**CHECKLIST UITBESTEDINGSCONTRACTEN**

Deze checklist geeft een overzicht van de verplichtingen die er vanuit de EBA Richtsnoeren inzake uitbesteding (EBA/GL/2019/02) aan uitbestedingscontracten worden gesteld. Een verwijzing naar ‘instellingen’ verwijst naar kredietinstellingen en beleggingsondernemingen in de zin van Richtlijn 2013/36/EU (CRD IV) and een verwijzing naar ‘betaalinstellingen’ verwijst naar betaalinstellingen en elektronischgeldinstellingen.

**N.B.: Deze checklist geeft een overzicht van de belangrijkste bepalingen voor uitbestedingscontracten volgens de EBA Richtsnoeren inzake uitbesteding, 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** |
| **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 toepasselijk 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. |  |  |  |
| **Voor kritieke of belangrijke functies - ALGEMEEN** | | | | |
| 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. |  |  |  |
| **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. |  |  |  |