VERBOND VAN VERZEKERAARS

NVGA

LEIDRAAD IT-RISICO'S VOLMACHT

TOELICHTING MET HANDVATTEN VOOR DE NEDERLANDSE VOLMACHTMARKT I.V.M. WET- EN REGELGEVING OVER INFORMATIEBEVEILIGING, DE GOOD PRACTICE INFORMATIEBEVEILIGING VAN DNB EN DE PRINCIPES VOOR INFORMATIEBEVEILIGING VAN AFM

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 instelling en de complexiteit van haar 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.

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 niet in overeenstemming is met het interne beleid als gevolg van onderuitbesteding door de dienstverlener.

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 klant. Klanten moeten namelijk kunnen vertrouwen op passende dienstverlening. Bovendien moeten ondernemingen integer en vertrouwelijk met hun gegevens omgaan. De AFM verwacht daarom dat ondernemingen zorgvuldig omgaan met informatiebeveiligingsrisico's.

De regelgeving kent open normen waardoor iedere verzekeraar een eigen beleid heeft 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 geborgd is in het Werkprogramma Risicobeheersing.

In dit document leest u welke beheersingsmaatregelen een gevolmachtigde zou kunnen treffen gericht op technologie, menselijk handelen, inrichting van processen en faciliteiten. Daarnaast staat 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.

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 deze leidraad is beschreven. Per onderdeel kunnen er door verzekeraars specifieke eisen gesteld worden waar de gevolmachtigde zich aan moet houden. Zo kan het bijvoorbeeld zijn dat de ene verzekeraar striktere eisen aan de technologische beveiliging stelt dan een andere verzekeraar. Desondanks biedt deze leidraad u voldoende houvast om uw IT-beveiliging 'Good practice proof' / 'AFM-principes-proof' te maken. Raadpleeg uw contactpersoon bij de verzekeraar voor eventueel maatschappij-specifiek beleid.

Pagina **1** van **16**

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 terugkomen. Binnen het gestelde in artikel 2.7 van de VSV maakt de gevolmachtigde zelf een keuze voor eventuele samenwerking met leveranciers. De set voorwaarden geeft de gevolmachtigde handvatten bij het vastleggen van de samenwerking. Het geeft de verzekeraar ook een instrument bij de beoordeling van het verzoek van de gevolmachtigde om goedkeuring te geven aan de (onder)uitbesteding.

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, de Good Practice Beheersing volmachten schadeverzekeraars van DNB, de Good Practice Uitbesteding Verzekeraars van DNB, de Good Practice informatiebeveiliging van DNB en de Principes voor Informatiebeveiliging van AFM.

Voor meer informatie over IT-beveiliging verwijzen wij u naar de documentatie van DNB, AFM en het Verbond van Verzekeraars, of uw volmachtgever.

INHOUD

1. TECHNOLOGIE EN CONTINUE TOETSING

Informatiebeveiliging en cybersecurity krijgen mede vorm door het treffen van technische maatregelen. Het gaat dan om maatregelen die betrekking hebben op de IT-infrastructuur, data, systemen en applicaties van de gevolmachtigde. Daarnaast wordt de organisatie op strategisch, tactisch en operationeel niveau aangestuurd, waarbij rekening wordt gehouden met informatiebeveiliging. Informatiebeveiliging is dynamisch. Technologie en bedreigingsfactoren ontwikkelen zich continu. Daarmee ontstaan nieuwe risico's. De gevolmachtigde actualiseert daarom haar risicobeoordeling periodiek op basis van inzicht in de voor de onderneming relevante dreigingen op het gebied van informatiebeveiliging. Een manier om inzicht in bestaande risico's te krijgen is door de effectiviteit van de risicobeheersingsmaatregelen te toetsen, uitgaande van bestaande dreigingen. Zowel interne als externe bronnen kunnen van toegevoegde waarde zijn in het bepalen van deze dreigingen.
Bij de implementatie en het onderhoud van systemen wordt het uitgangspunt 'secure by design' toegepast.

Steeds geldt het uitgangspunt dat de te nemen maatregelen/aanpassingen in verhouding staan tot de risico's voor de GA en volmachtgever

Relevante beheersingsmaatregelen
De gevolmachtigde heeft technische beheersingsmaatregelen zodanig ingericht dat zij een hoog niveau van beschikbaarheid, exclusiviteit en integriteit waarborgen. Daarbij houden risico-analyses van de gevolmachtigde rekening met actuele cyberdreigingen. Het onderhoud aan de IT-infrastructuur en IT-applicaties verloopt planmatig en gestructureerd, in lijn met de change management procedures. Security updates worden tijdig toegepast en de gevolmachtigde heeft in beeld van welke IT-infrastructuur en IT-applicaties de bedrijfsprocessen afhankelijk zijn en in hoeverre de IT-systemen kwetsbaar zijn voor cyberaanvallen. De gevolmachtigde heeft zowel preventieve, detecterende als corrigerende maatregelen geïmplementeerd om IT-systemen te beschermen tegen cyberaanvallen. De gevolmachtigde stelt informatiebeveiligingsbeleid op en draagt dit uit binnen de organisatie. Taken en verantwoordelijkheden zijn belegd en formele rapportagelijnen zijn zichtbaar ingericht volgens het informatiebeveiligingsplan. En bedrijfsprocessen en IT-systemen zijn opgezet volgens een door de gevolmachtigde vastgestelde informatiearchitectuur.

Samenvatting thema's waar maatregelen getroffen moeten worden
1. Up-to-date IT-infrastructuur, applicaties en systemen, die periodiek worden geanalyseerd.
2. Toegepast beleid ten aanzien van het plaatsen van patches/updates.
3. Informatiebeveiligingsbeleid met een beveiligingsplan, met verantwoordelijkheden en architectuur.
4. Naleving wetgeving zoals AVG (GDPR).
5. Roadmap (planning) voor het vernieuwen van hardware en programmatuur.
6. Periodiek overleg met leveranciers of (externe) deskundigen over risico's, incidenten, beveiliging en security IT omgeving.

2. MENSELIJK HANDELEN EN ORGANISATIE INRICHTING

De menselijke factor is zeer bepalend voor de beheersing van de informatiebeveiliging en cybersecurity risico's. De gevolmachtigde onderkent het risico van menselijk handelen voor informatiebeveiliging en creëert en ondersteunt een cultuur waarin medewerkers zich bewust zijn van het risico op informatiebeveiligingsincidenten en hierover open communiceren. Het is belangrijk dat alle medewerkers, externe inhuur en dienstverleners bekend zijn met het informatiebeveiligingsbeleid van de gevolmachtigde, hun verantwoordelijkheden kennen en kunnen werken volgens dit beleid. De taken ten aanzien van informatiebeveiliging zijn eenduidig belegd en in overeenstemming met de strategie en het beleid. De gevolmachtigde is verantwoordelijk voor de informatiebeveiliging van uitbestede processen en systemen. Waarbij de gevolmachtigde in deze situaties in staat wordt gesteld om periodiek te (laten) toetsten of de uitvoering van de uitbesteding ook voldoet.

Relevante beheersingsmaatregelen
Medewerkers met kennis van informatiebeveiliging en cybersecurity die aansluit bij de ambitie en het risico van de gevolmachtigde worden gescreend, aangetrokken en behouden. De gevolmachtigde investeert in het op peil houden van het kennisniveau en de competenties van de medewerkers door middel van opleidingen en trainingen. Basiskennis van informatiebeveiliging en cyberdreigingen wordt binnen en buiten de organisatie gedeeld.
De rollen en verantwoordelijkheden zijn geformaliseerd en gedocumenteerd en belegd op alle niveaus in de organisatie. Door middel van toegangsrechten is de toegang tot gegevens en informatiesystemen beheerst. De autorisaties van medewerkers passen bij de werkzaamheden, ook bij functiewijzigingen. En er wordt voor gezorgd dat de gevolmachtigde niet te afhankelijk is van één of enkele individuen met specifieke kennis.

Denk hierbij aan
Het hebben en houden van voldoende personeel met benodigde kennis. Waarbij de kennis van het personeel wordt bijgehouden en gedeeld. Bijhouden van de kennis betekent dat medewerkers trainingen volgen voor onder andere phising, spam, malware en spyware.

Natuurlijk kan het IT-beheer zijn uitbesteed. Dan moet de uitbesteding kwalitatief beoordeeld worden. Bijvoorbeeld door middel van periodiek overleg over de performance en relevante ontwikkelingen, het (laten) uitvoeren van een audit of een ISO verklaring. De verklaring zelf hoeft niet per se iets te zeggen over de kwaliteit. Een verklaring moet wel aan de beheersdoelstellingen voldoen die nodig zijn. En er moet rekening worden gehouden met bijvoorbeeld de scope, de periode en de kwaliteit van de auditorganisatie.

En tot slot heeft het personeel passende autorisaties en toegangsrechten volgens een autorisatiematrix en wachtwoordbeleid. En beschikt de organisatie over procedures, waaronder voor inrichting/toekennen rechten bij nieuwe medewerkers en voor het verwijderen van rechten bij uitdiensttreding van medewerkers, en zijn de accounts tot een individu herleidbaar. Om de gevolgen van een cyberaanval beheersbaar te houden kan een cyberverzekering hier een oplossing voor zijn.

Hou bij een ISO verklaring rekening met:
1. Periode van geldigheid; komt de periode overeen met de gewenste en afgesproken periode?
2. Auditorganisatie; is de reputatie van de auditorganisatie voldoende?

3. Scope; komt de scope in de verklaring overeen met de afgenomen dienstverlening door gevolmachtigde?
4. Onderaannemers; wordt er gebruik gemaakt van onderaannemers? Vallen deze in de scope van de verklaring. Zo niet wat zijn dan de beheersmaatregelen en welke evidence kan worden overlegd?
5. Beheersdoelstellingen; geven de in de verklaring opgenomen beheerdoelstellingen voldoende zekerheid met betrekking tot de diensten die aan de gevolmachtigde worden geleverd?
6. Bevindingen; is de impact van de bevindingen acceptabel? Welke vervolgmaatregelen zijn noodzakelijk?

3. INRICHTING VAN PROCESSEN EN FACILITEITEN

Processen geven richting aan een beheerste bedrijfsvoering en zijn noodzakelijk bij de beheersing van de risico's op het gebied van informatiebeveiliging en cybersecurity. Daarnaast wordt uitgegaan van fysieke beveiliging van toegang tot informatie, zoals kantoorgebouwen en datacenters. De inrichting van bedrijfsprocessen waarborgt de beschikbaarheid, integriteit en vertrouwelijkheid van processen en de hierin gebruikte systemen. Het ontwerp en de inrichting van de faciliteiten en apparatuur van de gevolmachtigde is in lijn met de eisen aan informatiebeveiliging. Verder past de gevolmachtigde een integrale ketenbenadering toe bij het bepalen van informatiebeveiligingsrisico's en de benodigde beheersmaatregelen.

Relevante beheersingsmaatregelen
De gevolmachtigde is voorbereid op informatiebeveiligingsincidenten om de impact hiervan op de bedrijfsvoering van de onderneming te beperken. Wanneer zich een informatiebeveiligingsincident voordoet, neemt de gevolmachtigde tijdig en doeltreffende respons- en herstelmaatregelen. De gevolmachtigde heeft een IT-continuïteitsplan ontwikkeld en houdt dit bij, met als doel de impact van een verstoring te beperken en de beveiligingsfuncties ongestoord voort te zetten. Naast beperken van de impact wordt herhaling zoveel mogelijk voorkomen. Het plan bestaat uit geformaliseerd beleid voor incidentenbeheer met escalatieprocedure en -criteria. Verder heeft de gevolmachtigde een beheerste wijze van doorvoeren van wijzigingen, met een testplan en goedkeuringsproces en een adequate registratie van de doorgevoerde wijzigingen.
Naast de processen is er beleid gedefinieerd en geïmplementeerd als het gaat om de toegang tot en de beveiliging van kantoorgebouwen, terreinen en IT-infrastructuur locaties. Maar ook de toegang tot de beveiligingssystemen zelf en controle op de effectiviteit van de maatregelen.

Denk hierbij aan
1. Een geïmplementeerd IT-continuïteitsplan
2. Inclusief incidentenbeheer en wijzigingsbeleid
3. En fysieke beveiliging van gebouwen, terreinen en locaties
4. Een goed back-up beleid
a. Inclusief recovery beleid
b. Inclusief recovery test
    i. Maandelijks deel recovery
    ii. Jaarlijks full-recovery
5. Procedure inrichting/toekennen rechten bij nieuwe medewerkers
6. Procedure verwijderen rechten bij uit dienst gaan medewerkers
7. Het hebben van een calamiteiten plan (zie NVGA-checklist), denk daarbij onder andere aan
    a. Brand
    b. Inbraak
    c. Aanrijding
    d. Wateroverlast
    e. Stroomuitval
    f. Internetuitval
    g. Pandemie
8. Het uit (laten) voeren van testen op de security (Penetratie test door een ethisch hacker of een periodieke scan door een gespecialiseerd bedrijf)

9. Procedure wijzigingsbeheer applicaties, waaronder een procedure inregeling nieuwe of aangepaste premie en polisvoorwaarden, provisie en volmachtbeloning
10. Waarborgen voor beschikbaarheid, integriteit en vertrouwelijkheid van data en informatie gedurende de volledige levenscyclus van data (opslag, gebruik en transport van data via communicatiekanalen).
11. Het hebben van een cyberverzekering
12. Het hebben van een procedure datalekken
13. Het hebben van een register datalekken
14. Het hebben van een IT incidenten procedure
15. Het hebben van een IT incidenten register

4. UITBESTEDING

4.1 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 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.

*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.

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	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 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. Voorbeeld 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 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	Misverstanden worden voorkomen door bijvoorbeeld een toestemmingsvereiste bij veranderingen en duidelijke omschrijving van de werkzaamheden behorend bij de prijzen.

	- Wijze en termijnen van facturatie en betaling - Btw	
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 - Servicecomponenten en kritische prestatie indicatoren - Service- en onderhoud afspraken - Prioriteiten incidenten - Overlegstructuur - Rapportage en informatieverplichtingen - Right to audit - Onderzoeksrecht nationale en Europese toezichthouder - Escalatie	Opmerking Vastlegging prestaties en afspraken bij voorkeur in een Service Level Agreement.

Verwerkersovereenkomst		
Uitgangspunt	De verwerkersovereenkomsten van de maatschappijen is een goed uitgangspunt. In de overeenkomst staan in ieder geval verwijzingen naar de AVG.	
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.
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) - Subverwerkers - 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 subverwerkers. 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 - Medewerking verlenen - Maatregelen om (verdere) schade te voorkomen - Niet (tijdig) melden betekent vergoeden van de boete	Naast de afspraken ook in de overeenkomst opnemen welke informatie gedeeld moet worden hoe de procedure en wat de contactgegevens zijn.

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; ’Subverwerker‘ Een partij die door Verwerker wordt ingeschakeld voor de uitvoering van (een deel van) de Hoofdovereenkomst en de daarbij horende verwerking.

4.2 Definitie uitbesteding

Het is niet altijd duidelijk wanneer sprake is van (onder)uitbesteding van 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 volmacht om te bepalen of werkzaamheden kritiek of belangrijk zijn. Als een volmacht werkzaamheden uitbesteedt is vanuit het oogpunt van een maatschappij sprake van onderuitbesteding.

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 onderuitbesteding 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.

*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.