**CHECKLIST IT AND OUTSOURCING CONTRACTS**

This checklist sets out the requirements for outsourcing contracts pursuant to the [EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)](https://extranet.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1). It also includes the key contractual provisions that must be included in ICT contracts with ICT third-party service providers pursuant to Article 28(7) and 30 of the Digital Operational Resilience Act (“**DORA**”), regardless of whether or not the ICT contract concerns outsourcing. and for IT contracts pursuant to the [Digital Operational Resilience Act](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554) (“**DORA**”). Any reference to ‘**institutions**’ refers to credit institutions and investment firms subject to [Directive 2013/36/EU (CRD IV)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0036), any reference to ‘**payment institutions**’ refer to payment institutions and electronic money institutions and any reference to ‘**financial entity**’ refers to all EU supervised financial institutions which are subject to DORA pursuant to Article 2(1) thereof.

**N.B.: This checklist provides an overview of the most important clauses (i) for outsourcing contracts pursuant to the EBA Guidelines on outsourcing arrangements and (ii) for ICT contracts pursuant to DORA, 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** |
| **EBA outsourcing guidelines - 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. | an appropriate transition period, during which the service provider, after the termination of the outsourcing agreement, would continue to provide the outsourced function to reduce the risk of disruptions; |  |  |  |
| 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. |  |  |  |
| **EBA outsourcing guidelines - For critical or important functions - GENERAL** |
| **NOTE:** Section 4 of the EBA outsourcing guidelines set out when a function is considered critical or important. Institutions should always consider a function as critical or important in the following situations:1. where a defect or failure in its performance would materially impair:
	1. the (payment) institution’s continuing compliance with the conditions of its authorisation or its other obligations under Directive 2013/36/EU (CRD IV), Regulation (EU) No 575/2013 (CRR), Directive 2014/65/EU (MiFID II), Directive (EU) 2015/2366 (PSD2) and Directive 2009/110/EC (EMD 2) and its regulatory obligations;
	2. its financial performance; or
	3. the soundness or continuity of its banking and payment services and activities.
2. when operational tasks of internal control functions are outsourced, unless the assessment establishes that a failure to provide the outsourced function or the inappropriate provision of the outsourced function would not have an adverse impact on the effectiveness of the internal control function;
3. when the (payment) institutions intends to outsource functions of banking activities or payment services to an extent that would require authorisation by a competent authority.
 |
| 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. |  |  |  |
| **EBA outsourcing guidelines - 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 |  |  |  |
| **DORA – General requirements for ICT contracts with ICT third-party service providers** |
| **NOTE**: These requirements apply to all contractual arrangements on the use of ICT services with ICT third-party service providers, regardless of whether the contractual arrangements constitute outsourcing. ‘**ICT services**’ is broadly defined as: *“digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services”* |
| 34. | A clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider, indicating whether subcontracting of an ICT service supporting a critical or important function, or material parts thereof, is permitted and, when that is the case, the conditions applying to such subcontracting. |  |  |  |
| 35. | The locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed, including the storage location, and the requirement for the ICT third-party service provider to notify the financial entity in advance if it envisages changing such locations. |  |  |  |
| 36.  | Provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data. |  |  |  |
| 37. | Provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the financial entity in the event of the insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider, or in the event of the termination of the contractual arrangements. |  |  |  |
| 38. | Service level descriptions, including updates and revisions thereof. |  |  |  |
| 39. | The obligation of the ICT third-party service provider to provide assistance to the financial entity at no additional cost, or at a cost that is determined ex-ante, when an ICT incident that is related to the ICT service provided to the financial entity occurs. |  |  |  |
| 40. | The obligation of the ICT third-party service provider to fully cooperate with the competent authorities and the resolution authorities of the financial entity, including persons appointed by them. |  |  |  |
| 41. | Termination rights and related minimum notice periods for the termination of the contractual arrangements, in accordance with the expectations of competent authorities and resolution authorities. |  |  |  |
| 42. | The conditions for the participation of ICT third-party service providers in the financial entities’ ICT security awareness programmes and digital operational resilience training in accordance with Article 13(6) DORA. |  |  |  |
| 43. | Termination rights in the following circumstances: |  |  |  |
| 43a. | significant breach by the ICT third-party service provider of applicable laws, regulations or contractual terms; |  |  |  |
| 43b. | circumstances identified throughout the monitoring of ICT third-party risk that are deemed capable of altering the performance of the functions provided through the contractual arrangement, including material changes that affect the arrangement or the situation of the ICT third-party service provider; |  |  |  |
| 43c. | ICT third-party service provider’s evidenced weaknesses pertaining to its overall ICT risk management and in particular in the way it ensures the availability, authenticity, integrity and, confidentiality, of data, whether personal or otherwise sensitive data, or non-personal data; |  |  |  |
| 43d. | where the competent authority can no longer effectively supervise the financial entity as a result of the conditions of, or circumstances related to, the respective contractual arrangement. |  |  |  |
| **DORA – General requirements for ICT services supporting critical or important functions** |
| **NOTE:** a ‘**critical or important function**’ has been defined in Article 3(22) DORA as: *“a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law”.* |
| 44. | full service level descriptions, including updates and revisions thereof with precise quantitative and qualitative performance targets within the agreed service levels to allow effective monitoring by the financial entity of ICT services and enable appropriate corrective actions to be taken, without undue delay, when agreed service levels are not met. |  |  |  |
| 45. | Notice periods and reporting obligations of the ICT third-party service provider to the financial entity, including notification of any development that might have a material impact on the ICT third-party service provider’s ability to effectively provide the ICT services supporting critical or important functions in line with agreed service levels. |  |  |  |
| 46. | Requirements for the ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies that provide an appropriate level of security for the provision of services by the financial entity in line with its regulatory framework. |  |  |  |
| 47. | The obligation of the ICT third-party service provider to participate and fully cooperate in the financial entity’s threat-led penetration testing (TLPT) as referred to in Articles 26 and 27 DORA. |  |  |  |
| **NOTE:** By way of derogation from point 47 above, the ICT third-party service provider and the financial entity that is a microenterprise may agree that the financial entity’s rights of access, inspection and audit can be delegated to an independent third party, appointed by the ICT third-party service provider, and that the financial entity is able to request information and assurance on the ICT third-party service provider’s performance from the third party at any time.A ‘**microenterprise**’ has been defined as: *“a financial entity, other than a trading venue, a central counterparty, a trade repository or a central securities depository, which employs fewer than 10 persons and has an annual turnover and/or annual balance sheet total that does not exceed EUR 2 million*.” |
| 48. | The right to monitor, on an ongoing basis, the ICT third-party service provider’s performance, which entails the following: |  |  |  |
| 48a. | unrestricted rights of access, inspection and audit by the financial entity, or an appointed third party, and by the competent authority, and the right to take copies of relevant documentation on-site if they are critical to the operations of the ICT third-party service provider, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies; |  |  |  |
| 48b. | the right to agree on alternative assurance levels if other clients’ rights are affected; |  |  |  |
| 48c. | the obligation of the ICT third-party service provider to fully cooperate during the onsite inspections and audits performed by the competent authorities, the Lead Overseer, financial entity or an appointed third party; and |  |  |  |
| 48d. | the obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits; |  |  |  |
| 49. | exit strategies, in particular the establishment of a mandatory adequate transition period: |  |  |  |
| 49a. | during which the ICT third-party service provider will continue providing the respective functions, or ICT services, with a view to reducing the risk of disruption at the financial entity or to ensure its effective resolution and restructuring; |  |  |  |
| 49b. | allowing the financial entity to migrate to another ICT third-party service provider or change to in-house solutions consistent with the complexity of the service provided. |  |  |  |