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

Commented [EU GDPR1]: To learn how to select the security clauses, read these articles:

- 6-step process for handling supplier security according to ISO 27001 https://advisera.com/27001academy/blog/2014/06/30/6-step-process-for-handling-supplier-security-according-to-iso-27001/
- Which security clauses to use for supplier agreements? https://advisera.com/27001academy/blog/2017/06/19/which-security-clauses-to-use-for-supplier-agreements/

23. a precisely specified change management process
24. [illegible]
25. [illegible]
26. [illegible]
27. [illegible]
28. [illegible]
29. responsibility of the supplier/partner to store data in accordance with regulations
30. conditions for agreement extension or termination
31. [illegible]