Leidraad IT-risico's Volmacht

Toelichting met handvatten voor de Nederlandse volmachtmarkt i.v.m. wet- en regelgeving over informatiebeveiliging (Good Practice Informatiebeveiliging van DNB)

maart 2024

Deze Leidraad vervangt de versie van 2021 en is volledig vernieuwd. De Leidraad is bedoeld als hulpmiddel. De tekst van wet- en regelgeving (IT - informatiebeveiliging), de Good Practice Informatiebeveiliging van DNB, DORA etc. zijn leidend.

VOORAF

De Wet op het financieel toezicht (Wft) vereist van een financiële dienstverlener dat hij beschikt over adequate procedures en maatregelen om IT-risico's te beheersen. Adequaat betekent in dit verband dat de procedures en maatregelen zijn gebaseerd op de aard, omvang en complexiteit van de risico's van de activiteiten van de dienstverlener en de complexiteit van zijn organisatiestructuur.

Sinds een aantal jaren onderzoekt DNB de kwaliteit van informatiebeveiliging en cybersecurity binnen de financiële sector. De afgelopen jaren ziet DNB in de financiële sector en daarbuiten een toename van potentieel zeer schadelijke cyberdreigingen. Daarnaast ziet DNB een financiële sector die door verschillende vormen van uitbesteding en samenwerkingsverbanden steeds meer in ketens opereert, met de daarbij behorende kansen en risico's voor informatiebeveiliging en cybersecurity. Zie DNB Q&A Toetsingskader Informatiebeveiliging, pagina 3.

DNB ziet dat instellingen in toenemende mate belangrijke bedrijfsprocessen zoals ICT, vermogensbeheer, klanten-, pensioen-, polis- en financiële administraties uitbesteden (outsourcing). Tegenover de voordelen van uitbesteding staan ook risico's waar een instelling zich aan blootstelt. In het kader van de informatiebeveiliging en cybersecurity is dat bijvoorbeeld de ongewenste omgang van de dienstverlener met vertrouwelijke gegevens van de instelling. Ook bestaat het risico dat de beveiliging van vertrouwelijke gegevens bij de dienstverlener of diens onderuitbestedingspartner niet in overeenstemming is met het beleid van de financieel dienstverlener. Zie DNB Q&A Toetsingskader Informatiebeveiliging, pagina 20.

DNB geeft in de Good Practice Informatiebeveiliging 2023 aan de onder haar toezicht staande instellingen actuele handvatten en beheersmaatregelen, waarmee zij kunnen voldoen aan de wettelijke bepalingen om de voortdurende beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van de (geautomatiseerde) gegevensverwerking te waarborgen.. Daarnaast heeft de Europese Commissie de digital operational resilience act (DORA) voor de gehele Europese financiële sector vastgesteld. Deze verordening vervangt bestaande regelgeving, en stelt wettelijke bepalingen om de cyberweerbaarheid van de financiële sector te verhogen.
DNB heeft daarnaast diverse handreikingen opgesteld waarin meer uitleg en toelichting staat over de termen of begrippen genoemd in de Good Practice Informatiebeveiliging of die ter aanvulling dienen (SBA-IB - De Nederlandsche Bank; Handreiking volwassenheidsniveaus SBA-IB - De Nederlandsche Bank; Woordenlijst bij SBA-ORM - De Nederlandsche Bank). DNB heeft naast aanpassing van de Good Practice een self assessment informatiebeveiliging ontwikkeld waarmee instellingen een analyse kunnen uitvoeren van hun volwassenheid voor wat betreft informatiebeveiliging . Zie Good Practice Informatiebeveiliging 2023 (dnb.nl)
Op grond van een risicoanalyse dienen instellingen beheersingsmaatregelen te treffen die passen bij de aard, omvang en complexiteit van de risico's van de activiteiten van de instelling en de complexiteit van haar organisatiestructuur. Deze beheersingsmaatregelen zijn niet alleen gericht op technologische oplossingen (Technology), zij zijn ook gericht op menselijk handelen (People), inrichting van processen (Processes) en faciliteiten (Facilities).
Zie DNB Q&A Toetsingskader Informatiebeveiliging

Ook de Principes Informatiebeveiliging van AFM bieden handvatten bij de invulling van wettelijke vereisten. AFM benadrukt dat het belangrijk is voor de onderneming én voor haar klanten. Klanten moeten namelijk kunnen vertrouwen op passende dienstverlening en passende beveiliging van hun

persoonsgegevens. Bovendien moeten ondernemingen integer en vertrouwelijk met de klantgegevens omgaan. De AFM verwacht daarom dat ondernemingen zorgvuldig omgaan met informatiebeveiligingsrisico's. Zie AFM publiceert Principes voor Informatiebeveiliging

Wettelijk kader
Het (wettelijk) kader voor deze leidraad wordt gevormd door de Wet op het financieel toezicht (Wft), Besluit prudentiële regels (Bpr), wet- en regelgeving vanuit EIOPA, Privacywetgeving (waaronder AVG en UAVG), de Good Practice Beheersing volmachten schadeverzekeraars van DNB, de Good Practice Uitbesteding Verzekeraars van DNB, de Good Practice informatiebeveiliging 2023 van DNB, de Principes voor Informatiebeveiliging van AFM en de Digital Operations Resilience Act (DORA).

INHOUD

1. GOOD PRACTICE INFORMATIEBEVEILIGING

In de Good Practice Informatiebeveiliging 2023 leest u welke beheersingsmaatregelen een gevolmachtigde zou kunnen treffen gericht op technologie, menselijk handelen, inrichting van processen en faciliteiten. Daarnaast is daarin omschreven wat verwacht wordt van de organisatie-inrichting om de beheersing van de risico's aan te sturen, voortdurend de effectiviteit van de maatregelen te toetsen en waar nodig te verbeteren.

De regelgeving kent open normen voor beheersing van IT-risico's. Om de implementatie hiervan in de volmachtmarkt te ondersteunen, is deze leidraad opgesteld. Het biedt handvatten voor een praktische invulling, die op dit moment al op onderdelen geborgd is in het Werkprogramma Risicobeheersing volmachten. De komende periode worden de taken in het Werkprogramma Risicobeheersing volmachten nog aangevuld op de onderdelen uit de Good Practice Informatiebeveiliging 2023 die ook van belang zijn voor een gevolmachtigde om aan te tonen dat hij de risico's op het gebied van informatiebeveiliging en cybersecurity voldoende beheerst.

Verzekeraars hebben ieder hun eigen beleid met betrekking tot IT-beveiliging, dat een samenhangend geheel van maatregelen, procedures en processen bevat waarmee informatiebeveiligingsrisico's worden beheerst. Dit beleid kan strenger of minder streng zijn dan in de Good Practice Informatiebeveiliging 2023 is beschreven. Per onderdeel kunnen er door verzekeraars specifieke eisen gesteld worden waar de gevolmachtigde zich aan moet houden. Zo kan bijvoorbeeld de ene verzekeraar striktere eisen stellen aan de technologische beveiliging dan een andere verzekeraar. Raadpleeg uw contactpersoon bij de verzekeraar voor eventueel maatschappij-specifiek beleid.

Als bijlage bij deze Leidraad is de Good Practice Informatiebeveiliging 2023 van DNB opgenomen. Deze Good Practice Informatiebeveiliging is recent aangepast. Zie Good Practice Informatiebeveiliging 2023 (dnb.nl)

De belangrijkste wijzigingen
De Good Practice Informatiebeveiliging 2023 kent dezelfde indeling als de Good Practice Informatiebeveiliging 2019/2020'. Het is een verdere verdieping en aanscherping, die past bij toenemende en veranderende cyberdreigingen.

De belangrijkste wijzigingen in de Good Practice Informatiebeveiliging 2023 zijn:

1. Aandacht voor de digitale operationele weerbaarheidsstrategie op korte, midden en lange termijn die uiteenzet hoe het Risk Management Framework, met inbegrip van regie op derde partijen wordt uitgevoerd.
2. Aandacht voor een risico-gebaseerde invulling per control. Instellingen kunnen daardoor verdergaand maatwerk toepassen ten aanzien van de inrichting en implementatie van hun specifieke informatiebeveiligingsmaatregelen.
3. Aandacht voor het uitvoeren van een business impact analyse, om daarmee de blootstelling van de instelling aan ernstige bedrijfsonderbrekingen en de potentiële gevolgen daarvan te kunnen beoordelen.
4. Aandacht voor de gewenste rol van het bestuur bij het onderwerp informatiebeveiliging in zijn geheel; de rol is ook in een aantal controls explicieter benoemd.

5. Aandacht voor het ontwikkelen en bijhouden van kennis van het dagelijks bestuur, RvC, RvT en sleutelfunctiehouders, door het aantoonbaar volgen van op hen toegespitste trainingen, om de belangrijkste IT- en cyberrisico's te begrijpen en te kunnen adresseren.
6. Aandacht voor kansen en risico's die samenhangen met technologische ontwikkelingen zoals quantum computing en artificial intelligence.
7. Met de geactualiseerde Good Practice Informatiebeveiliging 2023 bevordert DNB dat instellingen op het gebied van informatiebeveiliging en cybersecurity een stap maken in de richting naar implementatie van DORA per 17 januari 2025. Het is aan de instellingen om zich goed voor te bereiden op DORA. In 2024 bepaalt DNB hoe deze Good Practice Informatiebeveiliging zich verhoudt tot de dan uitgewerkte DORA regelgeving. Hierom kan in deze versie van de leidraad een verdere uitwerking van DORA nog niet worden opgenomen.

Voor de op dit moment lopende onderzoeken en voor de uitvraag sectorbrede analyse informatiebeveiliging (SBA-IB) 2024 blijft de Good Practice informatiebeveiliging 2019/2020 het uitgangspunt. Voor DNB onderzoeken, uitvragen en andere toezichtactiviteiten op het gebied van informatiebeveiliging die starten na het tweede kwartaal van 2024 hanteert DNB in beginsel de Good Practice informatiebeveiliging 2023. Dit zal waar van toepassing nadrukkelijk in de aankondigingsbrief van het desbetreffende onderzoek of uitvraag worden vermeld.

2. DORA

Wat is DORA?

DORA is een pakket van maatregelen dat digitale innovatie in de financiële sector moet bevorderen, en tegelijkertijd de daaruit voorvloeiende risico's moet beperken. Het is het eerste wettelijk kader op het gebied van ICT weerbaarheid voor veel soorten organisaties én voor de toezichthouder, waarbij concreet invulling gegeven wordt aan de norm 'beheerste bedrijfsvoering' . DORA borduurt voort op al bestaande wettelijke vereisten op het gebied van ICT risk management. In DORA komen alle wettelijke vereisten op dit gebied samen, met als doel meer harmonisatie binnen de EU, toezichthouders en de financiële ondernemingen.

DORA is verdeeld in vijf inhoudelijke hoofdstukken. Ieder hoofdstuk bevat diverse vereisten waar financiële ondernemingen aan moeten voldoen.

HOOFDSTUK	ONDERWERP	DOEL
Hoofdstuk II *(art. 4 – 14)*	ICT Risicobeheer, bestaande uit een onderdeel *Governance* en *ICT-Risicobeheer*	Ervoor zorgen dat financiële ondernemingen adequaat ICT-risicomanagement hebben ingericht.
Hoofdstuk III *(art. 15 – 20)*	ICT-gerelateerde incidenten: beheer, classificatie en rapportage	Het borgen van een adequaat proces/procedure voor het rapporteren, adresseren en beheren van alle ICT gerelateerde incidenten.
Hoofdstuk IV *(art. 21 – 24*	Testen van Digitale Operationele Veerkracht	Financiële ondernemingen worden verantwoordelijk voor het continu testen en beoordelen op de adequaatheid van maatregelen en veerkracht van de ICT-systemen, zodat mogelijke kwetsbaarheden aan het licht komen.
Hoofdstuk V *(art. 25 – 39)*	Beheer van ICT-risico van derde aanbieder: • Afdeling 1: basisbeginselen voor een degelijk beheer van het ICT-risico van derde aanbieder • Afdeling 2: toezichtkader voor cruciale derde aanbieders van ICT-diensten	Ervoor zorgen dat financiële ondernemingen een gedegen monitoring inrichten van het ICT-risico van derde aanbieders/ICT dienstverleners/Cloud Service Providers/etc.
Hoofdstuk VI *(art. 40)*	Regelingen voor informatie-uitwisseling	De Verordening maakt het mogelijk om informatie tussen ondernemingen te delen over cyberbedreigingen.

Inwerkingtreding DORA

Op 17 januari 2025 wordt DORA van toepassing. Dan moeten financiële entiteiten compliant zijn met DORA en de technische reguleringsnormen die nog ontwikkeld worden door de Europese toezichthoudende autoriteiten.

3. LEVERANCIER / (ONDER) UITBESTEDING

3.1 Uitbesteding

Er zijn diverse leveranciers waar een groot deel van de volmachtmarkt mee samenwerkt. Deze leidraad bevat een (niet limitatieve) set voorwaarden die in de overeenkomsten met leveranciers terug zouden kunnen komen. Ook al behoeft de uitbesteding de goedkeuring van de verzekeraar is het de gevolmachtigde die binnen het gestelde in artikel 2.7 van de VSV een keuze maakt voor eventuele samenwerking met leveranciers. De set voorwaarden geeft de gevolmachtigde handvatten bij het vastleggen van de samenwerking. Daarnaast geeft het de verzekeraar ook een instrument bij de beoordeling van het verzoek van de gevolmachtigde om goedkeuring te geven aan de (onder) uitbesteding.

3.2 ISAE 3402 type 2 of SOC 2 rapport

Vertegenwoordigers vanuit de NVGA en het Verbond van Verzekeraars zullen gezamenlijk met IT-leveranciers afstemmen over het door de leverancier periodiek (jaarlijks) aan de gevolmachtigde afgeven van een ISAE-3000 of 3402 (type 2) of SOC 1 of 2 (type 2) verklaring voor de IT diensten die de gevolmachtigde van de leverancier heeft afgenomen. Met die verklaring kan de gevolmachtigde aan de verzekeraar aantonen dat en hoe kritische processen die hij heeft uitbesteed worden beveiligd en de risico's al dan niet worden beheerst.

Voor een ISAE 3400 of 3402 of SOC 1 of 2 type 2 rapport worden werkzaamheden uitgevoerd om vast te stellen dat in een bepaalde periode de interne beheersmaatregelen, die in opzet in voldoende mate het risico afdekken, hebben bestaan en gedurende een in de rapportage opgenomen periode ook hebben gewerkt.
De inschatting van de NVGA en het Verbond van Verzekeraars is dat door de gezamenlijke afstemming leveranciers eerder bereid zullen zijn deze verklaring periodiek (in beginsel jaarlijks) te verstrekken dan wanneer individuele gevolmachtigden dit vragen.

3.3 Leverancier selectie informatiebeveiliging

In de precontractuele fase en bij de selectie van een leverancier (dus nog niet de dienst) is het van belang om snel inzicht te krijgen in de volwassenheid van de leverancier op het gebied van informatiebeveiliging. Meer algemene punten zoals *pre-employment screening, verwerkingsovereenkomst,* of *right-to-audit* worden contractueel afgesproken.
Met behulp van de ISO 27002-2022 standaard is een aantal belangrijke informatiebeveiligingseisen geselecteerd. Op basis hiervan zijn vragen geformuleerd die een organisatie kan stellen aan de betreffende leverancier om snel inzicht te krijgen in de security risico's.
Met de verkregen informatie kan worden besloten of de organisatie door wil gaan met de selectie van de dienst (fase 2) en vervolgens het contracteren, waarna formele security agreements kunnen worden afgesloten in het contracteringsproces.
In de inventarisatiefase kan de gevolmachtigde onderstaande vragen gebruiken om inzicht in de belangrijkste security vraagstukken te krijgen en advies te kunnen geven aan de contracteigenaren, procurement en/of andere business eigenaren.

<u>Security vragen aan leveranciersrelevant in de precontractuele fase</u>

1. Over welke security certificeringen en assuranceverklaringen beschikt u? *(ISO: 5.19 Information security in supplier relationships)*
2. Beschikt u over een actueel en door het management geaccordeerd informatiebeveiligings- en BCM-beleid? Welke security- en BCM-standaarden zijn hierin opgenomen? Kunt u uw informatiebeveiligings- en BCM-beleid met ons delen? *(ISO: 5.1 Policies for information security)*
3. Hoe ziet uw informatiebeveiligingsorganisatie eruit? Welke functionarissen/afdelingen voor informatiebeveiliging zijn bij u actief (zoals bijv. CISO en een SOC) en wat zijn de rapportagelijnen (bij voorkeur visueel weer te geven)? *(ISO: 5.2 Information security roles and responsibilities)*
4. Heeft u een formeel autorisatiebeleid en -proces ingericht? Kunt u deze met ons delen? *(ISO: 5.3 Segregation of duties)*
5. Heeft u in contracten met leveranciers (en onderaannemers) vastgelegd dat zij aan een vergelijkbaar (met uw eigen instelling/het voor de verleende diensten afgesproken niveau van beveiliging) niveau van informatiebeveiliging moeten voldoen? Is informatie over de data, systemen en diensten beschikbaar in een (of meer) register(s)? *(ISO: 5.9 Inventory of information and other associated assets)*
6. Is uw logische toegangsbeveiliging aantoonbaar ingericht conform het autorisatiebeleid? Waaruit blijkt dit (denk aan een Identity Access Management Systeem)? *(ISO: 5.15 Access control)*
7. Maakt u gebruik van standaard SLA-afspraken en zijn afspraken met betrekking tot informatiebeveiliging en rapportages hierin expliciet inbegrepen (graag een template toevoegen)? *(ISO: 5.19 Information security in supplier relationships)*
8. Beschikt u over een formeel incidentenmanagementproces waarbij klanten onverwijld worden geïnformeerd? *(ISO: 5.26 Response to information security incidents)*
9. Heeft u actuele (IT)-herstelplannen inclusief Business Continuity- en Disaster Recovery Plannen? Zijn deze plannen in de afgelopen 12 maanden getest? Beschikt u over exit-plannen met uw onderaannemers? *(ISO: 5.30 ICT readiness for business continuity)*
10. Beschikt u over een formeel privacy-beleid, is deze beschikbaar en wordt deze aantoonbaar nageleefd? *(ISO: 5.34 Privacy and protection of PII)*
11. Heeft uw organisatie een Secure Development Life Cycle geïmplementeerd en is deze ingericht in lijn met een markt standaard (b.v. Microsoft Security Development Lifecycle (SDL), OpenSAMM, BSIMM, SSE CMM, SafeCode of de NIST SSDF? *(ISO: 8.25 Secure development life cycle)*
    Penetration Testing is onderdeel van deze cyclus. In (assurance, audit) rapporten moet worden aangetoond dat minstens één keer per jaar een pentest is uitgevoerd en dat de bevindingen uit de test zijn opgelost op basis van de ernst van de bevindingen. *(ISO: 8.29 Security testing in development and acceptance)*
12. Beschikt uw organisatie over een security awareness programma en wordt de mate van security awareness van uw medewerkers periodiek gemeten? *(ISO: 6.3 Information security awareness, education and training)*
13. Heeft u een fysiek veiligheidsbeleid en wordt toegang tot kritieke ruimtes (serverruimtes, datacenters, etc.) gemonitord op evt. ongeautoriseerde toegang? *(ISO: 7.4 Physical security monitoring)*

14. Maakt u gebruik van security baselines gebaseerd op marktstandaarden (CIS-benchmarks, NIST, STIG, etc.) of leverancier security-richtlijnen? Zo ja: welke heeft u in gebruik en hoe worden deze gemonitord? *(ISO: 8.9 Configuration management)*
15. Hoe is de (fysieke/virtuele) scheiding (van de verschillende klanten) op netwerkniveau ingericht? *(ISO: 8.22 Segregation of networks)*
16. Voldoen de gebruikte versleuteling technologieën aan de gewenste en gecontracteerde beveiligingsniveaus en is hierbij rekening gehouden met het type, sterkte en kwaliteit van het versleutelingsalgoritme? Welke crypto standaarden heeft u in gebruik? Is hiernaast sleutelbeheer ingericht? *(ISO: 8.24 Use of cryptography)*
17. Maakt u gebruik van gescheiden omgevingen voor ontwikkeling, test, acceptatie en productie. Zijn deze voor iedere klant gescheiden (fysiek of logisch)? *(ISO: 8.31 Separation of development, test and production environments)*
18. Heeft u change management procedures en waarborgen dat alleen geautoriseerd wijzigingen worden geïmplementeerd en hoe zijn security aspecten van deze wijzigingen aangetoond? *(ISO: 8.32 Change management)*

3.4 Inhoud overeenkomst

Gevolmachtigden besteden in toenemende mate belangrijke bedrijfsprocessen uit. Dit brengt risico's met zich mee in het kader van informatiebeveiliging en data security. Het is voor gevolmachtigden van belang dat de prestaties van de dienstverlener en diens eventuele onder uitbestedingspartner overeenkomen met de eigen prestaties. In de contractvoorbereidingsfase wordt dan ook aandacht besteed aan de prestatie, en monitoring van deze prestaties. De maatregelen worden in een contract vastgelegd (fase 4 van het inkoopproces van Van Weele).

*In onderstaande tabellen staan **niet limitatief** de onderdelen die overwogen kunnen worden om terug te laten komen in een uitbestedings- en verwerkersovereenkomst.*

Overeenkomst uitbesteding		
Beschrijving dienstverlening	Generieke introductie van het soort bedrijf en de activiteiten en werkzaamheden die zijn uitbesteed	
Duur overeenkomst	Vastleggen van de geldigheid van de overeenkomst: - Ingangs- en einddatum - Looptijd - Afspraken over opzegging met en zonder opzegtermijn - Exitplan	Met opzegtermijn: minimaal 12 maanden om de continuïteit te waarborgen. Zonder opzegtermijn: Ieder der partijen is gerechtigd deze overeenkomst met onmiddellijke ingang te beëindigen, zonder inachtneming van enig opzegtermijn, indien: • ten aanzien van één van de partijen surseance van betaling of faillissement wordt aangevraagd of verleend respectievelijk uitgesproken;

		• één van de partijen onder curatele wordt gesteld of anderszins het vrije beheer over zijn vermogen verliest; • één van de partijen wordt ontbonden of in liquidatie treedt. • aanwijzingen van de toezichthouder(s) daartoe aanleiding geven; • een van de partijen niet voldoet aan wet- en regelgeving, waaronder begrepen het verliezen van een van de vereiste vergunningen. Voor het waarborgen van de continuïteit is het noodzakelijk om in een exitplan concrete afspraken te maken over beëindiging van (een deel van) de activiteiten en werkzaamheden. Onderdelen van een exitplan kunnen zijn: • Escrow • Periode van overdracht • Eisen t.a.v. overdracht van de data • Intellectueel eigendom • Scope • Vergoeding • Wijze van kennisborging- en overdracht Assests
Belangrijke verplichtingen	Verschillende onderwerpen die niet direct de activiteiten en werkzaamheden raken, maar wel belangrijk zijn om vast te leggen: - Geheimhouding - Aansprakelijkheid - Intellectueel eigendom - Informatieveiligheid - Opslag van data locatieopslag is binnen Europese Economische Ruimte (EER).	Deze verplichtingen gelden bij aanvang, maar ook na beëindiging van de overeenkomst, waarbij gelet wordt op vergaande beperkingen en/of uitsluitingen. Bij het vastleggen van de verplichting ook opnemen de eisen die relevant zijn voor de beschikbaarheid, integriteit en vertrouwelijkheid van de (klant)informatie. En de minimale maatregelen van de leverancier om de vereisten af te dekken. Zoals bijvoorbeeld Life Cycle Management, toegangsbeveiliging, fysieke beveiliging, back-up / recovery, beveiligde gegevensuitwisseling en cybersecurity.
Wijzigingen	Natuurlijk kunnen de activiteiten, werkzaamheden en de afspraken hierover wijzigen. Het is belangrijk om vast te leggen op welke wijze wijzigingen op de overeenkomst afgesproken worden: - Alleen schriftelijk - Na wederzijds goedkeuren	Wijzigingen treden in plaats van eerdere schriftelijke en mondelinge afspraken. <u>Voorbeeld</u> Indien enige bepaling uit deze overeenkomst geheel of gedeeltelijk nietig blijkt te zijn, bijvoorbeeld wegens gewijzigde wet- en regelgeving, zal deze overeenkomst van kracht blijven en zullen partijen zich inspannen deze bepaling of deel daarvan te vervangen door een bepaling of deel dat wel geldig is

		en dat zoveel mogelijk in lijn is met de oorspronkelijke bedoelingen van partijen.
Bijlagen	Opsomming en volgorde van werking van alle bijlagen die onderdeel uitmaken van de samenwerking: - Overeenkomst - Verwerkersovereenkomst - Algemene voorwaarden - Service Level Agreement	Bij voorkeur zijn de eigen algemene voorwaarden van toepassing.
Wet- en regelgeving	De overeenkomst bevat een artikel dat de partij voldoet aan de geldende wet- en regelgeving en dat het Nederlands recht toepasselijk is. Bovendien is vastgelegd in welke rechtbank geschillen behandeld worden.	Voorbeeld Partijen verbinden zich ertoe aan huidig Nederlands en Europees wet- en regelgeving te voldoen, in het bijzonder omtrent het verwerken van persoonsgegevens inclusief meldplicht bij datalekken.
Prijzen	Welke afspraken zijn gemaakt: - Vaste kosten en prijzen van eventueel meerwerk - Kosten project- en ondersteuningsuren - Prijswijzigingen - Wijze en termijnen van facturatie en betaling - Btw	Misverstanden worden voorkomen door bijvoorbeeld een toestemmingsvereiste bij veranderingen en duidelijke omschrijving van de werkzaamheden behorend bij de prijzen.
Medewerkers	Medewerkers voldoen aan eisen op het gebied van: - Integriteit - Kwaliteit en/of ervaring - Bevoegdheden en autorisaties	
Onderaannemers	Afspraken over samenwerking met onderaannemers zijn vastgelegd: - Altijd vooraf toestemming van de klant / opdrachtgever - Alle bepalingen uit de overeenkomst gelden ook voor onderaannemers.	
SLA en Monitoring	Vastleggen en periodiek bespreken van de samenwerking en prestaties van de leverancier: - Rollen en verantwoordelijkheden	Opmerking Vastlegging prestaties en afspraken bij voorkeur in een Service Level Agreement.

	- Servicecomponenten en kritische prestatie indicatoren - Service en onderhoud afspraken - Prioriteiten incidenten - Overlegstructuur - Rapportage en informatieverplichtingen - Right to audit - Onderzoeksrecht Nationale en Europese toezichthouder - Escalatie
DNB inzagerecht	De onder-uitbestedingspartner verschaft DNB desgevraagd – indien gewenst ter plaatse - toegang tot de relevante boeken en administratieve bescheiden en volgt na kennisgeving door de verzekeraar of de gevolmachtigde de met zijn bedrijfsprocessen verband houdende aan de verzekeraar of de gevolmachtigde gegeven aanwijzingen van DNB op. De onder-uitbestedingspartner informeert de gevolmachtigde onverwijld over de aan DNB met betrekking tot te verstrekken inlichtingen respectievelijk het door DNB te houden onderzoek van boeken en administratieve bescheiden.
Auditrecht	Het auditrecht van de verzekeraar en haar externe auditor zoals beschreven in de samenwerkingsovereenkomst dient onvoorwaardelijk te zijn geborgd in de overeenkomst tussen de gevolmachtigde en de onder- uitbestedingspartner.

Verwerkersovereenkomst	
Uitgangspunt	De verwerkersovereenkomsten van de maatschappijen is een goed uitgangspunt. In de overeenkomst staan in ieder geval verwijzingen naar de AVG.
Verwerkingen	De aard en het doel van de verwerking, de persoonsgegevens die worden verwerkt, de categorieën van betrokkenen en de rechten en plichten van de verwerkingsverantwoordelijke.

Duur van de overeenkomst	De looptijd van de verwerkersovereenkomst is gelijk aan de looptijd van de uitbestedingsovereenkomst.	Bij beëindiging van de uitbestedingsovereenkomst blijven de verplichtingen onverminderd van kracht en verleent de dienstverlener medewerking om de persoonsgegevens over te dragen of te vernietigen en te verklaren of aan te tonen dat dit ook daadwerkelijk gebeurd is.
Verwerkingsdoel	De verwerker verwerkt persoonsgegevens uitsluitend ten behoeve en volgens instructie van de verwerkingsverantwoordelijke.	Opnemen bepaling dat de verwerker de persoonsgegevens niet voor eigen doeleinden mag gebruiken.
Belangrijke verplichtingen	De dienstverlener (verwerker) volgt de instructies van de opdrachtgever op en de opdrachtgever bepaalt doel en middelen, daarom is het goed om het volgende vast te leggen: - Alleen verwerken ten behoeve van de afgesproken activiteiten en werkzaamheden - Kosteloos toegang verlenen tot persoonsgegevens - Overdracht persoonsgegevens - Beveiligingsmaatregelen (technische en organisatorische) - Sub-verwerkers - Informeren - Doorgifte van persoonsgegevens - Geheimhouding - Controle - Aansprakelijkheid	De dienstverlener mag de persoonsgegevens niet overdragen, tenzij noodzakelijk voor de uitvoering van de uitbestedingsovereenkomst, tenzij expliciet anders bepaald of uitdrukkelijk na toestemming. De dienstverlener treft technische en organisatorische maatregelen en informeert verwerkersverantwoordelijke hierover als die erom verzoekt. Alleen met toestemming van de opdrachtgever, waarbij de bepalingen uit de overeenkomst ook gelden voor de sub-verwerkers. Een verzoek van een overheidsinstantie mag een dienstverlener niet zelf beantwoorden, tenzij wettelijk verplicht. Het verzoek tot informatie en/of de informatieverstrekking moet direct gemeld worden. Ook als een klant beroep doet op één van de rechten moet gemeld worden welke informatie is verstrekt. Verwerking van persoonsgegeven buiten de EER is in beginsel verboden, tenzij uitdrukkelijk toestemming is gegeven. Bij verwerking buiten de EER moet de dienstverlening nog steeds aantoonbaar voldoen aan de vereisten van doorgifte zoals die gelden in de AVG. Alleen geautoriseerde medewerkers of mensen in opdracht van de dienstverlener mogen gegevens verwerken. De dienstverlener moet medewerking verlenen aan controles en tekortkomingen binnen een te bepalen tijd verhelpen, en anders is het een reden om de overeenkomst te ontbinden. De dienstverlener kan zich niet vrijwaren van schending of niet-nakomen van zijn aansprakelijkheid.
Meldplicht datalekken	De volgende afspraken in geval van een datalek bij de dienstverlener zijn vastgelegd: - Onverwijld melden, uiterlijk 48 uur	Naast de afspraken ook in de overeenkomst opnemen welke informatie gedeeld moet worden hoe de procedure en wat de contactgegevens zijn.

	- Medewerking verlenen - Maatregelen om (verdere) schade te voorkomen - Niet (tijdig) melden betekent vergoeden van de boete	
Wet- en regelgeving	De overeenkomst bevat een artikel dat de partij voldoet aan de geldende wet- en regelgeving en dat het Nederlands recht toepasselijk is. Bovendien is vastgelegd in welke rechtbank geschillen behandeld worden Bij wijziging van wet- en regelgeving kan de verwerkersovereenkomst eenzijdig aangepast worden.	
Begrippen	De volgende begrippen hebben de betekenis zoals deze is gedefinieerd in de Verordening 2016/679 (algemene verordening gegevensbescherming en worden met deze betekenis in de verwerkersovereenkomst gebruikt.	• persoonsgegevens • betrokkene • bijzondere persoonsgegevens • verwerking • beperken van de verwerking • profilering • pseudonimisering • bestand • verwerkingsverantwoordelijke • verwerker • ontvanger • derde • toestemming • inbreuk in verband met Persoonsgegevens • gegevens over gezondheid • hoofdvestiging • vertegenwoordiger • onderneming • concern • toezichthoudende autoriteit • betrokken toezichthoudende autoriteit • grensoverschrijdende verwerking En eventueel nog de volgende aanvulling: “diensten” Alle diensten die de Verwerker aan Verwerkingsverantwoordelijke verleent, zoals omschreven in de Hoofdovereenkomst; “Sub-Verwerker” Een partij die door Verwerker wordt ingeschakeld voor de uitvoering van (een deel van) de Hoofdovereenkomst en de daarbij horende verwerking.

Vertrouwelijkheid	Vertrouwelijkheid van medewerkers. Bijvoorbeeld door geheimhouding op te nemen en hoe deze geldt.	Verwerker waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden.
Passende technische en organisatorische maatregelen	Verwerker moet passende technische en organisatorische maatregelen treffen voor de beveiliging van de persoonsgegevens en de verwerkingsverantwoordelijke hierover informeren als hij hierom verzoekt.	Voorkeur is een algemene bepaling met een bijlage met meer specifieke technische en organisatorische maatregelen die dienen te worden genomen door de verwerker. Certificaten (bijv. ISO) kunnen een goede basis zijn om de beveiliging te waarborgen, scope kan echter groter zijn.
Subverwerkers	Subverwerkers mogen alleen worden ingeschakeld na voorafgaande toestemming van de verwerkingsverantwoordelijke, waarbij de bepalingen uit de overeenkomst ook gelden voor de subverwerkers.	
Bijstand bij AVG verplichtingen	Verwerker verleent de verwerkingsverantwoordelijke bijstand bij het nakomen van AVG verplichtingen.	
Schoning	Verwerker past schoning toe op basis van de wettelijke bewaartermijnen. Verwerker wist na afloop van de verwerkingsdiensten alle persoonsgegevens zoals door de verwerkingsverantwoordelijke wordt verzocht.	Tenzij opslag van de persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht.
Informatieplicht	Verwerker stelt alle informatie ter beschikking die nodig is om de nakoming van verplichtingen aan te tonen, bijvoorbeeld via een audit. Verwerker informeert verantwoordelijke wanneer het verwerkingsdoel veranderd.	
Overige verplichtingen	Naast bovengenoemde verplichtingen, verdient het aanbeveling om de volgende onderwerpen op te nemen in de verwerkersovereenkomst: - Overdracht persoonsgegevens -	- De dienstverlener mag de persoonsgegevens niet overdragen, tenzij noodzakelijk voor de uitvoering van de uitbestedingsovereenkomst, tenzij expliciet anders bepaald of uitdrukkelijk na toestemming.

	- Doorgifte van persoonsgegevens - Autorisaties - Controle - Aansprakelijkheid	Een verzoek van een overheidsinstantie mag een dienstverlener niet zelf beantwoorden, tenzij wettelijk verplicht. Het verzoek tot informatie en/of de informatieverstrekking moet direct gemeld worden. Ook als een klant beroep doet op één van de rechten moet gemeld worden welke informatie is verstrekt. - Verwerking van persoonsgegeven buiten de EER is in beginsel verboden, tenzij uitdrukkelijk toestemming is gegeven. Bij verwerking buiten de EER moet de dienstverlening nog steeds aantoonbaar voldoen aan de vereisten van doorgifte zoals die gelden in de AVG. - Alleen geautoriseerde medewerkers of mensen in opdracht van de dienstverlener mogen gegevens verwerken. - De dienstverlener moet medewerking verlenen aan controles en tekortkomingen binnen een te bepalen tijd verhelpen, en anders is het een reden om de overeenkomst te ontbinden. - De dienstverlener kan zich niet vrijwaren van schending of niet-nakomen van zijn aansprakelijkheid.

3.5 Definitie uitbesteding

Volgens de DNB handreiking SBA-ORM definities en artikel 1 lid 1 Wft wordt onder uitbesteden verstaan:

het door een financiële onderneming verlenen van een opdracht aan een derde tot het ten behoeve van die financiële onderneming verrichten van werkzaamheden:

a. die deel uitmaken van of voortvloeien uit het uitoefenen van haar bedrijf of het verlenen van financiële diensten; of

b. die deel uitmaken van de wezenlijke bedrijfsprocessen ter ondersteuning daarvan;

Het is niet altijd duidelijk wanneer sprake is van (onder)uitbesteding van wezenlijke (kritieke en belangrijke) processen. Er is in ieder geval sprake van kritieke of belangrijke (onder)uitbesteding als de uitbestede activiteiten tijdelijk of permanent uitvallen en dit leidt tot ongewenste risico's voor de klant/bemiddelaar/gevolmachtigd agent/verzekeraar. Of werkzaamheden kritiek of belangrijk zijn hangt af van de complexiteit en omvang van de volmacht en de impact van de (onder)uitbesteding op de bedrijfsvoering. Het is aan de gevolmachtigde om te bepalen of werkzaamheden kritiek of belangrijk zijn. Als een volmacht werkzaamheden uitbesteedt is vanuit het oogpunt van een maatschappij sprake van onder uitbesteding.

Bij uitbesteding is niet van belang wie de leverancier is; het gaat om de vraag om welke activiteit of dienst het gaat. Als één andere partij de activiteit of dienst uitvoert met andere partijen, moet bij degene aan wie (primair) wordt uitbesteed getoetst worden dat de onder uitbesteding aan dezelfde richtlijnen voldoet.

Gevolmachtigden kunnen voor de beoordeling of een uitbesteding kritiek of belangrijk is de volgende criteria of vragen hanteren:

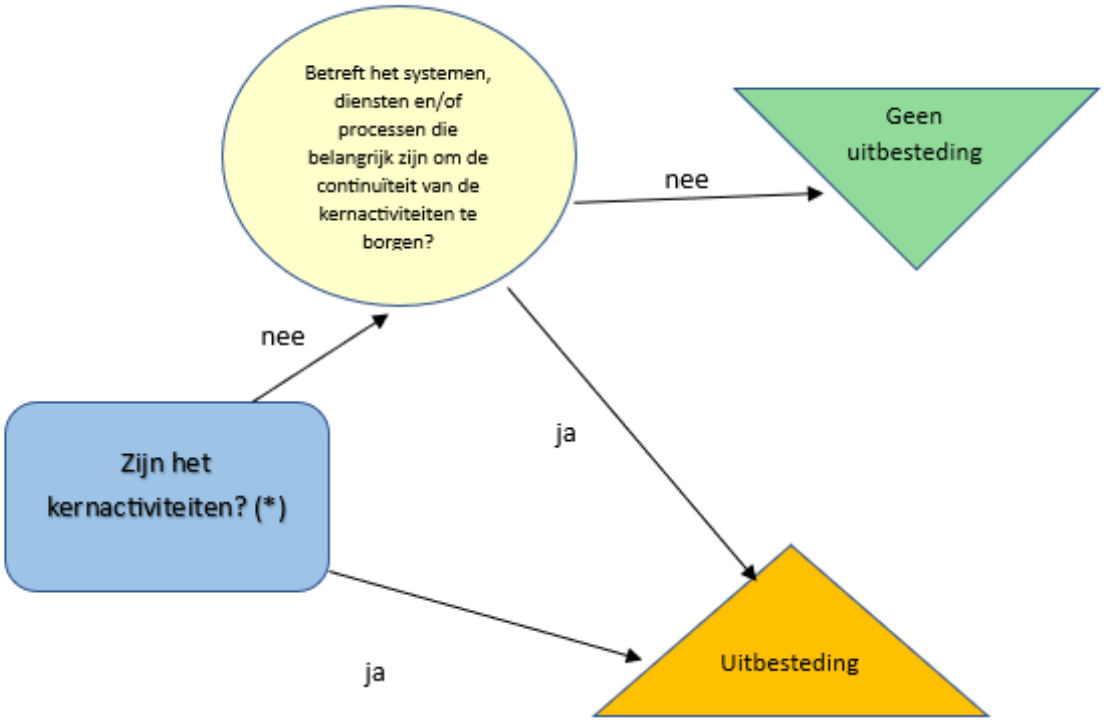
- In hoeverre is de uitbestede activiteit essentieel voor de bedrijfscontinuïteit, bedrijfsvoering en levensvatbaarheid van uw onderneming. Hierbij kunt u de vraag stellen, of het voor uw onderneming mogelijk is om aan de verplichtingen aan klanten te voldoen, zonder deze activiteit

- Wat is het directe operationele effect van onderbrekingen van de uitbestede activiteit en wat zijn de hiermee gepaard gaande juridische, operationele en reputatierisico's.
- Wat is het effect op uw kernactiviteiten en de verwachte inkomsten van uw onderneming bij verstoring van de uitbestede activiteit
- Wat zijn de gevolgen van een schending van de vertrouwelijkheid, integriteit of beschikbaarheid van de gegevens voor uw onderneming en de klanten van uw onderneming.

Ook als er sprake is van het gebruik van specifieke software of tooling kunnen de hulpvragen gebruikt worden. Op het moment dat de tool uitvalt, om wat voor reden dan ook, loopt de bedrijfsvoering dan door of stokt het proces? Kunt u dezelfde dienstverlening aan uw klanten verlenen als de tool uitvalt? Voldoet u nog aan uw verplichtingen? Als u deze vragen met nee heeft beantwoord, kunt u ervan uitgaan dat het (onder)uitbesteding is.

Door de NVGA is onderstaande beslisboom uitbesteding opgesteld, die als handvat kan dienen om te bepalen of er wel of geen sprake is van uitbesteding van kernactiviteiten:

Op basis van deze beslisboom heeft een Werkgroep met vertegenwoordigers van NVGA en Verbond van Verzekeraars een aantal praktijk situaties uitgewerkt, waarbij is aangegeven of wel of juist geen sprake is van uitbesteding van kernactiviteiten door de gevolmachtigde:



(*) een kernactiviteit is een activiteit waarbij de beslissingsbevoegdheid van de verzekeraar overgedragen aan de gevolmachtigde, bijvoorbeeld het doen van acceptatie, schadebehandeling en premie-incasso.

Als het gaat om uitbesteding van systemen, diensten en/of processen die belangrijk zijn om de continuïteit van de kernactiviteit te borgen, is het mogelijk dat de GA deze uitbesteding uit efficiency overweging gedaan heeft. Wanneer de GA dan nog wel de mogelijkheid heeft deze uitbesteding eenvoudig ongedaan te maken en de continuïteit van de kernactiviteit zelf, met eigen inzet, te borgen, dient hij dat gemotiveerd aan de verzekeraar aan te geven.

Nr.	Omschrijving	uitkomst conform beslisboom NVGA	speelt omvang een rol?
1	Huur bedrijfspand	Nee	
2	Interieurverzorging	Nee	
3	Verzorging hydrocultuur planten	Nee	
4	Wekelijkse boodschappen	Nee	
5	Platfom as a service	Ja	
6a	Assurantieapplicatie (geheel in eigen huis & beheer)	Nee	
6b	Assurantieapplicatie (maar niet geheel in eigen huis & beheer)	Ja	
7	Datacenter (PAAS toepassing)	Ja	
8	Extra externe back-up	Ja	
9	Glasvezelverbinding	Nee	
10	Internet abonnement	Nee	
11	Feitelijk leider	Nee	
12	Acceptanten	Nee	
13	Polisopmakers	Nee	
14	Schadebehandelaars	Nee	
15	Financieel medewerkers	Nee	
16	Inrichten nieuwe producten	Nee	
17	STP-straat	Ja	
18	Datacenter (STP-straat)	Ja	
19	Extranetten	Nee	
20	Atosi	Nee (verplicht door VG)	
21	Rolls	Ja	
22	VPI	Nee (verplicht door VG)	
23	Verleende volmachten	Nee	
24	Voorlopige dekkingsbevoegdheid TP	Ja	ja
25	Schaderegelingsbevoegdheid TP	Ja	ja
26	Premie incasso TP	Nee	ja
27	Verzenden polisdocumenten en nota's	Ja	
28	Incasso wanbetaling	Nee	ja
29	Financiële administratie (Exact online)	Ja	
30	Digitaal kennisportaal	Nee	
31	Naverrekenen / actualiseren	Nee	
32	CED Connect	Ja	ja
33	Schade expertise	Nee	ja
34	CIS databank	Nee (verplicht door VG)	
35	Volmacht Resultaat Analyse	Nee	
36	Schadebehandeling uitbesteed aan bijv. Dekra/CED	ja	ja

*In onderstaande tabel staan **niet limitatief** enkele concrete voorbeelden*

Back-up via een server in eigen pand	Als een volmacht een server in het eigen pand heeft ten behoeve van back-ups en deze server onderhouden wordt door iemand die in dienst is van de volmacht, is dit geen uitbesteding.
Online back-up via een IT bedrijf	Een online back-up via een IT bedrijf gebeurt vrijwel altijd op een server in data-centra. Dit valt onder (onder)uitbesteding.
Systeem in 'eigen huis'	Als een softwareleverancier alleen programmatuur levert en verder geen diensten verricht, is er geen sprake van (onder)uitbesteding.
Systeem in de cloud	Een softwareleverancier levert programmatuur via de cloud en beheert uw gegevens op een server in data-centra. Dit valt onder (onder)uitbesteding. In geval van software die u heeft aangekocht en in uw eigen cloud-omgeving installeert valt de cloud-omgeving onder (onder)uitbesteding. De aangekochte software echter niet.
Verzenddiensten	Verzenddiensten vallen onder uitbesteding. Ondanks het feit dat een volmacht bij een verstoring in een verzenddienst altijd kan terugvallen op fysieke postverzending, heeft dit impact op de bedrijfsvoering. De volmacht had hier immers geen mensen voor ingepland qua tijd en uren.
24/7 telefonische opvang	Maakt u gebruik van een eigen 24/7 telefonische opvang? Dan is het belangrijk om na te gaan wat de dienstverlening inhoudt. Als de uitbestedingspartner persoonsgegevens van klanten kan inzien of bewerken, dan wordt dit als (onder)uitbesteding gezien.
Vergelijkings-, offerte-, wijzigings-, of beëindigingstool	Verschillende bedrijven bieden als software een tool aan die bepaalde werkzaamheden overneemt. Deze tools kennen vaak een koppeling met de rekenboxen of het eigen systeem. Deze tools kunnen deel uitmaken van de wezenlijke bedrijfsprocessen in uw bedrijfsvoering. Indien bij uitval van de tool het proces stokt, u niet meer dezelfde dienstverlening kunt verlenen of niet meer kan voldoen aan uw verplichten, kunt u ervan uitgaan dat het (onder)uitbesteding is.
Automatische schadeafhandeling	Een claims engine werkt, via STP (Straight Through Processing), bulkschades geautomatiseerd af. De claims engine neemt de behandeling van een schade gedeeltelijk of volledig geautomatiseerd over. Het ligt eraan of de software gedownload is en in eigen beheer is van de volmacht. Als dit het geval is, dan is er geen sprake van (onder)uitbesteding. Staat de claimprogrammatuur van de dienstverlener in een cloud-omgeving en worden uw gegevens op een server in een datacentrum beheerd. Dan valt dit wel onder (onder)uitbesteding.