**CHECKLIST IT- EN UITBESTEDINGSCONTRACTEN**

Deze checklist geeft een overzicht van de verplichtingen die er vanuit de [EBA Richtsnoeren inzake uitbesteding (EBA/GL/2019/02)](https://www.eba.europa.eu/documents/10180/2761380/d10cc21f-82cc-48fe-ab8a-7c05e9e88ccd/EBA%20revised%20Guidelines%20on%20outsourcing_NL.pdf) aan uitbestedingscontracten worden gesteld. Er staan ook belangrijke contactuele bepalingen in die in ICT contracten met ICT-dienstverleners moeten zijn opgenomen overeenkomstig artikel 28(7) en 30 van de [Digital Operational Resilience Act](https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32022R2554) (“**DORA**”). Een verwijzing naar ‘**instellingen**’ verwijst naar kredietinstellingen en beleggingsondernemingen in de zin van [Richtlijn 2013/36/EU (CRD IV)](https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32013L0036), een verwijzing naar ‘**betaalinstellingen**’ verwijst naar betaalinstellingen en elektronischgeldinstellingen en een verwijzing naar ‘**financiële entiteit**’ verwijst naar alle EU gereguleerde financiële instellingen die onderworpen zijn aan DORA overeenkomstig artikel 2 lid 1 daarvan.

**N.B.: Deze checklist geeft een overzicht van de belangrijkste bepalingen voor (i) uitbestedingscontracten volgens de EBA Richtsnoeren inzake uitbesteding en (ii) ICT contracten volgens DORA, maar beoogt geen volledig overzicht** **van alle relevante bepalingen te geven. Er zal altijd een controle door een jurist moeten plaatsvinden.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Item** | **Verplichting** | **Opgenomen in het contract (ja/nee)?** | **Waar opgenomen** | **Commentaar** |
| **EBA Richtsnoeren inzake uitbesteding - Algemene verplichtingen** | | | | |
| 1. | Een heldere beschrijving van de te verrichten uitbestede functie. |  |  |  |
| 2. | De aanvangsdatum en einddatum, indien van toepassing, van de overeenkomst en de opzeggingstermijnen voor de dienstverlener en de (betaal)instelling. |  |  |  |
| 3. | Het toepasselijke recht. |  |  |  |
| 4. | Een duidelijke beschrijving van de financiële verplichtingen van de partijen. |  |  |  |
| 5. | Waar relevant, bepalingen inzake de toegankelijkheid, beschikbaarheid, integriteit, privacy en veiligheid van de betrokken gegevens. |  |  |  |
| 6. | Het recht van de (betaal)instelling om de prestaties van de dienstverlener doorlopend te bewaken. |  |  |  |
| 7. | De overeengekomen niveaus van dienstverlening (service levels), die nauwkeurige kwantitatieve en kwalitatieve prestatiedoelen voor de uitbestede functie omvatten. |  |  |  |
| 8. | De rapportageverplichtingen van de dienstverlener aan de (betaal)instelling. |  |  |  |
| 9. | Of de dienstverlener zich verplicht tegen bepaalde risico's dient te verzekeren en, indien van toepassing, de vereiste hoogte van de verzekeringsdekking. |  |  |  |
| 10. | De verplichting om bedrijfsnoodplannen ten uitvoer te leggen en te testen. |  |  |  |
| 11. | Bepalingen die ervoor zorgen dat toegang kan worden verkregen in de gegevens die het eigendom van de (betaal)instelling zijn, wanneer de dienstverlener insolvent is, zich in een afwikkelingsproces bevindt of zijn bedrijfsactiviteiten beëindigt. |  |  |  |
| 12. | De verplichting van de dienstverlener om met de toezichthouders en afwikkelingsautoriteiten van de (betaal)instelling samen te werken, met inbegrip van andere personen die door hen zijn aangewezen. |  |  |  |
| 13. | Voor instellingen een duidelijke verwijzing naar de bevoegdheden van de nationale afwikkelingsautoriteit, vooral naar de artikelen 68 en 71 van Richtlijn 2014/59/EU (BRRD), en met name een beschrijving van de “materiële verplichtingen” van het contract in de zin van artikel 68 van die richtlijn. |  |  |  |
| 14. | Het onbeperkte recht van (betaal)instellingen en toezichthouders om de dienstverlener te inspecteren en te controleren, vooral als het gaat om kritieke of belangrijke uitbestede functies, inclusief contractuele toegangs- en auditrechten aan de (betaal)instelling en haar toezichthouders. |  |  |  |
| 15. | Beëindigingsrechten, die tenminste van toepassing moeten zijn in de volgende situaties: |  |  |  |
| 15a. | wanneer de dienstverlener de geldende wet- en regelgeving of contractuele bepalingen overtreedt; |  |  |  |
| 15b. | wanneer er belemmeringen worden geconstateerd waardoor het mogelijk is dat er veranderingen in de uitvoering van de uitbestede functie optreden; |  |  |  |
| 15c. | wanneer er sprake is van materiële wijzigingen die gevolgen hebben voor de uitbestedingsregeling of de dienstverlener (bijv. onderuitbesteding of wijzigingen van onderaannemers); |  |  |  |
| 15d. | wanneer er zwakke punten zijn als het gaat om het beheer en de beveiliging van vertrouwelijke, persoonlijke of anderszins gevoelige gegevens of informatie; en |  |  |  |
| 15e. | wanneer de toezichthouder van de (betaal)instelling instructies geeft, bijvoorbeeld als de toezichthouder als gevolg van de uitbestedingsregeling niet langer in een positie is om doeltreffend toezicht op de (betaal)instelling te houden. |  |  |  |
| 16. | Een regeling van de overdracht van de uitbestede functie aan een andere dienstverlener of het opnieuw onderbrengen ervan bij de (betaal)instelling, inclusief: |  |  |  |
| 16a. | een heldere omschrijving van de verplichtingen van de bestaande dienstverlener, in het geval van een overdracht van de uitbestede functie aan een andere dienstverlener of weer terug aan de (betaal)instelling, inclusief de behandeling van gegevens; |  |  |  |
| 16b. | een passende overgangsperiode waarin de dienstverlener, na de beëindiging van de uitbestedingsregeling, de uitbestede functie blijft verrichten om het risico op verstoringen te beperken; en |  |  |  |
| 16c. | een verplichting voor de dienstverlener om de (betaal)instelling te helpen de functie op ordelijke wijze over te dragen wanneer de uitbestedingsovereenkomst wordt beëindigd. |  |  |  |
| 17. | De verplichting voor dienstverleners, waar relevant, om aan de juiste IT-beveiligingsnormen voor gegevens en systemen te voldoen. |  |  |  |
| 18. | De verplichting dat de dienstverlener vertrouwelijke, persoonlijke of anderszins gevoelige informatie moet beschermen en moet voldoen aan alle wettelijke vereisten betreffende de bescherming van gegevens die voor de (betaal)instelling gelden. |  |  |  |
| 19. | Het recht van de interne auditfunctie om de uitbestede functie via een op risico’s gebaseerde benadering te toetsen. |  |  |  |
| 20. | Voor dienstverleners in een EU lidstaat: een verwijzing naar de bevoegdheden van bevoegde autoriteiten en afwikkelingsautoriteiten inzake informatievergaring en onderzoek krachtens artikel 63, lid 1, onder a), van Richtlijn 2014/59/EU (BRRD) en artikel 65, lid 3, van Richtlijn 2013/36/EU (CRD IV). Als de dienstverlener in een derde land is gevestigd, moeten deze rechten ook van toepassing zijn. |  |  |  |
| 21. | De mogelijkheid van de instelling om periodieke penetratietests te kunnen uitvoeren om te kunnen beoordelen hoe effectief de ten uitvoer gelegde cyber- en interne ICT-veiligheidsmaatregelen en -processen zijn. |  |  |  |
| **EBA Richtsnoeren inzake uitbesteding - Voor kritieke of belangrijke functies - ALGEMEEN** | | | | |
| **N.B.:** Paragraaf 4 van de EBA Richtsnoeren inzake uitbesteding bepalen wanneer een functie als kritiek of belangrijk wordt aangemerkt. Instellingen moeten een functie altijd als kritiek of belangrijk aanmerken:  a. wanneer een gebrekkige of tekortschietende uitvoering ervan materiële nadelige gevolgen zou hebben voor:  i. het voortdurend voldoen door (betaal)instellingen aan de vergunningsvoorwaarden of andere verplichtingen waaraan zij uit hoofde van Richtlijn 2013/36/EU (CRD IV), Verordening (EU) nr. 575/2013 (CRR), Richtlijn 2014/65/EU (MiFID II), Richtlijn (EU) 2015/2366 (PSD2) en Richtlijn 2009/110/EG (EMD 2) zijn onderworpen, en van hun regelgevingsverplichtingen;  ii. hun financiële resultaten; of  iii. de soliditeit of continuïteit van hun bank- en betalingsdiensten en -activiteiten;  b. wanneer operationele taken van interne controlefuncties worden uitbesteed, tenzij uit de beoordeling blijkt dat het geen nadelige gevolgen voor de doeltreffendheid van de interne controlefunctie zou hebben als de uitbestede functie niet of op onjuiste wijze zou worden verricht;  c. wanneer zij van plan zijn functies van bankactiviteiten of betalingsdiensten op zo'n schaal uit te besteden dat daarvoor toestemming van een bevoegde autoriteit nodig is. | | | | |
| 22. | Of onderuitbesteding is toegestaan en zo ja, onder welke voorwaarden. Alle soorten activiteiten die van onderuitbesteding zijn uitgesloten moeten worden vermeld. |  |  |  |
| 23. | De locatie(s) (d.w.z. regio's of landen) waar de kritieke of belangrijke functie zal worden verricht en/of waar de relevante gegevens zullen worden bewaard en verwerkt, inclusief de mogelijke opslaglocatie, en de voorwaarden waaraan moet worden voldaan, met inbegrip van de vereiste om de (betaal)instelling in kennis te stellen als de dienstverlener voorstelt de locatie(s) te wijzigen. |  |  |  |
| 24. | Het onbeperkte recht van de (betaal)instelling en toezichthouders om de dienstverlener te inspecteren en te controleren, vooral als het gaat om de kritieke of belangrijke uitbestede functie, met inbegrip van volledige toegang tot alle relevante bedrijfslocaties (bijv. hoofdkantoren en operationele centra), inclusief het volledige scala aan relevante apparatuur, systemen, netwerken, informatie en gegevens die worden gebruikt om de uitbestede functie te verrichten en bijbehorende financiële informatie, personeel en de externe auditors van de dienstverlener. |  |  |  |
| 25. | De verplichting van de dienstverlener om aan alle toepasselijke wet- en regelgeving en contractuele verplichtingen te voldoen. |  |  |  |
| **EBA Richtsnoeren inzake uitbesteding - Voor kritieke of belangrijke functies – ALS ONDERUITBESTEDING IS TOEGESTAAN** | | | | |
| 26. | De verplichting van de dienstverlener om toezicht te houden op diensten die hij heeft onderuitbesteed, om ervoor te zorgen dat de contractuele verplichtingen tussen de dienstverlener en de (betaal)instelling voortdurend worden nagekomen. |  |  |  |
| 27. | De verplichting voor de dienstverlener om voorafgaande specifieke of algemene schriftelijke toestemming van de (betaal)instelling te krijgen alvorens tot onderuitbesteding van de gegevens over te gaan. |  |  |  |
| 28. | Een verplichting voor de dienstverlener om de (betaal)instelling te informeren over elke geplande onderuitbesteding, of materiële wijzigingen daarin, met name wanneer de dienstverlener zijn verantwoordelijkheden op grond van de uitbestedingsovereenkomst daardoor minder goed kan vervullen. De kennisgevingstermijn moet de uitbestedende (betaal)instelling in staat stellen de risico's van de voorgestelde wijzigingen te beoordelen en bezwaar te maken tegen wijzigingen voordat de geplande onderuitbesteding, of materiële wijzigingen daarin, plaatsvinden. |  |  |  |
| 29. | Het recht van de (betaal)instelling om bezwaar te maken tegen een beoogde onderuitbesteding, of materiële wijzigingen daarin, of dat expliciete goedkeuring is vereist. |  |  |  |
| 30. | Het recht om de overeenkomst in het geval van onnodige onderuitbesteding te beëindigen, bijvoorbeeld wanneer door de onderuitbesteding de risico's voor de (betaal)instelling materieel toenemen of als de dienstverlener tot onderuitbesteding overgaat zonder de (betaal)instelling daarvan in kennis te stellen. |  |  |  |
| 31. | De verplichting van de onderaannemer om aan alle toepasselijke wet- en regelgeving en contractuele verplichtingen te voldoen. |  |  |  |
| 32. | De toekenning van dezelfde contractuele toegangs- en auditrechten aan de (betaal)instelling en toezichthouder als aan de dienstverlener. |  |  |  |
| 33. | De verplichting van de dienstverlener om op passende wijze toezicht op de onderdienstverleners te houden, conform het beleid dat de (betaal)instelling heeft vastgesteld. |  |  |  |
| **DORA – Algemene verplichtingen voor ICT contracten met ICT dienstverleners** | | | | |
| **N.B.**: Deze verplichtingen zijn van toepassing op alle overeenkomsten inzake het gebruik van ICT-diensten, ongeacht de vraag of de overeenkomsten een uitbesteding zijn. ‘**ICT-diensten**’ is ruim gedefinieerd als:  *“digitale en gegevensdiensten die doorlopend via ICT-systemen aan een of meer interne of externe gebruikers worden verleend, waaronder hardware als dienst en hardwarediensten, met inbegrip van het verlenen van technische ondersteuning via software- of firmware-updates door de hardwareaanbieder, met uitzondering van traditionele analoge telefoondiensten”* | | | | |
| 34. | Een duidelijke en volledige beschrijving van alle door de derde aanbieder van ICT-diensten te leveren functies en ICT-diensten, met vermelding of het uitbesteden van een ICT-dienst die een kritieke of belangrijke functie ondersteunt, of van materiële onderdelen daarvan, is toegestaan en indien dit het geval is, welke voorwaarden op die uitbesteding van toepassing zijn. |  |  |  |
| 35. | De locaties, met name de regio’s of landen, waar de contractueel overeengekomen of uitbestede functies en ICT-diensten moeten worden geleverd en waar gegevens moeten worden verwerkt, met inbegrip van de opslaglocatie, en de verplichting voor de derde aanbieder van ICT-diensten om de financiële entiteit vooraf in kennis te stellen indien hij voornemens is van locatie te veranderen. |  |  |  |
| 36. | Bepalingen inzake beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid met betrekking tot de bescherming van gegevens, met inbegrip van persoonsgegevens. |  |  |  |
| 37. | Bepalingen inzake het waarborgen van de toegang, het herstel en de teruggave in een gemakkelijk toegankelijk formaat van door de financiële entiteit verwerkte persoonsgegevens en niet-persoonsgebonden gegevens in geval van insolventie, afwikkeling of stopzetting van de bedrijfsactiviteiten van de derde aanbieder van ICT-diensten, of in geval van beëindiging van de contractuele overeenkomsten. |  |  |  |
| 38. | Beschrijvingen van het dienstenniveau, met inbegrip van actualiseringen en herzieningen daarvan. |  |  |  |
| 39. | De verplichting van de derde aanbieder van ICT-diensten om de financiële entiteit zonder extra kosten, of tegen een vooraf bepaalde kostprijs, bijstand te verlenen wanneer zich een incident voordoet dat verband houdt met de aan de financiële entiteit geleverde ICT-dienst. |  |  |  |
| 40. | De verplichting van de derde aanbieder van ICT-diensten om volledige medewerking te verlenen aan de bevoegde autoriteiten en de afwikkelingsautoriteiten van de financiële entiteit, met inbegrip van de door hen aangestelde personen. |  |  |  |
| 41. | Beëindigingsrechten en de bijbehorende minimumopzegtermijnen voor de beëindiging van de contractuele overeenkomsten, in overeenstemming met de verwachtingen van de bevoegde autoriteiten en de afwikkelingsautoriteiten. |  |  |  |
| 42. | De voorwaarden voor deelname van derde aanbieders van ICT-diensten aan bewustmakingsprogramma’s op het gebied van ICT-beveiliging en opleidingen inzake digitale operationele weerbaarheid van de financiële entiteiten, overeenkomstig artikel 13 lid 6 DORA. |  |  |  |
| 43. | Het recht de overeenkomst te beëindigen in elk van de volgende omstandigheden: |  |  |  |
| 43a. | bij ernstige overtreding van de toepasselijke wetten, voorschriften of contractuele voorwaarden door de derde aanbieder van ICT-diensten; |  |  |  |
| 43b. | in omstandigheden die in de loop van de monitoring van het ICT-risico van derde aanbieders worden vastgesteld, waarvan wordt aangenomen dat deze wijzigingen kunnen brengen in de uitvoering van de functies waarin de contractuele overeenkomst voorziet, met inbegrip van materiële wijzigingen die de overeenkomst of de situatie van de derde aanbieder van ICT-diensten nadelig beïnvloeden; |  |  |  |
| 43c. | bij klaarblijkelijke zwakheden van de derde aanbieder van ICT-diensten in verband met zijn algemeen beheer van het ICT-risico en in het bijzonder met de manier waarop hij zorgt voor de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van persoonlijke of anderszins gevoelige gegevens of niet-persoonsgebonden gegevens; |  |  |  |
| 43d. | indien de bevoegde autoriteit niet langer doeltreffend toezicht kan uitoefenen op de financiële entiteit ten gevolge van de voorwaarden van of de omstandigheden in verband met de respectieve contractuele overeenkomst. |  |  |  |
| **DORA – Algemene verplichtingen voor ICT-diensten die kritieke of belangrijke functies ondersteunen** | | | | |
| **N.B.**: een ‘**kritieke of belangrijke functie**’ is als volgt gedefinieerd in artikel 3(22) DORA:  *“een functie waarvan de verstoring wezenlijk afbreuk zou doen aan de financiële prestaties van een financiële entiteit of aan de soliditeit of de continuïteit van haar diensten en activiteiten, of waarvan de beëindiging of gebrekkige of mislukte uitvoering wezenlijk afbreuk zou doen aan de permanente naleving door een financiële entiteit van de voorwaarden en verplichtingen uit hoofde van haar vergunning of haar andere verplichtingen uit hoofde van het toepasselijke recht inzake financiële diensten”.* | | | | |
| 44. | Beschrijvingen van het niveau van volledige dienstverlening, met inbegrip van actualiseringen en herzieningen daarvan met nauwkeurige kwantitatieve en kwalitatieve prestatiedoelstellingen binnen de overeengekomen dienstverleningsniveaus, teneinde de financiële entiteit in staat te stellen een doeltreffende monitoring van de ICT-diensten te verrichten en onverwijld passende corrigerende maatregelen te nemen wanneer de overeengekomen dienstverleningsniveaus niet worden gehaald. |  |  |  |
| 45. | Kennisgevingstermijnen en rapportageverplichtingen van de derde aanbieder van ICT-diensten ten aanzien van de financiële entiteit, met inbegrip van de kennisgeving van ontwikkelingen die materiële gevolgen kunnen hebben voor het vermogen van de derde aanbieder om op doeltreffende wijze de ICT-diensten die kritieke of belangrijke functies ondersteunen te leveren in overeenstemming met de afgesproken dienstverleningsniveaus. |  |  |  |
| 46. | Verplichtingen voor de derde aanbieder van ICT-diensten om bedrijfsnoodplannen in te voeren en te testen en te beschikken over ICT-beveiligingsmaatregelen, -instrumenten en -beleidslijnen waarmee de financiële entiteit kan zorgen voor een passend niveau van veiligheid bij het verlenen van diensten in overeenstemming met haar regelgevingskader. |  |  |  |
| 47. | De verplichting voor de derde aanbieder van ICT-diensten om deel te nemen aan en volledig mee te werken bij *threat led penetration testing* (TLPT) van de financiële entiteit als bedoeld in de artikelen 26 en 27 DORA. |  |  |  |
| **N.B.**:In afwijking van punt 47 hierboven, kunnen de derde aanbieder van ICT-diensten en de financiële entiteit die een micro-onderneming is, overeenkomen dat de rechten van toegang, inspectie en audit van de financiële entiteit mogen worden gedelegeerd aan een onafhankelijke derde partij die wordt aangesteld door de derde aanbieder van ICT-diensten, en dat de financiële entiteit de derde partij te allen tijde om informatie en garanties kan verzoeken met betrekking tot de prestaties van de derde aanbieder van ICT-diensten.  Een ‘**micro-onderneming**’ is gedefinieerd als: *“een financiële entiteit die geen handelsplatform, centrale tegenpartij, transactieregister of centrale effectenbewaarinstelling is, en waar minder dan 10 personen werkzaam zijn en waarvan de jaaromzet en/of het jaarlijkse balanstotaal niet hoger liggen dan EUR 2 miljoen.”* | | | | |
| 48. | Het recht om de prestaties van de derde aanbieder van ICT-diensten permanent te monitoren, hetgeen het volgende inhoudt: |  |  |  |
| 48a. | onbeperkte rechten van toegang, inspectie en audit door de financiële entiteit of een daartoe aangestelde derde partij alsook door de bevoegde autoriteit, en het recht om ter plaatse kopieën van relevante documenten te maken indien deze cruciaal zijn voor de activiteiten van de derde aanbieder van ICT-diensten, waarbij de doeltreffende uitoefening van dit recht niet wordt belemmerd of beperkt door andere contractuele overeenkomsten of ander uitvoeringsbeleid; |  |  |  |
| 48b. | het recht om andere garantieniveaus overeen te komen indien de rechten van andere cliënten worden aangetast; |  |  |  |
| 48c. | de verplichting van de derde aanbieder van ICT-diensten om tijdens de door de bevoegde autoriteiten, de lead overseer, de financiële entiteit of een aangestelde derde partij ter plaatse uitgevoerde inspecties en audits volledig mee te werken; en |  |  |  |
| 48d. | de verplichting om bijzonderheden te verschaffen over het toepassingsgebied, te volgen procedures en de frequentie van dergelijke inspecties en audits. |  |  |  |
| 49. | exitstrategieën, met name de invoering van een verplichte passende overgangsperiode: |  |  |  |
| 49a. | waarin de derde aanbieder van ICT-diensten de levering van de respectieve functies of ICT-diensten zal blijven voortzetten, teneinde het risico op verstoring bij de financiële entiteit te beperken of voor een doeltreffende afwikkeling en herstructurering te zorgen; |  |  |  |
| 49b. | waarin de financiële entiteit kan overstappen naar een andere derde aanbieder van ICT-diensten of naar interne oplossingen in overeenstemming met de complexiteit van de geleverde dienst. |  |  |  |