**CHECKLIST OUTSOURCING CONTRACTS**

This checklist sets out the requirements for outsourcing contracts pursuant to the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02). Any reference to ‘institutions’ refers to credit institutions and investment firms subject to Directive 2013/36/EU (CRD IV) and any reference to ‘payment institutions’ refer to payment institutions and electronic money institutions.

**N.B.: This checklist provides an overview of the most important clauses for outsourcing contracts pursuant to the EBA Guidelines on outsourcing arrangements, but does not purport to provide a complete overview of all relevant clauses. A check by a lawyer is always required.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Requirement** | **Included in the contract (yes/no)?** | **Where included** | **Comments** |
| **General requirements** |
| 1. | A clear description of the outsourced function to be provided. |  |  |  |
| 2. | The start date and end date, where applicable, of the agreement and the notice periods for the service provider and the (payment) institution. |  |  |  |
| 3. | The governing law of the contract. |  |  |  |
| 4. | A clear description of the parties' financial obligations. |  |  |  |
| 5. | Where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of the relevant data. |  |  |  |
| 6. | The right of the (payment) institution to monitor the service provider’s performance on an ongoing basis. |  |  |  |
| 7. | The agreed service levels, which must include precise quantitative and qualitative performance targets for the outsourced functions. |  |  |  |
| 8. | The reporting obligations of the service provider to the (payment) institution. |  |  |  |
| 9. | Whether the service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested. |  |  |  |
| 10. | The requirements to implement and test business contingency plans. |  |  |  |
| 11. | Provisions that ensure that the data that are owned by the (payment) institution can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the service provider. |  |  |  |
| 12. | The obligation of the service provider to cooperate with the competent authorities and resolution authorities of the (payment) institution, including other persons appointed by them. |  |  |  |
| 13. | For institutions, a clear reference to the national resolution authority’s powers, especially to Articles 68 and 71 of Directive 2014/59/EU (BRRD), and in particular a description of the ‘substantive obligations’ of the contract in the sense of Article 68 of that Directive. |  |  |  |
| 14. | The unrestricted right of (payment) institutions and competent authorities to inspect and audit the service provider with regard to, in particular, the critical or important outsourced function, including a contractual right of access and audit to the (payment) institution and its competent authorities. |  |  |  |
| 15. | Termination rights, which should apply at least in the following situations: |  |  |  |
| 15a. | where the service provider is in a breach of applicable law, regulations or contractual provisions; |  |  |  |
| 15b. | where impediments capable of altering the performance of the outsourced function are identified; |  |  |  |
| 15c. | where there are material changes affecting the outsourcing arrangement or the service provider (e.g. sub-outsourcing or changes of sub-contractors); |  |  |  |
| 15d. | where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information; and |  |  |  |
| 15e. | where instructions are given by the (payment) institution's competent authority, e.g. in the case that the competent authority is, caused by the outsourcing arrangement, no longer in a position to effectively supervise the (payment) institution. |  |  |  |
| 16. | Arrangements for the transfer of the outsourced function to another service provider or its re-incorporation into the (payment) institutions, including: |  |  |  |
| 16a. | the obligations of the existing service provider, in the case of a transfer of the outsourced function to another service provider or back to the (payment) institution, including the treatment of data; |  |  |  |
| 16b. | the obligations of the existing service provider, in the case of a transfer of the outsourced function to another service provider or back to the (payment) institution, including the treatment of data; |  |  |  |
| 16c. | an obligation of the service provider to support the (payment) institution in the orderly transfer of the function in the event of the termination of the outsourcing agreement. |  |  |  |
| 17. | The obligation for service providers, where relevant, to comply with appropriate IT data and system security standards. |  |  |  |
| 18.  | The obligation that the service provider protects confidential, personal or otherwise sensitive information and complies with all legal requirements regarding the protection of data that apply to the (payment) institution. |  |  |  |
| 19.  | The right of the internal audit function to review the outsourced function using a risk-based approach. |  |  |  |
| 20. | With respect to service providers located in a Member State: a reference to the information gathering and investigatory powers of competent authorities and resolution authorities under Article 63(1)(a) of Directive 2014/59/EU (BRRD) and Article 65(3) of Directive 2013/36/EU (CRD IV). If the service provider is located in a third country, these rights should also apply. |  |  |  |
| 21. | The ability of the institution to carry out security penetration testing to assess the effectiveness of implemented cyber and internal ICT security measures and procedures. |  |  |  |
| **For critical or important functions - GENERAL** |
| 22. | Whether sub-outsourcing is permitted and, if so, under which conditions. Any types of activities that are excluded from sub-outsourcing should be specified. |  |  |  |
| 23. | The location(s) (i.e. regions or countries) where the services will be provided and/ or where relevant data will be kept and processed, and the conditions to be met, including a requirement to notify the (payment) institution if the locations are changed. |  |  |  |
| 24. | The unrestricted right of the (payment) institution and competent authorities to inspect and audit the service provider with regard to the critical or important outsourced function, including full access to all relevant business premises (e.g. head offices and operation centres), the full range of relevant devices systems, networks, information and data used for providing the outsourced function and related financial information, personnel and the service provider’s external auditors. |  |  |  |
| 25. | The obligation of the service provider to comply with all applicable laws, regulatory requirements and contractual obligations. |  |  |  |
| **For critical or important functions - IN CASE SUB-OUTSOURCING IS PERMITTED** |
| 26. | A specification that the service provider is obliged to oversee those services that it has sub-contracted to ensure that all contractual obligations between the service provider and the (payment) institution are continuously met. |  |  |  |
| 27. | The requirement for the service provider the service provider to obtain prior specific or general written authorisation from the (payment) institution before sub-outsourcing data. |  |  |  |
| 28. | An obligation of the service provider to inform the (payment) institution of any planned sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. The notification period should allow the outsourcing (payment) institution to carry out a risk assessment of the proposed changes and to object to changes before the planned sub-outsourcing, or material changes thereof, come into effect. |  |  |  |
| 29. | The right of the (payment) institution to object to intended sub-outsourcing, or material changes thereof, or that explicit approval is required. |  |  |  |
| 30. | The right to terminate the agreement in the case of undue sub-outsourcing, e.g. where the sub-outsourcing materially increases the risks for the (payment) institution or where the service provider sub-outsources without notifying the (payment) institution. |  |  |  |
| 31. | The undertaking of the sub-contactor to comply with all applicable laws, regulatory requirements and contractual obligations. |  |  |  |
| 32. | The granting of the same contractual rights of access and audit to the (payment) institution and competent authority as those granted by the service provider. |  |  |  |
| 33. | The obligation of the service provider to appropriately oversee the sub-service providers, In line with the policy defined by the (payment) institution |  |  |  |