**Appendix – Security Clauses for Clients, Suppliers and Partners**

# Security Clauses for Cloud Services’ Clients

## Clauses for general cloud service provision

When drawing up an agreement as a Cloud Service Provider, it must be defined which of the following clauses will be included in the agreement with the client (the legal wording of the agreement must be prepared by the person responsible for legal matters):

1. details about the service provided
2. authorization for the organization to hire subcontractors to work on the cloud service customer’s environment, including a description of controls that must be fulfilled by subcontractors
3. the definition of the organization’s point of contact (person or department to act as the focal point of communication between the organization and the cloud service customer) regarding the cloud services provided under the contract
4. the identification of the cloud service customer’s point of contact with the organization’s customer support and care function, regarding cloud services provided by the organization under the contract
5. the allocation of information security roles and responsibilities between the organization (as the Cloud Service Provider), its suppliers involved in the cloud service provisioning, and the cloud service customer, concerning the fulfillment of information security implementation and provisioning
6. list of relevant authorities, identified by the cloud service customer, to be contacted concerning the operations between the cloud service customer and the organization (as the Cloud Service Provider)
7. the identification of the geographical locations of the organization (as the Cloud Service Provider) and the countries where it can store, process or transmit the Cloud Service Customer’s data. This information must also include those of suppliers and sub-contractors involved in the cloud service provision
8. information about legal requirements the organization (as the Cloud Service Provider), and its suppliers and sub-contractors involved in the cloud service provision, must comply with and that are relevant to the cloud service customer
9. the process for notifying the cloud service customer, in a timely fashion, about:
   * any intended changes that can impact the cloud service operations or data security
   * any technical vulnerability that can affect the cloud services provided, especially those for which the cloud service customer is responsible for handling
   * information security incidents related to the cloud service customer’s data
10. information, in a way that does not disclose information that can be improperly used, about:
    * the legal jurisdiction applicable to the organization’s cloud services under the contract
    * the organization’s secure development controls applied to its cloud environments
    * controls applied to protect records related to the use of cloud services by the cloud service customer
    * arrangements for the disposal and reuse of resources
    * arrangements for the return and removal of any cloud service customer’s assets when necessary, including a list of assets to be returned and removed
    * the use of cryptographic solutions and utility programs in the cloud environment – which ones are used, requirements for using them, and controls to ensure they cannot affect normal operations or breach the security controls of the cloud service
    * specifications of the organization’s backup capabilities
    * time reference used by the cloud systems, and how the cloud service customer can synchronize local clocks with the cloud service time reference
    * incident handling capabilities (e.g.: incident response time, escalation process, etc.) including procedures to respond to requests for digital evidence or other information from within the cloud computing environment
11. information about cloud service functionalities, in a way that do not disclose information that can be improperly used, that are available to the cloud service customer and allow it to:
    * classify and label its information and associated assets
    * manage its users’ access
    * manage access to services, functionalities, and data
    * apply cryptographic protections
    * log events
    * report information security incidents
12. the information, including format and periodicity, that will be available to the cloud service customer to:
    * monitor the use of cloud services and resource capacity
    * verify the organization’s (as the Service Provider) conformity regarding the implementation of legal and contractual requirements, as well as of the proper operation of information security controls
13. use of non-disclosure agreements with those who may have access to detailed information about security controls related to the cloud service to be provided

Note: It should be observed that the cloud service customer may have its own clauses to be included in the agreement. For more information about possible clauses to be included in the service agreement, the cloud service customer should be consulted.

## Clauses for cloud service provision as a PII processor

When drawing up an agreement as a Personally Identifiable Information (PII) cloud processor, besides the clauses suggested in section 1 of this guideline, it must be defined which of the following clauses will be included in the agreement (the legal wording of the agreement must be prepared by the person responsible for legal matters):

1. details about the PII cloud processing service – which kinds of PII will be processed, which cloud model will be used, available technologies, service level agreements and reliability, etc.
2. the allocation of information security roles and responsibilities between the organization (as the Cloud PII Processor), its sub-contractors, and the cloud service customer, concerning the fulfillment of PII protection
3. mechanisms to independently ensure that PII processing is done in conformance with legal and contractual requirements, as well as that the information security controls are implemented and operated in accordance with defined requirements
4. the definition of the organization’s point of contact (person or department to act as focal point of communication between the organization and the cloud service customer) regarding the processing of Personally Identifiable Information (PII) under the contract
5. mechanisms to provide secure log-on procedures as requested by the cloud service customer
6. information, in a way that does not disclose information that can be improperly used, about:
   * cryptographic solutions applied to protect the PII it processes
   * controls to protect PII used for testing purposes
   * controls to protect PII stored and in transit
   * specifications of its backup capabilities, including the generation of log of data restoration efforts
   * arrangements for the disposal and reuse of resources that may store PII data
   * arrangements for the return and removal of any cloud service customer’s PII upon the termination of the cloud service use agreement, including a list of PII to be returned and removed
   * controls applied to protect data logs gathered and stored related to the processing and use of the cloud service customer’s PII
   * incident handling capabilities (e.g.: incident response time, escalation process, etc.)
7. information about the PII cloud processor’s functionalities that are available to the cloud service customer:
   * manage its users access
   * manage its PII data
   * apply cloud service customer’s own cryptographic protections
   * backup and restore data
   * access and use of data logs regarding the cloud service customer’s PII processing
8. the assurance to:
   * not process PII for any other purposes other than those specified by the cloud service customer
   * not use cloud service customer’s PII for marketing or advertisement purposes without express consent
   * reject any request for disclosure of cloud service customer’s PII, unless those legally bound or authorized by the cloud service customer (consider the use of non- disclosure agreements)
   * notify the cloud service customer about any request to disclose its PII, except those requests for which by law the notification is prohibited
   * notify information security incidents related to the cloud service customer’s PII data
9. the identification of the geographical locations of the organization (as cloud PII provider) and the countries where it can store, process, or transmit the PII data. This information must also include those of suppliers and sub-contractors involved in the cloud service provision

Note: It should be observed that the cloud service customer may have its own clauses to be included in the agreement. For more information about possible clauses to be included in the service agreement, the cloud service customer should be consulted.

# Security Clauses for Suppliers and Partners

When drawing up an agreement with a supplier or partner, it must be defined which of the following clauses will be included in the agreement (The legal wording of the agreement must be prepared by the person responsible for legal matters.):

1. details about the service provided, specifying information to be made available for this purpose and how the information is classified
2. whether the supplier has the right to hire subcontractors; if yes, then written consent must be obtained from the organization, with a description of controls that must be fulfilled by subcontractors
3. a definition of classified information and how trade secrets are regulated
4. the duration of the agreement and of the obligation to keep confidential and classified information/trade secrets after agreement expiration (when writing this Article, it must be considered how business continuity will be ensured in the organization)
5. the right of the organization to access information stored or processed by the supplier/partner
6. the right to audit or monitor the use of confidential information and to monitor agreement execution at the supplier's/partner's facility, and whether the audits may be carried out by third parties; specify the rights of auditors
7. actions required after agreement expiration (return, destruction or erasure of confidential information, return of equipment, etc.) to ensure the protection of confidential information and to ensure business continuity in the organization
8. identification and use of key controls to ensure the protection of organizational assets – e.g. physical controls, controls for protection against malicious code, physical protection controls, controls to protect integrity, availability and confidentiality of information, controls to ensure the return or destruction of information assets after their use, controls to prevent copying and distributing information
9. ensuring access to financial reports, to reports by internal and external auditors, and to other reports related to business operations of suppliers/partners, which could be relevant for the organization
10. responsibilities and actions of the parties to the agreement in order to prevent access to the agreement by unauthorized people (e.g. only persons with the need to know may have access rights to information, etc.)
11. identifying the owner of information and how intellectual property rights are regulated
12. permitted use of classified information, i.e. prescribed method for handling such information
13. process for notifying the other party to the agreement of unauthorized access to information, confidentiality breaches or of any other incident
14. defining the incident response time, and establishing an escalation process for problem and incident resolution
15. actions ensuing from breach of agreement; responsibility of the supplier/partner for unperformed, untimely or incorrect transactions and other contracted activities
16. supplier's/partner's knowledge of the organization's key security policies and procedures
17. obligation to train employees of the supplier/partner in all activities in which they are involved
18. ensuring that suppliers/partners are aware of the need for security
19. forbidding that employees of the organization transfer to suppliers/partners
20. target service level and unacceptable service level
21. definition of service performance criteria, their monitoring and reporting
22. a precise definition of the reporting system and reporting format
23. a precisely specified change management process
24. access control system – define reasons for third-party access rights, permitted log-in and password process, authorization process for individual user access and allocation of privileges, obligation to maintain a record of all users and their access rights, process for removing access rights
25. a clause clearly stating that all access rights that are not explicitly authorized are forbidden
26. the right to monitor and revoke any activity related to the organization's assets
27. controls to ensure business continuity, in accordance with the organization's priorities – which services need to recover within which deadline
28. responsibility for damage in case of breach of contractual relations, including material liability in case of breach of confidentiality of information or in case of non-performance of services
29. responsibility of the supplier/partner to store data in accordance with regulations
30. conditions for agreement extension or termination
31. the language of the agreement and of the future communication between the organization and suppliers/partners
32. access to information related to resource usage made by the organization itself or by its cloud service customers (e.g.: number of processor cores for application, storage capacity available, network bandwidth available), during particular periods and usage peaks
33. availability of independent evidence that the supplier’s or partners’ information security is implemented and operated according to the objectives required by the organization and its cloud service customers, including security objectives for the protection of Personally Identifiable Information (PII)
34. availability of evidence that the supplier’s or partners’ supply chain can maintain or exceed the information security levels defined by [organization name] and by its cloud service customers
35. controls to ensure the protection of records created or gathered related to the use of cloud services by the organization’s cloud service customer.