

Aanvullende voorwaarden Wijdverspreide incidenten v2.2

Hiermee wordt aangekend dat de polis als volgt wordt gewijzigd:

WIJZIGINGEN VAN DEKKINGSOMSCHRIJVINGEN MET BETREKKING TOT INCIDENTEN MET BEPERKTE OMVANG EN WIJDVERSPREIDE INCIDENTEN

- 1.1 Artikel 1 (Dekkingsomschrijvingen) en artikel 2 (Uitbreidingen) worden gewijzigd door het volgende toe te voegen aan het begin van elk artikel:

Elk **cyberincident, bedrijfsonderbrekingsincident, cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout** kwalificeert als een **incident met beperkte omvang** of een **wijdverspreid incident**.

Voor een **incident met beperkte omvang** bestaat er dekking overeenkomstig de dekkingsomschrijvingen en uitbreidingen en de aanvullende sublimieten zoals vermeld op het polisblad.

Op de dekking voor een **wijdverspreid incident** is een **eigen risico, eigen aandeel** en gesublimeerd verzekerd bedrag per **verzekeringstermijn** van toepassing zoals vermeld onder sublimieten voor **wijdverspreide incidenten** op het polisblad.

DEFINITIES MET BETREKKING TOT INCIDENTEN MET BEPERKTE OMVANG EN WIJDVERSPREIDE INCIDENTEN

- 1.2 De volgende definities worden toegevoegd aan artikel 3 (Definities):

Alle andere wijdverspreide incidenten betekent een **wijdverspreid incident** dat niet voortvloeit uit een **wijdverspreide ernstige bekende kwetsbaarheidexploit, wijdverspreide software supply chain exploit** of **wijdverspreide ernstige zero-day-exploit**.

Bevoegde gebruiker betekent een persoon die door de **verzekerde organisatie** geautoriseerd is om toegang tot het **verzekerd computersysteem** of **gedeeld computersysteem** te hebben.

Data-incident bij een derde betekent:

- A. onrechtmatige of onbevoegde toegang tot, blootstellen, openbaar maken, verlies, wijziging of vernietiging van **persoonsgegevens** en/of vertrouwelijke of bedrijfseigen informatie van een **derde** waarvoor **verzekerde** wettelijk aansprakelijk is voor het waarborgen van vertrouwelijkheid; en/of
- B. datalek zoals gedefinieerd in **privacywetgeving**,
in een **computersysteem** beheerd door een gegevensbeheerder die een **derde** is of een gegevensverwerker die een **derde** is, op grond van een (schriftelijke) overeenkomst met **verzekerde**.

Incident met beperkte omvang betekent een **cyberincident** en/of **bedrijfsonderbrekingsincident** en/of **cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout** dat niet voorkomt uit een **wijdverspreide trigger**.

Groep met beperkte impact betekent een **verzekerde** of een **verzekerde** tezamen met:

- A. een persoon of rechtspersoon die een directe zakelijke relatie met de **verzekerde organisatie** heeft (een 'relatie') en:
- i. die door het **cyberincident, bedrijfsonderbrekingsincident, cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout** getroffen wordt uitsluitend als gevolg van deze relatie; of
- ii. waardoor een **cyberincident, bedrijfsonderbrekingsincident, cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout** voortkomt uitsluitend als gevolg van deze relatie; en/of

- B. een persoon of rechtspersoon die door het **cyberincident**, **bedrijfsonderbrekingsincident**, **cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout** wordt getroffen uitsluitend als gevolg van een directe of indirecte zakelijke relatie met een persoon of rechtspersoon zoals beschreven in onderdeel 2.a. van dit artikel; en/of
- C. uitsluitend met betrekking tot dekkingsomschrijvingen 1.1 (Cyberincident kosten) en 1.5 (Privacy- en netwerkbeveiligingsaansprakelijkheid), betekent een 'getroffen partij,' een persoon of rechtspersoon, die een directe zakelijke relatie met een gegevensbeheerder die een **derde** is heeft, en indien deze gegevensbeheerder een **data-incident bij een derde** ondervindt, op voorwaarde dat dit **data-incident bij een derde** leidt tot:
- i. een **schending geheimhoudingsincident**; en
 - ii. deze getroffen partij vergelijkbare meldingskosten maakt om te voldoen aan **privacywetgeving**.

De handeling, fout, nalatigheid of tekortkoming, of reeks van handelingen, fouten, nalatigheden of tekortkomingen die met elkaar verband houden die een **data-incident bij een derde** vormt of veroorzaakt is beperkt tot een **derde** met een directe zakelijke relatie met een dergelijke gegevensbeheerder.

Schending geheimhoudingsincident betekent een schriftelijke melding door **verzekerde**, aan een natuurlijk persoon, vrijwillig gedaan met voorafgaande toestemming van **verzekeraar** of om aan de meldplicht datalekken van de **privacywetgeving** te voldoen van een daadwerkelijke of vermoedelijke tekortkoming van **verzekerde** of een onafhankelijke contractspartij waarvoor **verzekerde** wettelijk aansprakelijk is, in het correct verwerken, beheren, bewaren, vernietigen, beschermen, gebruiken of op andere wijze beheren van:

- A. **persoonsgegevens** van deze natuurlijke persoon; en/of
- B. vertrouwelijke informatie van deze natuurlijke persoon, op voorwaarde dat deze natuurlijke persoon een **derde** is en dat **verzekerde** wettelijk aansprakelijk is om deze informatie vertrouwelijk te behandelen.

Wijdverspreide ernstige bekende kwetsbaarheidexploit betekent een **wijdverspreide trigger** dat betrekking heeft op de verspreiding van een kwetsbaarheid in software, firmware of hardware, die op het moment van de eerst bekende datum van verspreiding:

- A. is vermeld als een Common Vulnerability en Exposure (CVE) in de National Vulnerability Database beheerd door de National Institute of Standards and Technology (NIST) en het Nationaal Cyber Security Centrum (NCSC); en
- B. die een basisscore of totale score van 8,0 of hoger heeft gekregen volgens het Common Vulnerability Scoring System (CVSS) versie 2.0 of hoger.

Wijdverspreide ernstige zero-day-exploit betekent een **wijdverspreide trigger** die betrekking heeft op de verspreiding van een kwetsbaarheid in software, firmware of hardware, niet zijnde een **wijdverspreide ernstige bekende kwetsbaarheidexploit**, die binnen 45 dagen na melding van een bijbehorend **cyberincident**, **bedrijfsonderbrekingsincident**, **cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout** aan de **verzekeraar**:

- A. als een Common Vulnerability en Exposure (CVE) in de National Vulnerability Database beheerd door de National Institute of Standards and Technology (NIST) en het Nationaal Cyber Security Centrum (NCSC) wordt vermeld; en
- B. een basisscore of totale score van 8,0 of hoger volgens het Common Vulnerability Scoring System (CVSS) versie 2.0 of hoger krijgt.

Wijdverspreid incident betekent een **cyberincident**, **bedrijfsonderbrekingsincident**, **cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout** die voortvloeien uit een **wijdverspreide trigger**.

Wijdverspreide software supply chain exploit betekent een **wijdverspreide trigger** die betrekking heeft op het invoeren van malware, een backdoor of andere kwetsbaarheden in

een **verzekerd computersysteem** of een **gedeeld computersysteem** door middel van het kwaadaardig invoeren van source code in software, firmware of hardware die:

- A. aan meerdere cliënten van de software, firmware of hardware developer is geleverd;
- B. niet specifiek voor één cliënt, inclusief een **verzekerde**, op maat is ontwikkeld; en
- C. als betrouwbaar wordt aangemerkt door een digitaal certificaat, zoals een Software Publisher Certificate (SPC).

Wijdverspreide trigger betekent:

- A. een enkele handeling of reeks van handelingen die met elkaar verband houden, gepleegd door een partij of gecoördineerde partijen buiten de **verzekerde organisatie**; of
- B. een enkele fout, nalatigheid of tekortkoming, of reeks van fouten, nalatigheden of tekortkomingen die met elkaar verband houden, van een persoon of **computersysteem** buiten de **verzekerde organisatie**,

die een **cyberincident**, **bedrijfsonderbrekingsincident**, **cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout** vormt of veroorzaakt, en tevens een incident in een **computersysteem** van een persoon of rechtspersoon buiten de **groep met beperkte impact** vormt of veroorzaakt.

Onder **wijdverspreide trigger** wordt niet verstaan een handeling die tussenliggende, misleidende manipulatie van de handelingen van een **bevoegde gebruiker** vereist om een dergelijk **cyberincident**, **bedrijfsonderbrekingsincident**, **cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout** te vormen of veroorzaken.

WIJZIGINGEN VAN BEPALINGEN MET BETREKKING TOT INCIDENTEN MET BEPERKTE OMVANG EN WIJDVERSPREIDE INCIDENTEN

1.3 Artikel 5.3 (Verzekerde bedragen) onderdeel H is doorgehaald en wordt vervangen door:

- H. Indien een **wijdverspreid incident**, **achterstallige software** of **ransomware** is gedekt op meer dan één dekkingsomschrijving, uitbreiding of sublimiet zal enkel het laagst toepasselijke verzekerde bedrag per **verzekeringstermijn** van toepassing zijn ten behoeve van dergelijk(e) **wijdverspreid incident**, **achterstallige software** of **ransomware** inclusief het van toepassing zijnde **eigen aandeel** en **eigen risico**.

1.4 Aan Artikel 5.3 (Verzekerde bedragen) wordt de volgende bepaling toegevoegd:

Verzekerde bedragen voor incidenten wijdverspreide incidenten

- 1. De wijdverspreide incident sublimieten maken onderdeel uit van, en komen niet bovenop, de toepasselijke verzekerde bedragen per **verzekeringstermijn** vermeld op het polisblad, en geven geen extra dekking onder enige dekkingsomschrijving en/of uitbreiding waarvoor geen verzekerd bedrag per **verzekeringstermijn** is vermeld.
- 2. De wijdverspreide incident sublimieten maken onderdeel uit van het totale verzekerde bedrag per **verzekeringstermijn** vermeld op het polisblad.
- 3. Op gedekte **schade** en/of **kosten** als gevolg van een **serie-aanspraak** die voortvloeit uit een **wijdverspreid incident** is het bijbehorende **eigen risico** en **eigen aandeel** voor een dergelijk **wijdverspreid incident** en de wijdverspreide incident sublimiet van toepassing.

1.5 De volgende bepaling wordt toegevoegd aan artikel 5 (Algemene bepalingen):

Verplichtingen bij een cyberincident, bedrijfsonderbrekingsincident, cyberafpersingsincident en/of privacy- en netwerkbeveiligingsgerelateerde fout

Verzekerde zal alle redelijke maatregelen nemen om schade te beperken, bedrijfsactiviteiten voort te zetten, contractuele rechten en rechtsmiddelen veilig te stellen, eigendommen te beschermen en veilig te stellen, **computersysteem**, logboeken, boekhouding, bestanden, rapporten of bewijzen

(gezamenlijk 'bewijsmiddelen'), die redelijkerwijs noodzakelijk zijn voor het beoordelen van de vaststelling van de **schade** en/of **kosten** als gevolg van een **cyberincident**, **bedrijfsonderbrekingsincident**, **cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout**. Voor zover de **verzekerde** kosten maakt om bewijsmiddelen veilig te stellen, worden deze kosten met de voorafgaande toestemming van **verzekeraar** onder de definitie van **cyberincident kosten** gedekt.

A. BEWIJSVOERING

1. **Verzekerde** zal op verzoek aan **verzekeraar** de volledige gegevens van elk **cyberincident**, **bedrijfsonderbrekingsincident**, **cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout** verstrekken zo spoedig als redelijkerwijs mogelijk nadat deze zaak overeenkomstig artikel 5.10 (Melding) aan de **verzekeraar** is gemeld. Indien verzocht zullen deze gegevens de schriftelijke rapporten van dienstverleners die deelnamen in het onderzoek of de coördinatie van een dergelijke zaak bevatten, inclusief een cyberincident manager ingehuurd om een **cyberincident** en/of **bedrijfsonderbrekingsincident** te coördineren, of schriftelijke rapporten of correspondentie aan of van een opsporingsinstantie, overheidsorgaan, toezichhoudend orgaan van de sector of vergelijkbare entiteit.
2. De bewijsmiddelen geven volledige details van alle bedragen waarvan vergoeding of waarvoor betaling wordt verzocht, en vermelden gedetailleerd hoe deze bedragen zijn berekend en welke aannames zijn gemaakt en omvatten alle bewijzen die de bewijsvoering ondersteunen.
3. **Verzekerde** dient medewerking te geven en alle aanvullende informatie te verstrekken die redelijkerwijs door **verzekeraar** verzocht wordt in het onderzoek van een **cyberincident**, **bedrijfsonderbrekingsincident**, **cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout**, en dient het onderzoek en de controle van alle bewijsmiddelen die relevant zijn voor de vaststelling van een dergelijke zaak door **verzekeraar** toe te staan en te faciliteren, inclusief een verzoek aan externe dienstverleners om informatie namens **verzekeraar**.
4. **Verzekerde** is in geen geval verplicht om informatie aan **verzekeraar** te verstrekken dat specifiek onder een rechterlijk publicatieverbod valt. Zodra een dergelijk publicatieverbod niet langer volledig van kracht is, kan dergelijke informatie door **verzekeraar** worden gevraagd als onderdeel van de bewijsvoering.

B. RECHT OP INZAGE

Verzekeraar of een **derde** die namens **verzekeraar** handelt, heeft het recht maar niet de plicht om de bewijsmiddelen van **verzekerde** relevant voor de afhandeling van de **schade** en/of **kosten** als gevolg van een **cyberincident**, **bedrijfsonderbrekingsincident**, **cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout** te inspecteren, beoordelen en controleren, op voorwaarde dat dit recht op inzage geen erkenning van vergoedingsplicht namens of ten gunste van **verzekerde** vormt. Alle extra kosten met betrekking tot een dergelijke inzage zijn voor rekening van **verzekeraar** en worden niet in mindering gebracht op enige sublimiet, verzekerd bedrag per **verzekeringstermijn** of het totale verzekerde bedrag per **verzekeringstermijn** van deze **polis**.

C. VASTSTELLING EN BETALING VAN SCHADE

1. **Verzekeraar** mag gebruik maken van de bewijsmiddelen en elk onafhankelijk bewijs om te bepalen of een **cyberincident**, **bedrijfsonderbrekingsincident**, **cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout** een **incident met beperkte omvang** of **wijdverspreid incident** vormt. Dergelijk onafhankelijk bewijs kan openbare informatie of niet-openbare informatie verzameld tijdens het onderzoek door **verzekeraar** bevatten, inclusief rapporten van relevante **derden**, zoals overheidsinstanties, dienstverleners of forensische ICT-bedrijven, die het **cyberincident**, **bedrijfsonderbrekingsincident**, **cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout**, inclusief de oorzaak en omvang specificeren of beschrijven. Alle kosten gemaakt om dit onafhankelijk bewijs te verkrijgen zijn voor rekening van **verzekeraar** en worden niet in mindering gebracht op enige sublimiet, verzekerd bedrag per **verzekeringstermijn** of het totale verzekerde bedrag per **verzekeringstermijn** van deze **polis**.

2. **Cyberincident kosten** en **eerste hulp kosten** zijn gedekt respectievelijk onder dekkingsomschrijving 1.1 (Cyberincident kosten) en uitbreiding 2.1 (Eerste hulp kosten) onder de sublimiet en het verzekerde bedrag per **verzekeringstermijn** van toepassing op een **incident met beperkte omvang**, tot het moment dat:

- a. **verzekerde** feiten of bewijs verkrijgt of redelijkerwijs had behoren te verkrijgen, waaruit redelijkerwijs zou blijken dat het **cyberincident, bedrijfsonderbrekingsincident, cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout** een **wijdverspreid incident** is;

of, indien dit eerder is:

- b. de **verzekeraar** vaststelt dat een **cyberincident, bedrijfsonderbrekingsincident, cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout** een **wijdverspreid incident** is gebaseerd op de bewijsmiddelen of ander onafhankelijk bewijs.

Na dit moment worden alle verdere **cyberincident kosten** en/of **eerste hulp kosten** gedekt onder dekkingsomschrijving 1.1 (Cyberincident kosten) en/of dekkingsomschrijving 2.1 (Eerste hulp kosten) onder de sublimiet per **verzekeringstermijn** van toepassing op een **wijdverspreid incident**.

3. Als de **verzekeraar** vaststelt dat het onmogelijk of onpraktisch is om te bepalen of een **cyberincident, bedrijfsonderbrekingsincident, cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout** een **incident met beperkte omvang** of **wijdverspreid incident** vormt, heeft **verzekeraar** het recht, een dergelijke zaak als een **incident met beperkte omvang** te beschouwen en de **aanspraak** op die manier te behandelen.

4. De **verzekeraar** vergoedt gedekte **schade** en/of **kosten** met betrekking tot een **cyberincident, bedrijfsonderbrekingsincident, cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout** na ontvangst van de complete bewijsmiddelen, op voorwaarde dat **verzekerde** aan alle voorwaarden van deze **polis** heeft voldaan en **verzekeraar** en **verzekerde** het eens zijn over het te vergoeden bedrag. Indien relevante informatie onder een rechterlijk publicatieverbod valt, wordt de afwikkeling van **schade** en/of **kosten** als gevolg van een dergelijk **cyberincident, bedrijfsonderbrekingsincident, cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout** opgeschort, en worden de bewijsmiddelen tijdens deze periode als onvolledig beschouwd. Als de **verzekeraar** en **verzekerde** het niet eens worden over het bedrag van de gedekte **schade** en/of **kosten** onder deze **polis**, kan de **verzekeraar** alle onbetwiste bedragen betalen.

D. Indien **verzekerde** ervoor kiest geen bewijsmiddelen aan **verzekeraar** te verstrekken om te bepalen of een **cyberincident, bedrijfsonderbrekingsincident, cyberafpersingsincident** en/of **privacy- en netwerkbeveiligingsgerelateerde fout** een **incident met beperkte omvang** of **wijdverspreid incident** vormt, dan komen **verzekerde** en **verzekeraar** overeen dat een dergelijke zaak een **wijdverspreid incident** wordt beschouwd ten behoeve van dekking onder deze **polis**. Voor de toepassing van paragraaf D wordt de tekortkoming door **verzekerde** om geen bewijsmiddelen te verstrekken niet beschouwd als een schending van de verplichtingen van **verzekerde** onder deze **polis** beschouwd.

WIJZIGINGEN VAN UITSLUITINGEN MET BETREKKING TOT INCIDENTEN MET BEPERKTE OMVANG EN WIJDVERSPREIDE INCIDENTEN

1.6 Aan Uitsluiting 4.9 (Infrastructuur) wordt het volgende toegevoegd

Deze uitsluiting is niet van toepassing op een **Incident met beperkte omvang**.