JNPG Aanvullende Dekking Cyber Eigen Schade
Bijzondere Voorwaarden HDI CYB.ADD.1

Deze voorwaarden gelden in aanvulling op de beroepsaansprakelijkheidsvoorwaarden:

1 DEFINITIES

In deze polis wordt verstaan onder:

1.1 Bedrijfsschade

De vermindering van de brutowinst die rechtstreeks voortvloeit uit de onderbreking of belemmering van de gebruiksmogelijkheid van gegevens en/of software. Onder brutowinst wordt verstaan de vaste lasten vermeerderd met de nettowinst respectievelijk verminderd met het nettoverlies. Dit is gelijk aan de opbrengst uit de bedrijfsactiviteiten, verminderd met de variabele kosten.

1.2 Betrokkenen

a. de natuurlijke personen op wie de door een privacy incident getroffen persoonsgegevens betrekking hebben.
b. derden die zijn getroffen door een vertrouwelijkheidsincident.

1.3 Cyberincident

a. een privacy incident en/of;
b. een vertrouwelijkheidsincident en/of;
c. een netwerkbeveiligingsincident.

1.4 Derden

Iedereen met uitzondering van verzekerde en haar medewerkers.

1.5 Eigen risicotermijn

De eerste 12 uren na het eerste optreden van de onderbreking of belemmering van de technische gebruiksmogelijkheid van gegevens en software waarbinnen verzekerde de bedrijfsschade zelf draagt.

1.6 Extra kosten

De redelijke en noodzakelijke kosten van verzekerde, uitgezonderd vaste kosten, die worden gemaakt om bedrijfsschade te voorkomen of te beperken.

1.7 Gegevens

Gedigitaliseerde informatie die voor bedrijfsmatig gebruik noodzakelijk is. Onder gegevens wordt ten aanzien van een privacy incident en/of een vertrouwelijkheidsincident tevens fysieke informatie die voor bedrijfsmatig gebruik noodzakelijk is verstaan.

1.8 Hardware

Hardware omvat alle technische, fysiek aanwezige apparatuur van een computersysteem of netwerk waaronder begrepen maar niet beperkt tot: servers, routers, switches, computers, tablets, smartphones, printers en bekabeling.

1.9 Privacy incident

a. de onbevoegde openbaarmaking, verlies van en/of (vermoedelijke) onbevoegde toegang tot, persoonsgegevens waarvoor verzekerde verantwoordelijk is;
b. het verzamelen, verwerken, gebruiken van persoonsgegevens door verzekerde welke in strijd is met de Wet Bescherming Persoonsgegevens (WBP) of andere van toepassing zijnde binnen- of buitenlandse wettelijke regelingen inzake gegevensbescherming en/of gegevensverwerking;
c. het niet voldoen aan een wettelijke meldplicht ten aanzien van gegevensverlies.

1.10 Netwerkbeveiligingsincident

Een inbreuk op de netwerkbeveiliging door:

a. de verzending van malware waardoor de op de IT-infrastructuur aanwezige gegevens of software zijn verwijderd, veranderd of de toegang hiertoe is belemmerd, of heeft geleid tot een verstoring van de werking van de IT-infrastructuur;
b. een Denial-of-Service-aanval op de IT-infrastructuur;
c. de ongeautoriseerde binnendringing door derden van de IT-infrastructuur (hacking);
d. een onbevoegde verandering of verwijdering van op de IT-infrastructuur opgeslagen gegevens;
e. verlies en/of diefstal door derden van gegevensdragers van verzekerde waarop persoonsgegevens en/of vertrouwelijke gegevens van derden zijn opgeslagen;
f. de onbevoegde verkrijging of publicatie van toegangscodes van verzekerde;
g. de onbevoegde verhindering van de toegang van verzekerde tot de IT-infrastructuur.

1.11 IT-infrastructuur

Alle hardware, software, netwerkcomponenten, telecommunicatienetwerken en websites die bediend en/of beheerd worden door verzekerde.

1.12 Kredietmonitoringdiensten

Dienstverlening die er op is gericht om via het monitoren van financiële transacties financiële schade van betrokkenen als gevolg van identiteitsdiefstal te voorkomen.

1.13 Malware

Software die is ontwikkeld met het doel computerprogramma's, bestanden en/of calculaties te beschadigen, verstoren of op een andere manier nadelig te beïnvloeden, waaronder begrepen maar niet beperkt tot trojans, logic bombs, wormen en ransomware.

1.14 Persoonsgegevens

Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

1.15 Regelgevingsboete

Boetes die aan verzekerde door een toezichthouder zijn opgelegd in verband met een privacy incident.

1.16 Vertrouwelijkheidsincident

Een onbevoegde openbaarmaking en/of het verlies van zakelijke gegevens van derden waarop een wettelijke, of contractuele geheimhoudingsplicht rust.

1.17 Toezichthouder

Een (semi-)overheidsorgaan dat is belast met het toezicht op de verwerking en/of bescherming van persoonsgegevens.

1.18 Uitkeringstermijn

De op het polisblad weergegeven termijn waarvoor dekking voor de bedrijfsschade bestaat. De uitkeringstermijn begint na afloop van de eigen risicotermijn.

1.19 Verzekerde

Verzekeringnemer en/of overige op het polisblad vermelde meeverzekerde juridische entiteiten.

2 DEKKING

2.1 Omschrijving van de dekking

Verzekerd zijn de onder artikel 2.2 t/m 2.9 vermelde schade redelijke en noodzakelijke kosten van verzekerde als gevolg van een in het desbetreffende artikel beschreven verzekerde gebeurtenis die voor het eerst plaatsvindt tijdens de contracttermijn.

2.1.2 Eigen risico
Voor deze dekking is een eigen risico van toepassing zoals aangegeven op het polisblad.

2.2 IT-Forensisch onderzoek en incident response

2.2.1 Verzekerde gebeurtenis
De ontdekking van een cyberincident.

2.2.2 Vergoeding van kosten
Verzekeraars vergoeden de honoraria en kosten van IT-beveiligingsexperts voor:

a. IT-forensisch onderzoek om vast te stellen of er sprake is van een cyberincident, en waardoor deze werd veroorzaakt;
b. het coördineren van het cyberincident;
c. het doen van aanbevelingen als reactie op het cyberincident waaronder het voorkomen van nieuwe cyberincidenten.

2.3 Meldingskosten en juridisch advies

2.3.1 Verzekerde gebeurtenis
De ontdekking van een privacy incident en/of een vertrouwelijkheidsincident.

2.3.2 Vergoeding van kosten
Verzekeraars vergoeden:

a. de kosten voor het inlichten van betrokkenen en instanties voor gegevensbescherming.
   Onder kosten worden begrepen maar niet beperkt tot:
   - identificatie en het achterhalen van contactgegevens van de getroffen personen en/of organisaties
   - 'call center' kosten
   - verzendkosten
   - kosten voor het plaatsen van nieuwsberichten, mededelingen en advertenties in de media.
b. de kosten voor juridisch advies met betrekking tot de verzekerde gebeurtenis inclusief de beoordeling of er sprake is van een wettelijke meldplicht

2.3.3 Goedkeuring verzekeraars
Voor de kosten zoals vermeld onder artikel 2.3.2 sub a geldt dat uitdrukkelijke goedkeuring van verzekeraars is vereist indien er geen wettelijke meldplicht van toepassing is.

2.4 Public relations in geval van een crisis

2.4.1 Verzekerde gebeurtenis
Een feitelijk of beweerd cyberincident, dat met grote waarschijnlijkheid een aanzienlijke aantasting van de reputatie van verzekerde tot gevolg heeft.

2.4.2 Vergoeding van kosten
Verzekeraars vergoeden de honoraria en kosten van een PR-adviesbureau voor het opstellen en uitvoeren van een PR-strategie voor beheersing van de crisis en het behoud en/of herstel van de reputatie tot maximaal 20 dagen na de verzekerde gebeurtenis. Voor het inschakelen van de PR-adviseur is voorafgaande toestemming vereist van verzekeraars.

2.5 Kredietmonitoringdiensten

2.5.1 Verzekerde gebeurtenis
De ontdekking van een privacy incident.

2.5.2 Vergoeding van kosten
Verzekeraars vergoeden de kosten van kredietmonitoringdiensten en identiteitsdiefstalverzekeringen die verzekerde aan betrokkenen dient aan te bieden en/of te vergoeden.

2.5.3 Goedkeuring verzekeraars
Indien er geen sprake is van een wettelijke verplichting of een verplichting op grond van voorschriften van een toezichthouder, is voor vergoeding van de kosten uitdrukkelijke goedkeuring van verzekeraars vereist.

2.5.4 De kosten zullen worden vergoed tot maximaal één jaar na aanvang van de verzekerde gebeurtenis.

2.6 Herstel van gegevens en/of software

2.6.1 Verzekerde gebeurtenis
De ontdekking van een netwerkbeveiligingsincident.

2.6.2 Vergoeding van kosten

Verzekeraars vergoeden de gemaakte kosten (waaronder overuren van eigen medewerkers):

a. voor de vaststelling of gegevens en/of software die zich op de IT-infrastructuur van verzekerde bevonden, hersteld, opnieuw ingevoerd of opnieuw verzameld kunnen worden;
b. voor het herstel van de vroegere operationele toestand van gegevens, software en websites voor zover herstel mogelijk is.

Onder herstelkosten worden onder andere verstaan de noodzakelijke en redelijke kosten voor:

- het terugzetten van gegevens vanuit back-up systemen;
- het vervangen, opnieuw invoeren, of herstellen van gegevens inclusief het opstellen van daarvoor vereiste bewijsstukken;
- het vervangen, aanschaffen en opnieuw installeren van software

2.7 Regelgevingsboetes

2.7.1 Verzekerde gebeurtenis

Een aan verzekerde opgelegde regelgevingsboete.

2.7.2 Vergoeding van schade

Verzekeraars vergoeden:

a. de regelgevingsboete die aan verzekerde zijn opgelegd, doch uitsluitend voor zover deze:
   - op grond van het toepasselijke recht rechtmatig verzekerbaar zijn;
   - niet zijn gebaseerd op opzettelijk handelen of nalaten van de directie of het bestuur van verzekerde.
b. de kosten van verweer om zich tegen de boete te verdedigen

2.8 Bedrijfsschade

2.8.1 Verzekerde gebeurtenis

Een onderbreking of belemmering van de gebruiksmogelijkheid van gegevens en/of software als gevolg van een:

- inbreuk op de netwerkbeveiliging die leidt tot een verwijdering, wijziging en/of niet beschikbaarheid van gegevens en/of software
- een IT-forensisch onderzoek in het kader van artikel 2.2 uitgevoerd met toestemming van verzekeraars;
- een onmiddellijk bevel tot staking van de bedrijfsactiviteiten afkomstig van een toezichthouder in verband met een privacy incident

2.8.2 Vergoeding van schade en kosten

Verzekeraars vergoeden de:

a. bedrijfsschade die gedurende de uitkeringstermijn optreedt;
b. extra kosten, hiervoor geldt een sublimiet van EUR 10.000,00 per verzekerde gebeurtenis.

2.8.3 Berekening van de schadevergoeding

Bij de vaststelling van de bedrijfsschade moet rekening worden gehouden met:

a. alle omstandigheden die de bedrijfsvoering en het bedrijfsresultaat tijdens de onderbrekingsperiode gunstig of ongunstig zouden hebben beïnvloed, wanneer de onderbreking niet zou zijn opgetreden.
b. economische voordelen als gevolg van de onderbreking en/of belemmering die na het optreden van de bedrijfsschade doch binnen de uitkeringstermijn ontstaan.

2.9 Hacking van de telefooncentrale

2.9.1 Verzekerde gebeurtenis

De ontdekking van een netwerkbeveiligingsincident waarbij door derden onrechtmatig toegang is verkregen tot het telefoonnetwerk van verzekerde.

2.9.2 Vergoeding van kosten

Verzekeraars vergoeden de telefoonkosten van verzekerde die buiten de macht van verzekerde zijn gemaakt als direct gevolg van een verzekerde gebeurtenis.

2.9.3 Sublimiet

Voor deze dekking geld een sublimiet van EUR 10.000,00 per contractjaar.

3 UITSLUITINGEN

In aanvulling op de uitsluitingen zoals opgenomen in de beroepsaansprakelijkheidsvoorwaarden is van dekking uitgesloten, schade en/of kosten die voortvloeien uit en/of verband houden met:

3.1 Storingen / onderbrekingen

Elke vorm van onderbreking of storing van infrastructurele voorzieningen zoals:
- stroom-, gas-, olievoorzieningen;
- internetverbindingen;
- kabelverbindingen;
- satellieten;
- telecommunicatienetwerken,

doch uitsluitend voor zover de oorzaken van de onderbreking of storing niet in de macht liggen van verzekerde.

3.2 Overheidsmaatregelen

Een maatregel opgelegd door een (semi) overheidsinstelling, behalve zover gedekt onder artikel 2.7 regelgevingsboetes.

3.3 Herstel van gegevens en software

Ten aanzien van artikel 2.6:
a. geplande uitschakelingen van het netwerk;
b. de introductie van nieuwe IT-processen, IT-infrastructuur of software;
c. gebreken die bij afsluiting van de verzekering reeds aanwezig waren en waarmee verzekerde wordt verondersteld bekend te zijn geweest.

3.4 Bedrijfsschade

Ten aanzien van artikel 2.8:
a. gebreken of onderbrekingen van de IT-infrastructuur van derden en buiten de macht liggen van verzekerde
b. winsten en kosten die niet met het productie-, handels- of industrieel bedrijf samenhangen, en buiten de eigenlijke bedrijfsdoelstelling worden behaald (bijv. door kapitaaltransacties of transacties met onroerend goed) of ontstaan;
c. boete of schadevergoeding aan derden, contractueel of uit anderen hoofde verschuldigd
d. de onmogelijkheid om de IT-infrastructuur van verzekerde te koppelen aan IT-infrastructuur van derden behalve als dit veroorzaakt wordt door een inbreuk op de netwerkbeveiliging.

3.5 Boetes

Boetes gebaseerd op enig civiel recht en/of strafrecht, behalve zover deze gedekt zijn onder artikel 2.8.

3.6 Octrooien/patenten/bedrijfsgeheimen

Inbreuken op het octrooi- en/of patentrecht en/of de schending van bedrijfsgeheimen en/of andere schade als gevolg van het verlies van octrooieer- en/of patenteerbaarheid.

3.7 Licenties

Licenties, inclusief de betaling van licentiekosten. Deze uitsluiting geldt niet voor kosten voor aanschaf van vernieuwde licenties die in aanvulling op artikel 2.6 zijn ontstaan omdat verzekerde gegevens en/of software waren beveiligd tegen onbevoegd kopiëren of onbevoegde toegang.

3.8 Handel, transacties, waardepapieren en effecten

a. handelsverliezen of handelsverplichtingen van verzekeringnemer;
b. verliezen bij foutieve elektronische betaalopdrachten of bestellingen door of namens verzekeringnemer;
c. het aankopen of verkopen van waardepapieren of overige in effecten vastgelegde activa;
d. het onrechtmatig uitvoeren van handelstransacties door verzekeringnemer vanwege een overschrijding van volmachten;

4 VOORWAARDEN VOOR DEKKING

Verzekerde heeft uitsluitend recht op dekking indien is voldaan aan ondergenoemde voorwaarden, behalve voor zover verzekerde aannemelijk maakt dat het niet voldoen aan de voorwaarden geen invloed heeft gehad op de schade, of haar niet toe te rekenen valt:

- er is een gedocumenteerd beleid opgesteld welke regelmatig wordt geactualiseerd ten aanzien van de beveiliging van (persoons)gegevens;
- er is een persoon binnen de organisatie van verzekerde expliciet verantwoordelijk gesteld voor de bescherming van persoonsgegevens;
- verzekerde heeft haar gehele IT-infrastructuur beveiligd met (een) firewall(s) en (een) virusscanner(s) die automatisch word(t)en geüpdatet;
- verzekerde gebruikt passwords voor haar gehele IT-infrastructuur die minimaal 8 tekens en een combinaties van letters, cijfers en hoofdletters dienen te bevatten;
- verzekerde maakt minimaal wekelijks een back up welke buiten de IT-infrastructuur wordt bewaard;
- verzekerde voert tijdig de voor haar werkzaamheden gebruikelijke software updates uit.