EUROPEAN
COMMISSION

Brussels, 18.6.2020
C(2020) 4190 final

Standard under Decision (EU, Euratom) 2017/46

Principles for outsourcing of communication and information systems

Table of Contents

1. INTRODUCTION 2
2. SCOPE 2
3. SECURITY RULES 4
3.1. Outsourced information must be identified and categorised 4
3.2. Commission Use (CU) and sensitive non-classified (SNC) information must be hosted within the European Union 4
3.3. Relevant legal requirements and conditions must be included in outsourcing contracts 4
3.4. Commission information must be isolated from other clients of the outsourcing provider 5
3.5. Authentication mechanisms and credentials must be controlled by the Commission 5
3.6. The availability of Commission information must be ensured 6
3.7. The availability of security-related logs must be ensured 6
3.8. A security incident response procedure must be in place 7
3.9. External network connections must be approved 7
3.10. Persistent encryption mechanisms must be under the control of the Commission 7
3.11. Access to Commission information by service provider staff must be minimised 8
3.12. Outsourcing must be recorded in GovIS2 8
4. VERIFICATION PROCEDURE 8
APPENDIX: OUTSOURCING CONTRACTS 9

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111

Commission européenne, 2920 Luxembourg, LUXEMBOURG - Tel. +352 43011

1. INTRODUCTION

Commission Decision (EU, Euratom) 2017/46[1] assigns the responsibility to the Directorate-General for Human Resources and Security (DG HR) to 'propose principles and rules for the outsourcing of CISs[2] in order to maintain appropriate control of security of the information[3].' This standard contains the high-level security rules that must be applied to all outsourced CISs.

This standard focuses on the risks to information that can arise from outsourcing (see chapter 2 for a more detailed definition). The rules in this document must be applied in addition to the general IT security standards that support Decision 2017/46. In particular, the risk management process and suitable countermeasures[4] must be applied to ensure that risks are mitigated and residual risks can be accepted so that the benefits of outsourcing outweigh the additional risks. This must be documented in a security plan.

The rules in this document must be applied in particular when information is stored outside the Commission, for example in a cloud service that includes online software solutions delivered as part of a broader contract for business services.

The Directorate-General for Informatics (DG DIGIT) should be used as a broker for outsourced cloud services. DG DIGIT recently published the Commission's cloud strategy[5] and has framework contracts with major cloud providers that include a high level of security controls, making it easier for system owners and data owners to comply with this standard.

Decision 2017/46 emphasises that the responsibility for a system and its security cannot be outsourced. All systems must have a system owner in the Commission, and security requirements must be followed up by the system owner or a representative within the Commission.

More information on the Commission's general and IT security policies is available on MyIntracomm[6].

2. SCOPE

Due to the variable nature and scope of outsourcing arrangements, it is necessary to define what constitutes outsourcing in the context of this procedure. The implementing rules for Article 6 of Decision 2017/46[7] define outsourcing as follows:

---

1 Hereafter "Decision 2017/46".

22 Communication and information systems.

3 Article 6(6) of Decision 2017/46.

4 See the Standard on Information Security Risk Management at https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Pages/IT-security-standards-and-guidelines.aspx

5 https://ec.europa.eu/info/sites/info/files/ec_cloud_strategy.pdf

6 See https://myintracomm.ec.europa.eu/corp/security/EN/newDS3/PolicyLegislation/Pages/default.aspx and https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Pages/IT-security-standards-and-guidelines.aspx.

'For the purposes of this Decision, a Commission CIS is considered to be outsourced when it is provided on the basis of a contract with a third party contractor, under which the CIS is housed on non-Commission premises. This includes the outsourcing of individual or multiple CISs or other IT services, data centres on non-Commission premises, and the handling of Commission data sets by external services.'

The main criterion for the definition of outsourcing is the location of the CIS's hardware infrastructure, as the legal jurisdiction where the computer systems reside is a key factor in many of the related risks and the Commission's immunity protocols do not apply to externally located systems. As a result, this document focuses on outsourcing activities where information under the responsibility of the Commission[8] is stored outside the Commission's data centres. This also implies that outsourcing will often involve external network connections that may require a separate agreement.

These rules apply to all outsourced CIS environments, including production, test and development systems and any backups. They must also be applied when Commission information is handled by an external system under a contract for services that includes the provision of an external software solution (e.g. a SaaS solution).

The Data Protection Regulation[9] applies equally to outsourced systems and system owners must implement the relevant measures, most of which are not specific to outsourced systems.

---

7 Commission Decision (EU, Euratom) 2018/559 of 6 April 2018 laying down implementing rules for Article 6 of Decision (EU, Euratom) 2017/46 on the security of communication and information systems in the European Commission, OJ L 93, 11.4.2018, p.4.

8 This includes information handled by the Commission on behalf of an external Data Owner.

9 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons 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, OJ L 295, 21.11.2018, p.39.

3. SECURITY RULES[10]

3.1. Outsourced information must be identified and categorised

The security needs of the information that a CIS handles must be determined under the responsibility of the data owner(s) in line with the guidance issued by the DG HR Security Directorate (HR.DS) under Commission Decision (EU, Euratom) 2015/443[11].

This classification must be reported in GovIS2 using the fields 'Confidentiality level', 'Integrity level' and 'Availability level'. The subsequent risk management process and security plan must include consideration of any risks relating to outsourcing or cloud services.

Systems handling information that is classified as RESTREINT UE/EU RESTRICTED or higher must not be located outside Commission premises. Whenever a new system is planned to handle this information, the system owner must contact HR.DS prior to the launch of the project for advice and to initiate the accreditation process[12].

3.2. Commission Use (CU) and sensitive non-classified (SNC) information must be hosted within the European Union

Any information that is not Publicly Available[13] must be hosted within one or more EU Member States. Commission Use and sensitive non-classified information must be protected under Article 339 of the Treaty on the Functioning of the European Union on professional secrecy, Article 17 of the Staff Regulations, and the Data Protection Regulation[14].

Outside EU Member States, these laws are not applicable, and Commission information will be subject to national legislation that might, for example, include legal rights to seize data.

3.3. Relevant legal requirements and conditions must be included in outsourcing contracts

Outsourcing providers often have standard contracts, or standard terms and conditions, which they provide to all of their customers. However, these contracts might not contain all of the

---

10 In this document, the word 'must' is used to indicate a rule that is mandatory in all circumstances. 'Should' is used to indicate a rule that is strongly recommended. Any exceptions to either type of rule should be explained in the CIS's security documentation.

11 See Security Notice C(2019) 1903 Information assessment and classification, 5.3.2019.

12 See Security Notice C(2019) 1890 Security accreditation of communication and information systems handling EUCI, 5.3.2019.

13 Publicly Available (PA), Commission Use (CU) and sensitive non-classified (SNC) are the terms defined for the different confidentiality levels of non-classified information within the Commission (see Security Notice C(2019) 1903 Information assessment and classification).

14 The European Data Protection Supervisor *"recommends that the processing of personal data entrusted by the EU institutions to Cloud Service Providers, and any sub-processing, as a rule, take place within the EU"* ('Guidelines on the use of cloud computing services by the European institutions and bodies', 16 March 2018, p. 19).

provisions that are required by the Commission or that would be needed to safeguard Commission information.

Any contract that involves the processing of Commission information outside Commission premises must include appropriate terms on the protection of information in compliance with Article 29 of Regulation 2018/1725.

The appendix of this document provides a list of relevant issues for which the Commission will provide standard clauses for inclusion in outsourcing contracts.

3.4. Commission information must be isolated from other clients of the outsourcing provider

Multi-tenant solutions are common in cloud services, usually for cost reasons. Isolation failure, whereby customers of an outsourcing provider can access information belonging to another customer, is a common cause of security breaches in cloud systems. System owners must obtain assurance from outsourcing providers on the measures that are put in place to prevent isolation failure.

Measures to protect against isolation failure must be appropriate and proportionate; for example, it is likely that the outsourcing provider's technical management infrastructure will still be shared among multiple clients.

An exception can be made for information categorised as "Publicly Available" (PA information) if the risk assessment shows that it does not need to be isolated.

3.5. Authentication mechanisms and credentials must be controlled by the Commission

Authentication checks are a significant factor in the overall security of a system, preventing unauthorised users from accessing information. In an outsourced CIS, they are even more important as the Commission cannot control who can access the network where the system resides.

Where possible, outsourced CISs must use Commission corporate identity and access management services, primarily EULogin. If this is not possible, the Commission should be responsible for defining the end users in the CIS even when using authentication mechanisms of an outsourcing provider. Access rights that are granted to staff from the provider, and the numbers of staff with such (often privileged) access, should be kept to the strict minimum (see § 3.11).

In addition, the strength of the authentication mechanism must be determined in light of the additional risks involved in an outsourced solution[15]. The use of two-factor or multi-factor authentication is highly recommended for all outsourced systems, and is required for systems that

[15] See the IT security standard on access control and authentication at https://myintracomm.ec.europa.eu/corp/digit/itsecurity/Pages/IT-security-standards-and-guidelines.aspx.

handle sensitive non-classified information. This is mandatory for privileged access to any outsourced system.

3.6. The availability of Commission information must be ensured

In outsourced CISs, the Commission relinquishes direct control of its own information and hands control to a third party. Measures must be in place to mitigate the ensuing risks, in line with the business continuity requirements relating to the CIS.

Above all, the Commission must avoid situations where a third party is solely in charge of Commission information. The main risks are the unavailability of information and vendor lock-in.

As a result, measures must be in place to ensure that business-critical information is available from another source. One solution, for example, could be to make a regular backup of the information, stored at the Commission or with another cloud provider[16] (e.g. an external data escrow service). The most appropriate solution should be implemented to fulfil the business and security needs based on the identification of the information whose availability needs to be guaranteed.

3.7. The availability of security-related logs must be ensured

The existence of security (audit) logs is an important security control. To ensure their availability and to prevent unauthorised manipulation of log records, the critical security-related logs must be identified and should be stored by a service that is not under the control of the outsourcing provider. This service should preferably be hosted inside dedicated infrastructure that is exclusively controlled by the Commission to ensure that no third party can access, alter or delete the logs.

As CISs can generate large volumes of log entries and it may be impractical to make a separate copy of all of them, it is important to identify those that are significant for auditing or incident response purposes. These may include records of events such as:

- user login attempts;
- changes to system, environmental or network configuration;
- updates of critical business information;
- significant transactions (e.g. financial payments);
- log file management;
- hardware identification information.

Where necessary, security alerts should be defined and sent to the Commission in real time when a potential breach of security is detected (e.g. multiple failed login attempts within a short timeframe).

[16] Most cloud service level agreements stipulate that the responsibility for backups lies with the customer.

3.8. A security incident response procedure must be in place

The Commission must be aware of any security incidents that occur in the outsourced service and must be capable of investigating them, with assistance from the outsourcing provider where necessary. The following measures should be in place in addition to the measures laid down in Decision 2017/46 and its implementing rules:

- the appropriate incident response procedure must be included or referred to in the contract;
- security points of contact must be identified at the outsourcing provider and at the Commission;
- the outsourcing provider must commit to reporting security incidents that affect Commission information to the Commission as soon as they are detected;
- IT security incidents must be reported to the DIGIT Computer Security Incident Response Capability (EC DIGIT CSIRC) for investigation;
- in addition to the normal reporting to the LISO, the Commission's security point of contact must report any security incident to the Local Security Officer (LSO) of the department concerned, and the LSO must report any serious incidents to HR.DS, in particular any incident that involves information leaks[17];
- the investigators in HR.DS must have access to the log files and all other relevant information when investigating security incidents.

3.9. External network connections must be approved

Outsourced systems will usually need to communicate with the Commission's internal network. This connection may be established through the Commission's standard internet communications infrastructure or through different connections, such as a dedicated connection to the outsourcing provider.

In the latter case, the external network connection(s) must be approved by HR.DS, with the establishment of a security convention that is a multi-party agreement between HR.DS, DIGIT, the system owner and the external provider.

3.10. Persistent encryption mechanisms must be under the control of the Commission

The use of encryption is recommended for outsourced CISs, in particular for sensitive non-classified information. Encryption helps to mitigate the risks of exposure of information outside the Commission's internal environment. Outsourcing providers often offer encryption services, but care must be taken when procuring and configuring such services to ensure that the Commission has final control over the encryption mechanisms[18].

In particular, system owners are advised to make use of encryption mechanisms that are generated and managed by the Commission, such as encryption certificates for secure email.

---

[17] Any leaks involving personal data must be reported immediately to the data protection coordinator.

[18] For example, information is provided on the encryption algorithms or protocols so that the Commission can determine whether they are adequate, and the Commission has control of all keys used to protect Commission information.

When information is persistent (i.e. not just held temporarily during processing) and is encrypted at rest, key escrow procedures must be available.

Any non-standard use of encryption in Commission CISs is subject to the approval of the Crypto Approval Authority, which falls under the responsibility of HR.DS. For further information, see the *Standard on Cryptography and Public Key Infrastructure*[19].

The use of encrypted communication protocols is also strongly recommended for all non-persistent communications.

3.11. Access to Commission information by service provider staff must be minimised

Outsourcing providers will inevitably have some level of access to any Commission CIS and its information, as they have physical access to the hardware. In general, they will also have administrative access at some levels of the IT systems, depending on the outsourcing model. However, the extent of this access must be minimised as far as possible to reduce the risks relating to external personnel with administrator-level access to Commission information, and their actions in the system must be logged (see § 3.7).

This also relates to other security measures such as the level of assurance given by the outsourcing provider with regard to its internal human resources controls.

This must be documented in the service contract.

3.12. Outsourcing must be recorded in GovIS2

If outsourcing is used as part of the infrastructure, this must be recorded in GovIS2, using 'Outside EC' as the value for 'Hosting mode' field (or 'Mixed' where a part of the system resides on Commission premises). The relevant project documentation must be attached (or referred to) in GovIS2.

4. VERIFICATION PROCEDURE

HR.DS will verify that these rules have been implemented. At least once a year, HR.DS will select a sample of outsourced systems and check whether the measures have been implemented adequately. HR.DS will determine the size of the sample.

The results of the verification procedure will be reported to the ITCB if significant risks are identified.

[19] See https://myintracomm.ec.europa.eu/corp/security/EN/newDS3/PolicyLegislation/Pages/security-rules.aspx

APPENDIX: OUTSOURCING CONTRACTS

Contracts should contain all of the provisions that the Commission needs. Some cloud service providers may be reluctant to customise services to specific needs, in particular if providers rely on subcontracted services. This issue is magnified in cloud computing with respect to traditional hosting or housing because of standardisation, different service models and changes in technology.

Third parties are not subject to the Commission's internal legislation, including its decisions on security. As a result, all security requirements must be established in contracts. It is not necessary to require contractors to follow the Commission's security policy if they have suitable and equivalent or stronger policies in place, but the points below and any other specific security requirements should be detailed in outsourcing contracts.

Security requirements must be included in all relevant contracts, including the contracts for the provision of systems, as well as contracts for related services such as support, development and business processes related to the outsourced CIS.

Commission departments should ensure that they have the necessary means to guarantee that a service provider fulfils their requirements. The following issues should be considered when drawing up outsourcing contracts:

- There must be restrictions on where the outsourced systems are physically located (e.g. only in EU Member States), including any information stored in other locations such as backups. Similarly, the legal jurisdiction of the contract must be within the EU and must comply with the Commission's rules on third party contracts.

- Providers must inform the Commission of any relocation of hardware to different premises.

- Providers must notify the Commission if they receive requests for data seizure from national authorities (e.g. law enforcement) or other third parties. The Commission must be involved as much as possible in responding to such requests in line with the relevant national legislation.

- Providers may be required to follow well-known standards or obtain relevant certification, e.g. for IT security or cloud computing security.

- Service Level Agreements should include relevant security requirements and reporting. Penalties for non-compliances, including security breaches, are a significant motivator for contractors to carry out the agreed measures.

- Essential security logging activities should be defined, including their retention period (see rule 7, 'The availability of security-related logs must be ensured').

- Data restoration in the event of an outage should be in line with the Commission's business continuity needs.

- The contract should specify whether and under what conditions the Commission or the contractor is permitted to perform penetration tests or vulnerability scans.

- 'Right to audit' clauses: service providers' claims regarding security and compliance should be validated in a formal, independent way to give confidence to those claims.

- Clauses related to incident handling, e.g. obligation to report incidents (including cases of isolation failure) and to provide access to relevant information in case of investigation, in particular formal investigations by DG HR.

- Right to terminate the contract without penalties in the event of major or persistent security issues.

- Handling of data at the end of the contract, i.e. how the Commission recovers its data, and how and when the contractor (securely) deletes any Commission data. Data escrow services may be considered as part of the contract.

- Bankruptcy of a cloud provider may mean that Commission data may be left on defunct servers and prove difficult to recuperate. It is advisable to include a provision in the contract that enables immediate access to data upon bankruptcy or other causes of force majeure.

- The extent of subcontracting permissible under the contract and the security responsibilities of subcontractors should be covered. Transfers of Commission data to third party must be excluded.

- Contractor staff with access to Commission systems may be required to sign a non-disclosure agreement or undergo a security background check as required because of the sensitivity of the information handled.

- Responsibilities for the protection of personal data, in particular with regard to their handling by contractors as data processors, and the necessary conditions for such processing, in accordance with the conditions and requirements set out under Article 29 of Regulation (EU) 2018/1725.