_EN.pdf and to a letter from the EDPS to clarify the relationship between a DPIA and Information Security Risk Management:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Accountability/16-04-22_Mail_DPOs_WW_EN.pdf.

R2 - Confidentiality and integrity risks for data in transit over the Internet

The service required will be outside the EU institution's data centre and not reachable through leased lines. Another communication link needs to be provided, most probably the Internet, as per most CSPs.

Among possible safeguards:

- Use only CSPs that offer dedicated lines to connect to their services + effective encryption;

  Mitigating strength: high, very high

- Implement Virtual Private Networks (VPN) over the internet, possibly using encryption and authentication also at multi-protocol level;

  Mitigating strength: high

- Use strong encryption (e.g. HTTPS with effective TLS implementation);

  Mitigating strength: medium-high

R3 - Possible lack of availability linked to limited or no Internet access

Among possible safeguards:

- Multiple internet providers with hot-swap;

  Mitigating strength: high

- Redundant lines from the same provider;

  Mitigating strength: medium-high

- Do not use Internet but leased lines, as a link from the user to the CSP;

  Mitigating strength: very high

R4 - Internet surveillance risks (ISPs + internet backbone and routing infrastructure)

Among possible safeguards:

- Limit prospective CSPs to EU Countries

  Mitigating strength: medium-high

- Do not use Internet but leased lines, as a link from the user to the CSP, always within EU territory.

  Mitigating strength: very high

- Use end-to-end effective encryption (e.g. HTTPS with effective TLS implementation)

  Mitigating strength: high

R6 - Possible vulnerabilities in access policies and security controls

This risk exists specifically in case of multi-tenancy: public or community clouds.

Among possible safeguards:

- Request the CSP to provide evidence of implementation of relevant effective security measures that be adequate to the nature of the personal data processed, by:

- self-declaration of compliance with cloud security standards and best practices

  Mitigating strength: low

- providing assurance by accredited third parties (cloud security certification tackling this risk and adequate to the nature of the personal data processed).

  Mitigating strength: medium/high, depending on the trustworthiness of the certification scheme.

This assurance should be given throughout the service provisions and during service termination and hand over.

- Request the CSP to isolate the computing environment from other users‘ one:
  - Physical isolation such as the use of different servers for different users

    Mitigating strength: high

  - Using different virtual machines within the same server for different users

    Mitigating strength: medium

- Adequate encryption for data at rest and in transit within the cloud infrastructure among different security perimeters. The encryption robustness and the key management scheme should be determined based on the risk assessment. The possibility of keeping the data encrypted while being processed is still subject matter of research but the EU institution is invited to verify the status of the art. If encryption keys are managed by the CSP, adequate security measures to protect them are essential for encryption effectiveness[52].

  Mitigating strength:/high, very high if combined with good isolation from other tenants' data

R12 - Lack of appropriate auditability (by the EU institution or agreed third parties) and of supervision and investigation activities by competent authorities, including forensics

The EU institution should ensure that the CSP guarantees an appropriate level of auditability to be able to demonstrate, on request, compliance and efficiently and effectively respond to investigative inquiries. Some pre-conditions:

- Any processing of personal data must be securely logged to verify processing operations and responsibilities and that these logs are at disposal of the EU institution for checks. Those logs must be protected with the same measures as the originating personal data.
- Develop technical capability to manage and analyse logs.

Among possible safeguards:

- The EU institution or any third party on behalf of the EU institution to perform periodic audits of the CSP infrastructure affecting the requested service.

  Mitigating strength: in principle very high, but it depends on auditing capability and complexity of the CSP's IT infrastructure.

[52] Among others, papers from ENISA could be used to assess encryption algorithms and keys:

- Study on cryptographic protocols and Algorithms, key size and parameters report 2014.

- The CSP to provide evidence of accredited/mutually trusted third parties audits performed periodically. The third party accreditation should be according to a trustworthy cloud standard/certification, tackling relevant risks and adequate to the nature of the personal data processed.

  Mitigating strength: high

- The CSP to provide evidence of internal audits/self-assessments performed periodically, tackling relevant risks and adequate to the nature of the personal data processed.

  Mitigating strength: low; medium if in a recognised code of conduct framework

R14 - Possible vendor lock-in (activity sale or stop, due to bankruptcy or other.): data unavailable or different privacy policy/applicable law

Among possible safeguards:

- Design and periodically test a fall-back solution to support the targeted EU institution’s business processes. Periodic backup outside the CSP premises (either in the EU institution’s premises or by another CSP) needs to be performed to minimise the possible data lost.

  Mitigating strength: high

- Design and test a migration plan to change CSP.

  Mitigating strength: needed but not sufficient

R18 - Other cloud computing specific IT security risks (see also Annex 4).

Here we just provide an example. For all other cloud specific IT security risks we invite you to consult your Security Officer and specialised references such as in Annex 5.

<u>Vulnerabilities linked to the use of the client software</u>

The cloud service might imply the use of (usually thin) clients such as commercial browsers or other clients or mobile apps developed by the CSP. This could lead to any possible related risks due to vulnerabilities on the client agent. This is not just a cloud specific risk but could be a change with respect to the currently used IT system and thus pose new risks, which could have an impact also on other systems and personal data managed by the EU institution.

Among possible safeguards:

- In the choice and configuration of the browser, the EU institution should give specific consideration to its privacy related features/weaknesses, such as:
  - the encryption of channel for the HTTP communications and specifically the support for strong protocols and encryption keys;
  - any other processing operations on the transmitted/received data that is not needed for the use of the cloud service (including transfers of data to recipients other than the cloud service)
- The EU institution could consider using browsers dedicated to the cloud service so that the impact of attacks coming from other websites could be limited. A stronger measure would be using a virtual desktop connected to a remote secure dedicated server where the dedicated browser is installed.
- If the CSP provides their own client to connect to the cloud service, the EU institution should request that the CSP adequately manage the security risks linked to the client.

- Specific care should be given to the security management of mobile apps as cloud clients[53], due to their specific risks[54].
- The EU institution should timely install security updates from commercial browser companies or from the CSP.

[53] See EDPS guidelines on the protection of personal data processed by mobile applications provided by EU institutions and bodies, available at:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/16-11-07_Guidelines_Mobile_apps_EN.pdf.

[54] See also Article 29 Working Party Opinion WP202 on apps on smart devices, available at:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

Annex 1. Glossary

Term	Description
Authentication	The process to ensure and confirm the identity of a user or a machine performing an operation (usually via an IT system)
Encryption keys	Pieces of information that are usually used to encrypt (or decrypt) data in a unique way. As such they represent the "secret" allowing to eventually enable the selective disclosure of the data only to those who know that secret.
Virtual Private Network (VPN)	A VPN is a point-to-point secure (encrypted) connection usually built over a public network
Cloud Service Provider (CSP)	A provider of cloud-based IT services.
Personal data	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.
Special categories (of personal data)	Under the current Regulation those data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life. The proposal for a new Regulation adds genetic data and biometric data for the purpose of uniquely identifying a natural person. These categories are subject to specific rules.
Controller	Community institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data.
Processor	Natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
Sub-processor	Natural or legal person, public authority, agency or any other body which processes personal data on behalf of a processor.
Data Protection Officer (DPO)	Staff member of an organisation tasked with supporting the organisation in ensuring compliance with the applicable data protection law. Appointment, tasks and powers are defined in the Regulation (and the new Regulation).
Data subject	Individual whose personal data are processed.

Standard Contractual Clauses (SCC)	Clauses, to be used in contracts between controller and processor or between a processor and another processor acting as sub-processor, provided for by the Regulation (and the proposal for a new Regulation), adopted by the European Commission or by a supervisory authority according to the procedures in the law and providing the needed contractual assurance.
Binding Corporate Rules (BCR)	Rules including all essential principles and enforceable rights to be used by a group of undertakings for international transfers of personal data from the Union organisations within the same group of undertakings to ensure appropriate safeguards as provided by the law.
Data Protection Impact Assessment (DPIA)	Assessment of risks to the rights and freedoms of natural persons due to the processing of their personal data. The new Regulation provides mandatory elements and circumstances under which it is obligatory. Nonetheless, controllers can carry out this assessment and obtain relevant benefits beyond those circumstances.
Framework contract	The framework contract is a contract template associated to a public procurement procedure, which, once the procurement is awarded, needs to be further instantiated into “specific contracts” in order to further and definitively specify the contractual terms for the provision of services or products.
Specific contract	See definition of “framework contract”.
Service Level Agreement (SLA)	Official commitment, often part of contracts, defining the quality of the services delivered by the provider to the customer. For example, the minimum average monthly availability of a cloud service can be an element defined in an SLA.
Certification	Confirmation of compliance to standards/best practices by authorised third parties. Certifications may support CSPs as an element to ensure compliance with the new data protection rules if according to what is provided for in the law.
Code of Conduct	A series of self-determined rules that individuals or companies may use to commit themselves beyond what already mandatory by law or to implement what is mandatory by law. Codes of conduct may support CSPs as an element to ensure compliance with the new data protection rules if according to what is provided for in the law.
Virtual machine	A virtual machine is a “virtual” computer running on a physical computer, with its own operating system, application and devices, isolated from other virtual machines running on the same physical computer. This is possible via a "virtualisation” software application running on that computer.

Annex 2. Further legal analysis

This Annex provides some further legal insight and reasoning to support the guidance given in the chapters, without aiming at being exhaustive.

Hereafter, we briefly present some reasons (**on top of the one regarding the applicability of the Protocol on Privileges and Immunities of the European Communities**) supporting **the recommendation** made at paragraph 63 of these Guidelines, namely that the processing of personal data entrusted by EU institutions to CSPs, and any sub-processing, **as a rule**, takes place **within the EU**[55].

1) The location of the CSP and of its data centre and/or servers outside the EU are factors that, *among others*, determine the applicability or not of the law of a third Country (issue of applicability of third Country law and jurisdiction).

Some examples relating to **different areas of law** (other than data protection legislation) could be briefly mentioned, as follows:

i) As for the application of **criminal law**, we recall that access by a non-EU Law Enforcement Authority (LEA) to a data centre **located in a Member State of the EU** would require -as a rule- a request by the LEA to the Member State pursuant to a specific international agreement, Mutual Legal Assistance Treaty (MLAT) or Memorandum of Understanding, setting out adequate data protection safeguards[56]. Such MLAT request would **not** be required in case of access by the non-EU LEA to a datacentre located in its own territory.

At the same time, we recall that the **Cybercrime Convention** (Budapest Convention)[57], as common safeguard also applying to non EU Member States which are Parties to the Convention, lays down, under Article 15, that "Each Party shall ensure that the establishment, implementation and application of the powers and procedures [for criminal investigations] incorporate the principle of **proportionality**."

[55] Processing outside the EU should be *the exception* (for example, in case of low risk data processing) and the EU institution shall describe and justify in this case the necessity of those processing operations, taking special care due to possible data protection risks and risks to effective supervision by the supervisory authority.

In this case, the rules on transfers of personal data to non-EU countries would also apply. For guidance on transfers of personal data to non-EU countries and international organizations, based on current Regulation (EC) No. 45/2001, please refer to the EDPS Position Paper "Guidance on International Transfers: Article 9", including the relevant EDPS Cases, available at:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf.

Please note however that the aforesaid EDPS Paper will be updated to take into account the revised provisions of the proposed Regulation on international transfers of personal data.

[56] In case 'Microsoft Ireland', the United States Court of Appeal for the Second Circuit on 14 July 2016 ruled that the US law (Stored Communication Act, SCA) "*does not authorize a U.S. court to issue and enforce a SCA warrant against a United States-based service provider for the contents of a customer's electronic communications stored on servers located outside the United States. The SCA warrant in this case may not lawfully be used to compel Microsoft to produce to the government the contents of a customer's e-mail account stored exclusively in Ireland.*" The US Court of Appeal referred among other to the criterion of '*locus rei sitae*'. The ruling is available at: http://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412.

[57] The **Convention on Cybercrime** of the Council of Europe (CETS No.185), known as the Budapest Convention, is available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

ii) Under **civil procedural law**, a data centre located in an EU Member State (and thus subject, according to the general principle of territoriality, to the civil procedural law of that Member State) cannot be searched for civil litigation-'**pre-trial discovery**' under US law (that is, the mandatory disclosure of information that itself may not be of direct relevance but could lead to the discovery of relevant information before the trial). In this case, as recommended by the Article 29 Working Party, requests for disclosure should preferably be made through the Hague Convention on the taking of evidence abroad in civil and commercial matters, which "provides a standard procedure for issuing "letters of request" or "letters rogatory" which are petitions from the Court of one Country to the designated central authority of another requesting assistance from that authority in obtaining relevant information located within its borders.". Conversely, a data centre located in the US is searchable for such pre-trial discovery ("litigation hold") under the jurisdiction and according to the applicable law of the US.[58]

iii) With reference to the activity of **national intelligence services**, we point out that: "All Member States [of the EU] are Parties to the "European Convention on Human Rights" [ECHR]. Thus, they have to comply with the conditions Article 8 ECHR provides for their own **surveillance programmes**. (...). Article 1 ECHR also obliges the Parties to secure everyone within their jurisdiction the rights and freedoms provided in the Convention. In both scenarios, **EU Member States, as well as any Party to the ECHR**, can be brought before the ECtHR for a violation of European legal subjects' right to respect for private life"[59].

These safeguards do **not** apply to States that are **not** party to the ECHR (the list of States, which signed and ratified the ECHR is available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures?p_auth=55fMgptN). All EU Member States are parties to the ECHR.

In substance, the storage and processing of data at a datacentre or by a company located in the territory of a given Country ordinarily triggers the competence of the public body of that Country to request access to the data processed in said datacentre in the context of an enforcement action **applying the public law** of such Country (e.g. criminal law, procedural law, data retention legislation, etc.). This **risk** must be carefully assessed by the EU institution.

2) Moreover, we recall the recent **case law** of the Court of Justice of the European Union (CJEU):

[58] See WP29 Working Document 1/2009 on **pre-trial discovery for cross border civil litigation**, available at:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf.

[59] Opinion of Article 29 Working Party 04/2014, On surveillance of electronic communications for **intelligence and national security** purposes, available at:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.

The European Parliament, in its Resolutions of 10 December 2013 on cloud computing and of 12 March 2014 on surveillance, expressed concerns regarding in particular the access by Third Countries intelligence services to cloud providers using storage servers located in Third Countries.

See also the study by the EU Fundamental Rights Agency (FRA) "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU", available at: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-surveillance-intelligence-services_en.pdf.

This report maps the legal frameworks on surveillance in place in EU Member States. It also details oversight mechanisms introduced across the EU, outlines the work of entities tasked with overseeing surveillance measures, and presents the various remedies available to individuals seeking to challenge such intelligence activities.

In the '**data retention case**'[60], the CJEU pointed out (at para. 68) to the circumstance that: « *[the data retention] directive does not require the data in question to be retained within the* ***European Union****, with the result that* ***it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security*** *(…) is fully ensured. Such a* ***control****, carried out on the basis of* ***EU law****, is an essential component of the protection of individuals with regard to the processing of personal data* » (*emphasis added*).

In the '**Schrems case'**[61], the CJEU also highlighted that **effective control by fully independent Data Protection Authorities**, provided with all powers which are necessary in this respect, is an essential element of protection of personal data.

In the '**Tele2 case**'[62], similarly the CJEU stated (at para. 122) that: "With respect to the rules relating to the **security and protection of data** retained by providers of electronic communications services, it must be noted that Article 15(1) of Directive 2002/58 does not allow **Member States** to derogate from Article 4(1) and Article 4(1a) of that directive. Those provisions require those providers to take appropriate technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data. Given **the quantity** of retained data, **the sensitivity** of that data and **the risk of unlawful access** to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. In particular, the national legislation must make provision for the data **to be retained within the European Union** and for the irreversible destruction of the data at the end of the data retention period" (*emphasis added*).

3) In case of hosting location of the cloud architecture in non-EU Member States, it could also be **more problematic for the EDPS to cooperate and coordinate inspections** with national EU 'fellow DPAs' and thus ensure the overall enforcement of the rules of the Regulation.

Therefore, in the light of the above, **the EDPS recommends that -*as a rule*- the processing of personal data entrusted by EU institutions to CSPs (including for back up, business continuity purposes and transit, as well as locations from where remote operations are performed), *and any sub-processing*, takes place within the EU**.

[60] Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, of 8 April 2014.

[61] Judgment of the Court (Grand Chamber) of 6 October 2015 (request for a preliminary ruling from the High Court (Ireland)) — *Maximillian Schrems v Data Protection Commissioner* (Case C-362/14).

[62] Judgement of the Court of Justice of the European Union in Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, of 21 December 2016.

Annex 3. Cloud computing: basic concepts and models

Cloud computing definition

Cloud computing technologies and services can be implemented in a wide variety of architectures, under different service and deployment models. The term is used with different meanings in different contexts. The most widely used definition is that published by the US National Institute of Standards and Technology (NIST)[63] which states that "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". The NIST document defines three service models (Software as a Service - SaaS; Platform as a Service - PaaS; and Infrastructure as a Service - IaaS) and four deployment models: public, private, community and hybrid (a composition of the former three models) cloud environments. In these Guidelines, the terms and acronyms should be understood within the meaning of that definition.

As said earlier, these Guidelines focus on public cloud environments as they pose specific personal data protection challenges. Hybrid cloud services involving private and public cloud infrastructures are also in scope because of the public component and its interaction with private infrastructures in providing services.

Traditional outsourcing and cloud computing

Using public cloud services is indeed a new way of outsourcing. This is so when an organisation that used to process their data in their own data centre decides to use a cloud based service. This involves both the risks of traditional outsourcing and those specific to cloud computing, which are explored in Annex 4. So, cloud computing is not “just another way of outsourcing” and needs specific analysis and safeguards.

It is worth noticing that some IT companies are advertising any service available through the public internet as cloud-based, even if it does not meet cloud service criteria such as:

- On-demand self-provisioning of computing capabilities such as server time and network storage.
- Easy and quick resources provisioning and scalability, with pay-per-use model.
- Broad access over the internet with standard client user agents (e.g., browsers).
- Pooling of providers’ dynamically assigned resources to serve multiple cloud users, with no user knowledge and/or control over resource location.
- Seamless optimisation of measured resources allocated by the service provider.

Not all services offered over the Internet possess indeed these characteristics, which can also be present in different degrees, depending also on the service model. Furthermore private, community and other promiscuous deployment models have appeared that retain or drop cloud specific features also based on their specificity. Cloud computing specific risks are linked to these features, the way they have been implemented, and the way cloud computing companies and services have developed.

[63] US NIST SP 800-145, The NIST Definition of Cloud Computing, Sept. 2011. Link: https://csrc.nist.gov/publications/detail/sp/800-145/final.

Examples of publicly available cloud services

Even though every IT service can nowadays be deployed and operated in a cloud environment, some examples of cloud based services are reported that might be of interest for the EU institutions, to render the relevance of the topic under discussion and the inherent risks. A non-exhaustive list follows:

- SaaS: basic data storage services, office automation suites, document and workflow management services, staff management applications, mobile device management platforms.
- PaaS: software infrastructure, such as virtualised servers with specific OSs and basic related software stack, e.g. web and application servers, databases, commonly used programming languages environment and other tools. Linux based set of virtual machines with relevant software stack and open source databases and software utilities is an example that could be used by EU institutions to deploy and operate e.g. websites;
- IaaS: computing infrastructure made up of virtual machines, storage and network infrastructure, including security devices, where in principle any kind of software service under any platform can be deployed and operated. EU Institutions could use IaaS services to replace their own data centre.
- Hybrid: an EU institution might want to use technology that provides ideally seamless load balancing or dynamic allocation of public cloud resources to integrate and supplement their own storage or computing infrastructure.

These could be provided by either commercial CSPs or by “outsourced private (or community) cloud” infrastructures (where machines are outsourced by the EU institution to a hosting company in a cloud configuration) or even by completely private or community cloud infrastructures owned by one or more EU institutions[64].

[64] See reference in the previous footnote for a more in depth description of possible deployment models.

Annex 4. Data protection specific risks of cloud computing

In this section, we identify high-level risks entailed by the use of cloud computing services. First, a list of risks linked to the general cloud computing features of a public cloud infrastructure is proposed. Then those risks are further analysed for specific types of cloud services, based on other existing service and deployment models (see Annex 3, and a relative assessment is made with respect to the other models).

These risks need to be integrated and possibly further detailed in a comprehensive data protection risk assessment (or DPIA - see section 4.1) whereby all possible threats and vulnerabilities having an impact on personal data are considered and all compliance requirements are taken into account.

Each specific feature of cloud computing involves relevant data protection risks. Some cloud features can jointly concur in posing, or reinforcing, certain risks.

- *Fx – cloud computing feature description*
  - ➢ *Rx – risk description*

- ***F1 - The EU institution has not used or has had limited experience with cloud based services.***
  - ➢ **R1 - No previous sufficient experience with procuring cloud computing services** could lead to underestimating the risks or choosing inappropriate safeguards. Relying on cloud services for core institutional business processes or for processing of sensitive data without expertise could jeopardise data protection institutional tasks and responsibilities and have consequences on data subjects.

- ***F2 - Services are offered over the public Internet****, which represent the usual communication link between CSPs and cloud users. This would represent a change for the EU institution that in general processes its data in its own data centre or in the data centre of another EU institution (e.g. EC - DIGIT) usually connected through dedicated communication links.*
  - ➢ **R2 - Confidentiality and integrity risks for data in transit over the Internet**. Unauthorised access and change of data in transit can happen along the internet links between the CSP and the cloud user, including the fixed and mobile infrastructure to access the Internet Service Providers (ISPs). The unauthorised access to personal data might cause that the data will be used for purposes that are different than those authorized and agreed upon and cause damage to the data protection and privacy rights of the individuals concerned.
  - ➢ **R3 - Lack of availability** linked to limited or no Internet access due to wrong capacity planning, possible internet service provider unavailability, network congestion, cyber-attacks, etc. In this case, the EU institution, and the data subjects, would not be able to access their data.
  - ➢ **R4 - Internet surveillance by governments and security services** on ISPs, the internet backbone and the routing infrastructure. There could be an interest in certain personal data processed by the EU institution by governments and security services of the Countries crossed by the internet segments possibly used to connect to the prospective CSP.

- **R5 - Intrusive data retention legal provisions for law enforcement purposes** applicable over the CSP and ISPs could increase the usual retention period thus augmenting the probability of possible abuse and data leaks. This can vary from Country to Country, including within the EU. Nonetheless, as highlighted in Annex 2, higher level of cooperation with the EDPS and higher data protection safeguards are expected in case of EU countries, as opposed to non-EU ones.

- ***F3 - Multi-tenancy nature of public cloud services,*** *usually hosting data of different customers in the same data centre or even within the same security perimeter or the same server.*
  - **R6 - Possible vulnerabilities in access policies and security controls**, such as accidents and cyber-attacks coming from the client infrastructure of one or more of the various users of the CSP could compromise the EU institution's data. Furthermore the different CSP users might be based in Countries with a level of protection for personal data that is different (lower) than the one of EU countries (see also R7).

- ***F4 - The physical location of cloud user's data may be unknown to the user or, if known, rarely verifiable.*** *Medium - large cloud providers usually have data centre located in many Countries. Data can be dynamically located in the different data centres depending on computing resource availability, redundancy needs and economic factors. The data location is not always communicated to the cloud user or this is done with limited precision (e.g. only country name).*
  - Foreign jurisdiction issues:
    - **R7 - Different applicable laws** and thus possible different levels of data protection, depending mainly on whether data are located inside or outside the EU. It can also happen that the headquarters of the CSP are in the EU but the company has subsidiaries or use sub-processors outside the EU. Different requirements, as currently laid down in Regulation (EC) No. 45/2001, and, for the future, in the proposed Regulation[65] apply in this case to the EU institution, triggering the applicability of the rules on transfers of personal data to non-EU countries.
    - **R8** - Increased risk of **CSPs required to cooperate with/disclose data to law enforcement authorities based on rules different from EU ones** or anyhow nor complying with rules applicable to the EU institutions.
  - **R9** - Increased risk for **cloud users and data subjects of not being in control of their data** (location).

- ***F5 - Trend towards "commoditisation" of the IT service.***

  Cloud services offer the EU institutions the opportunity of delegating (more or less, depending on the service and deployment models) the IT management to the CSP, often with minimal interaction for service provisioning and configuration.

  Due to the necessity of managing a critical mass of computing resources to offer cloud services and to CSPs market concentration, a contractual imbalance often exists between CSPs and cloud customers, especially if the latter are individuals or SMEs. In

[65] See Article 9 of the Regulation; Articles 44-50 of the GDPR.

the EU institutions' context this can happen in particular to small organisational units and small institutions and bodies.

Economies of scale, allowing lower services fees, rely also on rigid contractual terms and little customisation of features and conditions.

- **R10 - Unfair and rigid terms of use and service contracts**. Possible "take it or leave it" terms of use and contractual terms are offered with little or no negotiation options and unilateral possible change of terms by the CSP, with short or no pre-notice. These contracts might not offer the EU institution the instruments to adequately protect personal data and comply with Regulation (EC) No. 45/2001 and, even more so, with the proposed Regulation.

- **R9 - Increased risk for cloud users and data subjects of not being in control of their data** (general). This risk is not new and is typical of any outsourcing, but it is particularly significant for cloud services. Despite the level of delegation enjoyed by the CSP, the responsibility as a "controller" to comply with the data protection provisions stays always with the EU institution.

- **R11 - Lack of control over the security measures.** The EU institutions can design and implement the security measures to protect personal data for the part of the cloud service they are in control of. This depends heavily on the service and deployment models (see following sections). For what is delegated to the CSP, users are usually not offered the possibility to manage the security risks and choose the appropriate technical and organisational security controls, as requested by Regulation (EC) No. 45/2001[66] and by the proposed Regulation[67].

- **R12 - Lack of auditability** by the cloud user or third parties to get assurance that the CSP, as a processor, is acting on behalf of the EU institution and provides sufficient guarantees as to the implementation of the security controls[68]; this also includes **possible obstacles to supervision and investigation activities** by competent authorities, including forensics.

- **R13 - Challenges for effective replies to data subjects exercising their data subject's rights**, such as requests for exhaustive information on the processing of personal data relating to them, requests for data blocking and erasure, etc. in accordance with Regulation (EC) No. 45/2001[69] and the proposed Regulation[70].

- **R14 - "Vendor lock-in" following the sale or stop of the CSP's activity**, due to bankruptcy or other unexpected events: data could be unavailable or different applicable law or data protection contractual provisions might apply for the new CSP without the EU institution being able to intervene.

- **R15 - Lack of data portability.** Proprietary formats, specific data schemes and the use of other supporting application could jeopardise an efficient and effective repatriation of the EU institution's data and virtual machines configuration or their hand over to a new CSP. Furthermore, there is the risk that the personal data are not permanently erased by the (former) CSP after the hand-over.

[66] Articles 22, 35 and 36 of the Regulation.

[67] Articles 32-34 of the GDPR

[68] As required by Article 23 of the Regulation.

[69] As required by Article 28 of the GDPR.

[70] Articles 13-20 of the Regulation; Articles 17-23 of the GDPR.

- ***F6 - Several providers and sub-processors can operate together, e.g. in a complex and layered approach, to provide the service requested, and a dynamic integration of new players is often possible.***

  - **R16 - Not clear allocation of responsibilities within the service providers chain (CSPs and sub-processors)** in implementing safeguards and personal data processing requirements such as data quality, data security, ensuring data subject’s rights and auditability. Processors’ and sub-processors’ responsibilities could get lost within the chain so that nobody takes them on.

- ***F7 - Increased number of personal data transfers performed in a seamless and fast way involving many parties and crossing borders, and data replication for better availability and faster access.***

  - **R9 - Increased risk for cloud users and data subjects of not being in control of their data** (location, jurisdiction, level of protection).

  - **R13 - Possible challenges for an effective application of data subject’s rights** (see above).

  - **R17 - Challenges for data retention and effective data erasure**. The available cloud-based applications might not provide adequate features to correctly manage the retention time so that data are permanently deleted when no longer necessary for the purposes lawfully pursued. Furthermore, the CSP might use a cloud infrastructure where data might be replicated for hot swaps and disaster recovery with the risk of leaving around copies of the data also after erasure through the available cloud service functional features. Repositories could also be moved from one server to another for cloud infrastructure optimization and a possible failure of the mechanism could leave unnecessary copies of the data.

- ***F8 - (Personal) data security in a cloud infrastructure implies specific risks compared to a “traditional” on-premises data centre.***

  If in certain cases CSPs might offer better security measures that those implemented in a “traditional” data centre managed by the EU institution, the typical cloud-based design introduces specific risks or amplifies existing ones.

  Some cloud security issues that have data protection consequences have already been identified elsewhere in this section. Other IT security specific risks need to be tackled, too.

  - **R18 - Other cloud computing specific IT security risks (not exhaustive):**

    - Security of the user’s agent (e. g. browser, mobile app)
    - Authenticity of the requested services
    - Challenging management of encryption keys
    - Identity and authentication management challenges
    - Virtualisation layer and virtual machines vulnerabilities.

Specific issues in the IaaS service model

In this model, virtual machines are allocated by the CSP to the user from a pool of common resources. The cloud user has control over many configuration aspects of the IT infrastructure, over the software platform and the applications developed over it. No control at all over data centre physical security.

- ***F5***

    - ➢ Lack of transparency over some aspects of the underlying technical infrastructure (basic virtualisation software, hardware and some networking) and relevant technical and organisational safeguards.
    - ➢ Control over the security measures at application and platform level. Limited control over some low level machine software security, network security and no control over data centre physical security.
    - ➢ Possible implementation of auditability at application, platform and machine configuration level. Limited (insofar as networking is configurable) or no implementation of auditability at network level and no control over possible auditability features on physical security.
    - ➢ Tools to accommodate data subjects' rights can be developed.
    - ➢ Lower portability related risks.
- ***F3***
    - ➢ Here the risk focuses on shared resources (basic networking infrastructure, hardware and physical security) and is lower than in the SaaS and PaaS models.

Specific issues in the PaaS service model

In this service model operating systems with programming languages and other software tools including compatible data repositories are provided by the CSP to the user, deployed over virtual machines. The cloud user has control only over some configuration aspects of the platform, the applications developed over the platform and the data processed. No control at all over the underlying IT infrastructure and the data centre physical security.

- ***F5***
    - ➢ Lack of transparency over some aspects of the underlying technical infrastructure (but for software platform configuration and applications, hardware and networking) and relevant technical and organisational safeguards.
    - ➢ Control over the security measures at application level and some at platform level. Limited control over network security and no control over data centre physical security.
    - ➢ Possible implementation of auditability at application and platform level. Limited or no auditability at network level and no control over possible audits on physical security.
    - ➢ Tools to accommodate data subjects' rights can be developed.
    - ➢ Some portability challenges because of possible different implementations of software platforms and possible different performance issues.
- ***F3***
    - ➢ Further to what already mentioned, here processing operations belonging to different users might even share the same server.

Specific issues in the SaaS service model

The user is provided with a software application supporting specific business processes. The cloud user has control only over the configuration of the cloud-based application and the data processed. No control at all over the application code OSs, databases, webservers, application servers, virtual machines and basic virtualisation software, physical servers, networking and security devices, the data centre physical security.

- ***F1***
    - This risk of underestimating the risks or choosing inappropriate safeguards is higher because business departments could be tempted at procuring SaaS cloud services without sufficient IT and data protection expert advice.
- ***F5***.
    - Lack of transparency and control over the application code and the underlying technical infrastructure and technical and organisational safeguards
    - No control over the security measures but for some at application level (e.g. user authentication and authorisation over application features).
    - Lack of implementation of auditability particularly high.
    - Possible lack of tools to accommodate data subjects' rights.
    - The lack of portability could be increased by specific formats and other possible constraints such as application business rules, specific workflows, settings and dependencies from other applications.
- ***F3***
    - Further to what already mentioned, here more specifically e.g. processing operations belonging to different users might run within the same virtual machine or even in the same application instance, which further increases risks.

Specific issues in the Outsourced Private/Community Cloud deployment model

Here some machines within a user(s)-specific security perimeter are deployed in CSP's data centres for the exclusive use of the cloud user(s).

- ***F2***

    Services are not necessarily offered over the public Internet: if so, no relevant risks.

    Dedicated communication link could be available or setup. In this case:

    - Possible confidentiality and integrity risks limited to the communication service provider.
    - Lack of availability linked to communication service provider unavailability (due to technical failure or other).
    - Possible risks linked to data retention for law enforcement purposes.
- ***F3***
    - The risk is lower (even of the public IaaS) and often limited to some basic networking resources and physical security. Nevertheless, systems formerly deployed in different security perimeters and under different responsibilities, are now together within the same cloud infrastructure and exposed to different security risks. This is even more applicable to community clouds.
- ***F4***
    - This risk is far lower or more often does not exist in an outsourced private cloud.
- ***F5***

    - Transparency, choice of security measures, auditability related risks are far lower, since in general the user has more control.
    - Far lower risk of not accommodating data subject’s rights, having a level of control that is in general higher than the public IaaS.
    - Lower portability related risks.

- ***F6***
    - In case of external contractors the risk stays, even though is usually lower than in public clouds because the user has more contractual negotiation power.

- ***F7***

  Locations are usually known by the user and processing more under control:
    - Far lower risks linked to transfers and data subjects’ rights.
    - Lower risks for data retention and effective erasure, just because of the intrinsic seamless mechanisms for allocating resources in a cloud-based infrastructure (redundancy, dynamic allocation, distributed paradigm).

- ***F8***
    - The following risk are very limited if the public internet is not used as a communication link to the outsourced services:
        - authenticity of the requested services
    - The following risks are in general very limited:
        - challenging management of encryption keys
        - identity and authentication management challenges.

Specific issues in the On-site Private/Community Cloud deployment model

Here the cloud infrastructure is deployed within the security perimeter of the cloud user(s) in their premises. In case of community clouds, one or more of the participating entity will be hosting the infrastructure for all.

- ***F2***
    - Services are not offered over the public Internet: no relevant risks for private clouds. In case of Community clouds, some cloud users will need to use communications facilities to connect. In this case the same considerations as for Outsourced Community Clouds apply.

- ***F3***
    - Basically far lower risk. Nevertheless, systems formerly deployed in different security perimeters and under different responsibilities, are now together within the same cloud infrastructure and thus exposed to different security risks. This is even more applicable to community clouds.

- ***F4***

  The physical location of cloud user’s data is known by the user: no relevant risks.

- ***F5***

  In general very low or no risks but:

    - Some very low transparency risks are left because of the intrinsic dynamic and seamless mechanisms for allocating resources in a cloud-based infrastructure. Nevertheless, the user has complete control over it.
    - Some very low risks for effective application of data subjects’ rights are left because of the intrinsic seamless mechanisms for allocating resources in a cloud-based infrastructure (redundancy, dynamic allocation, distributed paradigm). Nevertheless, the user has complete control over it.

- ***F6***
    - No risk of unclear allocation of responsibilities if the cloud infrastructure is managed by internal staff.
- ***F7***

  Locations are known by the user and processing more under control:
    - Far lower or no risks linked to transfers and data subjects’ rights.
    - Some very low risks for data retention and effective erasure are left, just because of the intrinsic seamless mechanisms for allocating resources in a cloud-based infrastructure (redundancy, dynamic allocation, distributed paradigm).
- ***F8***
    - The following risks are far lower or not any longer specific since the cloud infrastructure is private and not outsourced:
        - challenging management of encryption keys
        - identity and authentication management challenges
        - authenticity of the requested services.

Annex 5. References and useful readings

Policy papers from EDPS, Article 29 Working Party

- Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", November 2012:

  https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf

- Article 29 Working Party Opinion 05/2012 on Cloud Computing:

  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

Policy papers from other EU Data Protection Authorities

- "Guidance on the use of cloud computing" - UK Information Commissioner's Office (ICO), October 2012:

  https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

- "Personal data protection and cloud computing" - Information Commissioner of Slovenia, June 2012:

  https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Cloud_computing_and_data_protection_-_ENG_final.pdf

- "Data protection 'in the cloud'" - Data Protection Commissioner of Ireland, July 2012:

  https://www.dataprotection.ie/docs/03/07/12_Cloud_Computing/1221.htm

- "Recommendations for companies planning to use Cloud computing services" - Commission Nationale de l'Informatique e des Libertés (France), June 2012:

  https://www.cnil.fr/sites/default/files/typo/document/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf

- "Cloud computing: how to protect your data without falling from a cloud" - Vademecum - Garante per la Protezione dei Dati Personali:

  http://194.242.234.211/documents/10160/2052659/CLOUD+COMPUTING+%E2%80%93+PROTECT+YOUR+DATA+WITHOUT+FALLING+FROM+A+CLOUD.pdf

- Guía para clientes que contraten servicios de Cloud Computing - 2013, Agencia Española de Protección de Datos:

  http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf

- Resolution on cloud computing, Punta del Este, Uruguay, 26 October 2012, 34° Conferencia Internacional de Autoridades de protección dos datos y privacidad:

  http://194.242.234.211/documents/10160/2150357/Resolution+on+Cloud+Computing.pdf

Papers and references from the European Union Agency for Network and Information Security (ENISA)

- ENISA on cloud computing: https://www.enisa.europa.eu/topics/cloud-and-big-data

In particular see:

  - Relevant publications: https://www.enisa.europa.eu/topics/cloud-and-big-data?tab=publications
  - Relevant articles: https://www.enisa.europa.eu/topics/cloud-and-big-data?tab=articles
  - On cloud security: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security

Papers from standardisation organisations

- "Privacy in Cloud Computing" - International Telecommunication Union Telecommunication Standardisation Sector (ITU-T) Watch Report, March 2012:

  http://www.itu.int/en/ITU-T/techwatch/Pages/cloud-computing-privacy.aspx

- ISO/IEC 27017:2015 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services:

  https://www.iso.org/standard/43757.html

- ISO/IEC 27018:2014 - Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors:

  http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498

Papers from the industry: the Cloud Select Industry Group (CSIG)

- "Cloud Service Level Agreement Standardisation Guidelines" - Cloud Select Industry Group - Brussels, 24 June 2014:

  https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines

Papers from the industry: the Cloud Security Alliance (CSA)

https://cloudsecurityalliance.org/download/

Policy papers from the International Working Group on Data Protection in Telecommunications (Berlin Group)

- Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum", Berlin Group, April 2012:

  https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=3065

Technical papers from NIST

- NIST Cloud Computing Program

  https://www.nist.gov/programs-projects/cloud-computing

- "The NIST Definition of Cloud Computing" - NIST Special Publication 800-145, September 2011:

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

- “Cloud Computing Synopsis and Recommendations” - NIST Special Publication 800-146, May 2012:

  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

- “Guidelines on Security and Privacy in Public Cloud Computing” - NIST Special Publication 800-144, December 2011:

  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Other technical and policy papers

- “Cloud Computing Security Considerations” - Australian Government Department of Defence - Intelligence and Security - Cyber Security Operations Centre, September 2012:

  http://www.asd.gov.au/publications/csocprotect/Cloud_Computing_Security_Considerations.pdf