# Informatie over Cyberhulp

## Cyberhulp is onderdeel van uw inboedelverzekering

## Inhoud

# Wat te doen bij schade?

U denkt dat er is ingebroken op uw computer, u krijgt te maken met ransomware, persoonsgegevens blijken in verkeerde handen gevallen te zijn of iemand maakt gebruik van uw identiteit om een lening te krijgen. Bij dit soort cyberincidenten is het belangrijk dat u zo snel mogelijk in actie komt om de schade te beperken.

### De Cyberhulplijn

Soms merkt u niet direct dat er sprake is van een cyberincident. Maar al bij het vermoeden van cyberincident belt u direct met de Cyberhulplijn. Hier zijn voor u geen kosten aan verbonden.

Een medewerker van de Cyberhulplijn helpt u te bepalen wat er aan de hand is en helpt u de gevolgen van een cyberincident te beperken.

### Inschakelen van een specialist

Is het cyberincident niet opgelost na overleg met de medewerker van de Cyberhulplijn? In dat geval kan een specialist op technisch, juridisch of fraudegebied, worden ingeschakeld om het cyberincident helpen op te lossen.

Hiervoor bent u verzekerd. U betaalt € 100,- zelf, dit noemen we het eigen risico. Alle kosten daarboven krijgt u tot € 5.000,- vergoed. Alleen bij ransomware zijn de kosten van een specialist beperkt tot € 2.500,-. De inzet van een specialist wordt eerst met u overlegd en de inzet van de specialist gebeurt alleen als u hiervoor akkoord geeft. Als de kosten hoger zijn, dan wat u op basis van deze verzekering vergoed krijgt, dan kunt u toch gebruik blijven maken van de specialist. U krijgt dan tijdig een begroting van de nog te verwachten kosten. Deze kosten moet u dan wel zelf betalen aan de specialist.

### Cyberhulp Kennisportaal

U kunt op ieder moment gebruikmaken van het Cyberhulp Kennisportaal. Ons kennisportaal bevat veel tips en informatie over cybercriminaliteit en identiteitsfraude. Wij leggen u uit wat cybercriminaliteit is en hoe u zich hiertegen beschermt. U bezoekt het Cyberhulp Kennisportaal op aon.mycybercentre.com

# Leeswijzer

U heeft bij ons een inboedelverzekering. Op het polisblad van uw inboedelverzekering staat Cyberhulp als een standaard onderdeel van uw inboedelverzekering vermeld. Cyberhulp kent deels eigen polisvoorwaarden. Wij zetten hier de belangrijkste punten uit die voorwaarden op een rij.

Deze verzekering bevat voor u misschien nieuwe woorden op het gebied van cyber. Daarom vindt u van alle woorden in de kleur blauw een uitleg in de begrippenlijst. Deze lijst staat aan het einde van dit document. Ook worden er praktijkvoorbeelden gegeven. Deze staan in blauwe kaders.

# Cyberhulp in het kort

**Waarvoor is Cyberhulp?**
Deze dekking biedt hulp en beschermt u tegen de financiële gevolgen van cyberincidenten.

Uw computer doet niets meer omdat een hacker hem heeft geblokkeerd. Of iemand steelt uw identiteitsgegevens en misbruikt ze voor de aankoop van spullen. Of iemand stelt u aansprakelijk omdat zijn persoonsgegevens, door u, bij onbevoegden terecht kwamen.

Dit zijn cyberincidenten. Met Cyberhulp krijgt u hulp bij vier soorten cyberincidenten: beveiligingsincidenten, privacy-inbreuk, identiteitsfraude en ransomware. Een medewerker van de Cyberhulplijn onderzoekt het incident en helpt het cyberincident zo snel mogelijk op te lossen.

Behalve hulp, vergoedt Cyberhulp ook de schade en/of kosten van specialisten die worden ingezet. Bij elk soort cyberincident staat in de voorwaarden precies aangegeven welke schade en/of kosten van specialisten vergoed worden.

Vaak gebeurt een cyberincident via uw computer. Derden breken dan in op uw computersysteem om er kwaadaardige software op te zetten of om gegevens te stelen. Een privacy-inbreuk of identiteitsfraude kan zich ook voordoen zonder computer. De gegevens staan bijvoorbeeld op papier of op een andere drager. Ook dan biedt Cyberhulp dekking.

Onder een computersysteem vallen meer apparaten dan u misschien denkt. Behalve uw pc, laptop of tablet, zijn uw smartphone, smartwatch en game consoles ook computersystemen. Eigenlijk alle apparaten die met het internet verbonden kunnen worden.

Zakelijke activiteiten zijn niet gedekt en ook niet de gegevens die gebruikt worden voor zakelijke activiteiten. Dus als u uw computersysteem ook gebruikt voor uw werk, dan kunt u geen gebruik maken van de Cyberhulp. Als u als vrijwilliger gegevens verwerkt voor een lokale club, vereniging of liefdadigheidsinstelling, kunt u wel gebruik maken van Cyberhulp.

### Wat te doen bij schade?

- Bel direct de Cyberhulplijn.
- Doe er alles aan om (verdere) schade te voorkomen en te beperken.
- Help mee aan alles wat wij doen om de schade af te handelen.

### Waar bent u bijvoorbeeld voor verzekerd?

- U heeft toegang tot de Cyberhulplijn en het Cyberhulp portaal.
- De kosten voor onderzoek naar het mogelijke cyberincident.
- De kosten die gemaakt worden voor het inschakelen van een specialist.
- De kosten voor het herstellen van uw computersysteem na een cyberincident.
- De schade van derden die u moet betalen door een privacy-inbreuk.
- De kosten om de gevolgen van identiteitsfraude te beperken.

### Waar bent u bijvoorbeeld niet voor verzekerd?

- Schade die ontstaat omdat een oplichter u vraagt een bedrag over te maken, en u doet dit.
- Schade aan het computersysteem zelf.
- Boetes.
- Schade aan personen.
- Schade en kosten die ontstaan omdat u de in voorwaarden genoemde beveiligingsmaatregelen niet gebruikt.
- Schade en kosten doordat het systeem van een ander niet of niet goed werkt, zoals internet-, telecom- of nutsbedrijven.
- Schade en kosten omdat u het computersysteem zakelijk gebruikt of er zakelijke data op heeft staan.

## Wat krijgt u vergoed?

Bij elk (vermoeden van een) incident krijgt u kosteloos hulp van een medewerker van de Cyberhulplijn. Als een medewerker het cyberincident niet kan oplossen, wordt een specialist ingeschakeld. In dat geval worden de schade en kosten vergoed die per incident opgenoemd staan in de polisvoorwaarden.

## Wat betaalt u zelf?

Als u slechts gebruik heeft gemaakt van de Cyberhulplijn betaalt u niets. In alle andere gevallen betaalt u € 100,- per cyberincident. Dit noemen we het eigen risico.

## Wie zijn er verzekerd?

Wie er zijn verzekerd staat in de polisvoorwaarden van uw inboedelverzekering. Meestal zijn dit u en uw inwonende gezinsleden met wie u in gezinsverband samenwoont.

Aan deze Leeswijzer kunt u geen rechten ontlenen. In de Voorwaarden Cyberhulp staat precies waarvoor u wel en niet verzekerd bent, op welke dienstverlening u kunt rekenen en wat uw rechten en plichten zijn. Lees de Voorwaarden Cyberhulp zorgvuldig door.

# Voorwaarden Cyberhulp

2023-12

Deze voorwaarden Cyberhulp vormen één geheel met de voorwaarden van uw inboedelverzekering. Op het polisblad van uw inboedelverzekering staat Cyberhulp als een standaard onderdeel van uw inboedelverzekering vermeld. In de voorwaarden van uw inboedelverzekering staan ook de algemene bepalingen voor bijvoorbeeld premiebetaling, opzegging en herziening van tarieven. Als er verschillen zijn, gelden de polisvoorwaarden Cyberhulp.

Lees de voorwaarden Cyberhulp zorgvuldig door. Hierin staat wat uw rechten en plichten zijn en wat wel en niet verzekerd is.

## Inhoudsopgave

## 1. Dekkingsoverzicht

De Cyberhulp biedt dekking tot maximaal de verzekerde bedragen die in dit dekkingsoverzicht staan. Verzekeraar vergoedt niet meer dan maximaal het verzekerde bedrag van EUR 5.000 per jaar, voor alle in artikel 2 omschreven schades en kosten tezamen.

| | |
|---|---|
| **1. Eigen risico** | |
| U heeft een eigen risico per cyberincident van | € 100,- |
| **2. Het maximale verzekerd bedrag per jaar** | **€ 5.000,-** |
| Binnen het maximaal verzekerd bedrag is | |
| - gemist loon ( zie 2.1.3) gemaximeerd tot | 20 dagen en € 250,- per dag en € 2.500,- per jaar |
| - ransomware ( zie 2.1.4) gemaximeerd tot | € 2.500,- per jaar |

**3. De verzekerde periode**

De looptijd van de Cyberhulp voorwaarden is gelijk aan en onlosmakelijk verbonden met de looptijd van uw inboedelverzekering.

**4. Dekkingsgebied**

De gehele wereld, met uitzondering voor aanspraken uit de USA en Canada.

## 2. Wat is verzekerd?

U bent verzekerd voor de in dit artikel genoemde schade en kosten. Het incident en de daaruit volgende schade en kosten moeten zijn ontstaan en gemeld tijdens de verzekerde periode. Heeft u te maken met een cyberincident? Meld dit dan zo snel mogelijk bij de Cyberhulplijn.

### 2.1.1 Schade door een privacy-inbreuk.

Onder privacy-inbreuk verstaan we de diefstal van persoonsgegevens door onbevoegden die geen verzekerde zijn of verlies van persoonsgegevens die u als particulier verwerkt, bezit of beheert. De persoonsgegevens kunnen op uw computersysteem of op papier staan. Betrokken personen, van wie de persoonsgegevens zijn gelekt, kunnen schade leiden omdat hun persoonsgegevens nu openbaar zijn. Betrokkenen kunnen proberen deze schade op u te verhalen.

U organiseert een feest en heeft de namen en adressen van alle gasten opgeschreven. U laat deze lijst per ongeluk in de trein liggen, waardoor de gegevens in handen van derden komen.

Hoewel uw gasten nog geen schade hebben geleden, wilt u weten wat u nu moet doen om de gevolgen van deze privacy-inbreuk te beperken. Moet u uw gasten informeren? Hoe doet u dat het beste? Een specialist adviseert u nu wat u het beste kunt doen

De persoonsgegevens moeten: (a) in uw directe zorg, bewaring en controle zijn of (b) in de zorg, bewaring of controle van een provider waarmee u een schriftelijke overeenkomst heeft, waarin die partij zich verplicht om voor u alle schade en kosten te betalen die het gevolg zijn van een privacy-inbreuk.

Het volgende wordt vergoed:

- Kosten van een computerspecialist om te onderzoeken welke persoonsgegevens zijn ingezien door onbevoegden;
- Kosten voor een specialist, die u adviseert over wat u het beste kan doen, in het geval van een privacy-inbreuk;
- De advocaatkosten en griffierechten voor het onderzoek en de verdediging in rechtszaken, die tegen u zijn aangespannen door betrokken personen;
- Schade van betrokken personen die het gevolg is van een privacy-inbreuk en die u verplicht bent te betalen.

### 2.1.2 Schade door een beveiligingsincident

Onder een beveiligingsincident wordt verstaan:

- Het falen van bestaande technische of fysieke beveiligingsmaatregelen van uw computersysteem, om te voorkomen dat onbevoegden toegang tot uw computersysteem krijgen;
- Een Denial of Service aanval (DoS attack);
- Fysieke diefstal of verlies van uw computersysteem, waardoor onbevoegden toegang tot data krijgen;
- Overdracht van kwaadaardige codering (malicious code) van uw computersysteem naar het computersysteem van een derde waardoor schade kan ontstaan.

Uw computer wordt gehackt en uw foto's worden gestolen en gebruikt op websites waar u niet wilt dat ze op staan. U wilt de computer zo snel mogelijk afsluiten voor de hacker. De verzekeraar zal, na uw melding bij Cyberhulp, een IT-specialist inschakelen die u hierbij kan helpen.

Uw computer wordt gehackt en er wordt malware op geplaatst, waardoor uw contacten uit uw naam e-mails ontvangen, met het verzoek om zo snel mogelijk geld over te maken. U wilt uw computer zo snel mogelijk weer malware vrij krijgen en uw contacten waarschuwen. De door de verzekeraar ingeschakelde specialist zal u hierbij, na uw melding bij Cyberhulp, helpen. Ook zult u advies krijgen over wat u het beste kunt doen om uw contacten te waarschuwen.

Uw telefoon wordt uit uw tas gestolen en ondanks dat u die beveiligd heeft met een sterk wachtwoord, heeft een onbevoegde toegang gekregen tot uw data. Een door de verzekeraar ingeschakelde specialist kan, na uw melding, onderzoeken waar de dief allemaal toegang toe heeft gekregen en wat er nu het beste kan worden gedaan.

Het volgende wordt vergoed:

- Aanspraken van derden die het gevolg zijn van een beveiligingsincident en die u verplicht bent te betalen;
- Kosten voor de hulp van een specialist. In dit geval is dat een IT-deskundige die u helpt vast te stellen of er sprake is van een

beveiligingsincident. Als dit het geval is zal de specialist u helpen, om het computersysteem, voor zover mogelijk, in de staat te herstellen van voor het incident;
- De advocaatkosten en griffierechten voor het onderzoek en de verdediging in rechtszaken, die tegen u zijn aangespannen door derden, die door het beveiligingsincident schade hebben geleden;

**Let op**: Bij diefstal van een computersysteem wordt de schade aan of de waarde van het gestolen computersysteem zelf niet vergoed.

### 2.1.3 Schade door identiteitsfraude

Onder identiteitsfraude wordt verstaan: een gebeurtenis waarbij onbevoegden uw persoons- en of identificatiegegevens misbruiken. De identiteitsgegevens kunnen afkomstig zijn van uw computersysteem, papier of andere media.

U ontvangt een rekening voor spullen, die u via het internet zou hebben gekocht. Deze spullen zijn niet door u, maar door iemand gekocht die uw identiteit heeft misbruikt. U belt direct de Cyberhulplijn. Maar de schuldeiser heeft weinig geduld en stuurt een dagvaarding. U zal moeten bewijzen dat u niets besteld heeft, want anders moet u de rekening betalen. U krijgt daarbij hulp van een specialist. Ook de kosten van de procedure worden betaald tot het verzekerd bedrag. Daarnaast zal moeten worden onderzocht of uw identiteit misschien ook nog voor andere zaken is misbruikt. Een IT-specialist zal uw computersysteem onderzoeken en de beveiliging herstellen. Een specialist zal zorgen voor alle officiële verklaringen en berichten aan toezichthoudende instanties en financiële ondernemingen.

U wilt een vliegreis gaan maken, maar bij de douane wordt u tegengehouden, omdat u nog diverse verkeersboetes niet zou hebben betaald. Deze overtredingen zijn gemaakt door iemand die uw identiteit heeft gestolen en auto's op uw naam heeft gehuurd. U meldt dit direct de Cyberhulplijn. U bent dagen bezig om met hulp van een specialist bewijs te verzamelen dat u de overtredingen niet heeft gemaakt. Uw werkgever geeft u daarom onbetaald verlof. De kosten van de specialisten en het gemiste loon worden tot het verzekerd bedrag door de verzekering vergoed.

Het volgende wordt vergoed:

*A. Kosten documenten*
De noodzakelijke kosten voor notariële verklaringen of soortgelijke documenten om aan toezichthoudende instanties, financiële of kredietverlenende ondernemingen of kredietbeoordelaars te bewijzen dat er identiteitsfraude is gepleegd.

*B. Advocaatkosten*
De advocaatkosten en griffierechten voor:

- Het onderzoek en de verdediging in rechtszaken die tegen u zijn aangespannen, door personen of organisaties die een lening hebben verstrekt aan een derde, die uw identiteit frauduleus heeft gebruikt;

- Het aanvechten van gerechtelijke uitspraken, waarbij onterecht een vordering tegen u is toegewezen, als gevolg van het feit dat onbevoegden uw identiteit frauduleus (heeft) gebruikt;

- Het controleren van de juistheid of volledigheid van uw BKR-gegevens, naar aanleiding van het frauduleus gebruik van uw identiteit.

*C. Gemist loon*
Gemist loon tot een maximum van 20 dagen en tot maximaal € 250,- per dag en tot maximaal € 2.500,- per jaar.

D. Kosten aanvraag lening
Kosten voor het door u opnieuw aanvragen van een lening, als de oorspronkelijke aanvraag door de kredietverstrekker is afgewezen, op basis van onjuiste informatie als gevolg van de identiteitsfraude.

*E. Telefoonkosten*
De telefoonkosten om een identiteitsfraude te melden en te bespreken met bedrijven, wetshandhavingsinstanties, financiële instellingen, kredietverstrekkers, of kredietrapportagebureaus;

*F. Kosten voor identiteitsherstel*
Kosten van een fraudespecialist die u helpt bij het herstel van uw identiteit. De fraudespecialist helpt u om de geregistreerde informatie bij financiële ondernemingen, kredietverstrekkers, organisaties voor kredietregistratie,

incassobureaus of overheidsinstellingen te herstellen, in de staat zoals die was vlak voor de identiteitsfraude en voor zover dit mogelijk is.

U maakt zelf de keuze of u hulp wilt bij identiteitsherstel. U moet bij hulp dan wel:

1. verklaren aan de verzekeraar dat u slachtoffer van fraude bent geworden en
2. bij de politie aangifte doen van de identiteitsfraude.

De in A tot en met F genoemde vergoedingen zijn in tijd gemaximeerd tot 12 maanden na de dag waarop de identiteitsfraude voor het eerst heeft plaatsgevonden.

### 2.1.4 Kosten voor hulp bij ransomware

Onder ransomware wordt verstaan: Een kwaadaardige codering die ervoor zorgt dat u uw computersysteem geheel of gedeeltelijk niet meer kunt gebruiken.

Uw computer is besmet met ransomware waardoor u uw documenten niet meer kunt openen. U kunt bijvoorbeeld niet meer bij uw vakantiefoto's. Of u krijgt helemaal geen toegang meer tot uw computer. U belt de Cyberhulplijn. Een medewerker van de Cyberhulplijn helpt u de ransomware van uw computer te verwijderen, zodat u weer bij uw gegevens kunt.

Het volgende wordt vergoed:

Wanneer u te maken krijgt met ransomware op uw computersysteem, krijgt u hulp van een computerspecialist die zal proberen om de ransomware van uw computersysteem te verwijderen en de systeemfunctionaliteit te herstellen, zodat u weer toegang heeft tot uw computersysteem. De hulp kan telefonisch of bij een computerspecialist worden aangeboden. Als het niet mogelijk is om de ransomware te verwijderen en u over een back-up beschikt, kan de computerspecialist proberen hiermee uw computersysteem te herstellen. Dit gebeurt alleen na uw uitdrukkelijke toestemming.

### 2.2 Onderling met elkaar verband houdende cyberincidenten

Als meerdere incidenten met elkaar verband houden, dan worden deze gezien als één cyberincident. Het ene incident kan het gevolg zijn van het andere, of de incidenten kunnen dezelfde oorzaak hebben. Bijvoorbeeld als er identiteitsfraude plaatsvindt als gevolg van een beveiligingsincident. De datum van het eerste cyberincident is bepalend voor de dekking.

## 3. Wat is niet verzekerd?

In sommige gevallen bent u niet verzekerd voor de schade en kosten voor specialisten. Dat noemen we uitsluitingen.

### Uitsluitingen

3.1.1 Verlies, diefstal of beschadiging van uw computersysteem.

3.1.2 Losgeld.

3.1.3. Wettelijke of contractuele opgelegde boetes, straffen of maatregelen of vergoeding ter compensatie.

3.1.4 Belastingen.

3.1.5 Schade van de volgende (rechts-) personen:

a. Schade geleden door een rechtspersoon waarvan u (deels) eigenaar bent of waarin u een belang heeft;
b. Schade geleden door een rechtspersoon waar u werkzaam bent of werkzaamheden voor verricht;
c. Aanspraken van verzekerden onderling.

3.1.6 Schade of kosten die verband houdt met:

a) Zakelijk gebruik van uw computersysteem of zakelijke data die op uw computersysteem staan.
b) Het niet voldoen aan de beveiligingsmaatregelen genoemd in artikel 5.2
c) Lichamelijk of geestelijk letsel, ziekte of overlijden van een persoon;
d) Uw faillissement of surseance van betaling
e) Enige contractuele aansprakelijkheid of verplichting;
f) Schending van enig auteursrecht, handelsmerk, octrooi of ander intellectueel eigendomsrecht, of inbreuk, publicatie of misbruik van enig handelsgeheim;
g) Handelsverliezen, handelsverplichtingen of verandering van waarde van rekeningen, elk verlies, overdracht of diefstal van geldmiddelen of roerende zaken van anderen die aan uw zorg, bewaring of zeggenschap zijn toevertrouwd;
h) Diefstal, verlies, beschadiging of waardevermindering van geldmiddelen waaronder e-valuta (zoals bitcoins), effecten, beleggingen of investeringen;

i) Een frauduleuze instructie aan een financiële instelling om geldmiddelen over te boeken van uw rekening (geld- of overschrijvingsfraude);

j) Social engineering fraude;

k) Opzet, fraude, grove schuld of bewuste roekeloosheid van u of een medeverzekerde, al dan niet in groepsverband.

l) Het recht dat geldt in de USA/Canada.

3.1.7 Schade of kosten door een daadwerkelijke of vermeende storing, onderbreking of afsluiting:
- van nutsvoorzieningen;
- telecommunicatie;
- van andere infrastructuurvoorzieningen ondersteund door het internet. Bijvoorbeeld diensten van uw internetprovider die uw website of internettoegang beheert.

3.1.8 Schade, of kosten die verband houden met:

a. Brand, rook, explosie, elektromagnetische velden, bliksem, wind, overstroming, oppervlaktewater, aardbeving, vulkanische uitbarsting, vloedgolf, aardverschuivingen, hagel, andere natuurrampen of elk ander fysiek voorval, op welke manier dan ook veroorzaakt;
b. Overspanning of inductie;
c. het gebruik van locatie gebaseerde diensten of locatie gebaseerde gegevens, zoals GPS en locatie gebaseerde applicaties of media;
d. Terrorisme.

3.1.9 Schade, aansprakelijkheid of kosten die verband houden met molest

3.1.10 Schade of kosten die is/zijn gedekt op een andere verzekering, of gedekt zou zijn, indien deze verzekering niet zou hebben bestaan.

3.1.11 Schade en kosten als gevolg van een cyberincident dat bij het ingaan van de verzekering al bekend was, of redelijkerwijs kon worden voorzien.

## 4. Wie betaalt wat?

U denkt dat er sprake is van een cyberincident en belt de Cyberhulplijn. Dan worden de kosten voor de medewerker, die u helpt, volledig vergoed door de verzekeraar. U heeft geen eigen risico en de gemaakte kosten voor deze dienstverlening tellen niet mee voor de berekening van het totaal aan vergoedingen per jaar. Het maximaal verzekerde bedrag is hier dus niet van belang, u mag zo vaak bellen als u wilt.

Als een medewerker van de Cyberhulplijn uw cyberincident niet kan oplossen, kan een specialist worden ingeschakeld. Voordat een specialist wordt ingeschakeld, zal de verzekeraar u informeren over de werkzaamheden en de kosten. Alleen als u toestemming geeft voor de werkzaamheden, zullen deze worden uitgevoerd.

Er dan geldt dan wel een eigen risico. U krijgt daarvoor een rekening van de specialist. De verzekeraar vergoedt dan de kosten boven het eigen risico aan de specialist, tot maximaal de verzekerde bedragen en termijnen zoals genoemd in het dekkingsoverzicht Cyberhulp.

Als verwacht wordt dat de kosten hoger zijn dan het verzekerd bedrag, geeft de verzekeraar dit op tijd aan. U krijgt dan ook te horen wat deze hogere te verwachte kosten zijn. U kunt dan kiezen of u nog gebruik wilt blijven maken van de specialist, wanneer de verzekeraar de kosten niet meer vergoedt. Als u van de specialist gebruik wilt blijven maken, moet u hierover zelf afspraken met hem maken en u moet hem rechtstreeks betalen.

## 5. Wat zijn uw verplichtingen?

U heeft een aantal verplichtingen om de schade zo beperkt mogelijk te houden. Houdt u zich niet aan de één van deze hier genoemde verplichtingen, dan kan de verzekeraar een uitkering weigeren of verminderen.

### 5.1

Als er sprake is van een cyberincident moet u:

- Dit zo snel mogelijk melden bij de Cyberhulplijn;

- Alle informatie geven over wat er is gebeurd en alle informatie geven die nodig kan zijn om uw melding te beoordelen;
- Volledig meewerken aan de behandeling van de schade en het verhalen van de schade op de veroorzaker en niets doen wat de belangen van verzekeraar kan schaden;
- Geen aansprakelijkheid erkennen, betalingen doen, verplichtingen aangaan, kosten maken of een schikking treffen zonder toestemming van verzekeraar.

5.2

U moet aan de volgende beveiligingsmaatregelen voldoen:

- Pas het door de leverancier standaard of vooraf ingestelde of meegeleverde wachtwoord direct aan;
- Maak gebruik van een sterk wachtwoord of een ander sterk beveiligingsprotocol, zoals een vingerafdruk, om toegang te krijgen tot elk apparaat dat op het internet kan worden aangesloten. Deze verplichting geldt alleen voor zover het apparaat de mogelijkheid heeft om een sterk wachtwoord of een ander beveiligingsprotocol in te stellen;
- Deel uw wachtwoorden niet met anderen en bewaar ze niet vlakbij bij uw computer;
- Maak gebruik van redelijke beveiligingsoplossingen: Installeer antivirus en anti-spyware software en firewalls op pc's en laptops en vernieuw deze zodra er een update is, bewaar en verstuur gegevens veilig;
- Gebruik geen computersysteem met een jailbreak. Met het installeren van een jailbreak worden de door de fabrikant ingebouwde systeembeveiligingen van het computersysteem omzeild;
- Laat uw computersysteem en documenten niet onbeheerd achter in een openbare ruimte;
- Gebruik uw computersysteem niet voor het peer to peer delen van bestanden;
- Als u een smartphone of tabletcomputer gebruikt voor bankzaken, moet u de mobiele bank-app van uw bank of financiële instelling gebruiken. Dus bijvoorbeeld niet het web-interface van uw bank.

5.3

U gaat akkoord met het gebruik van een computerspecialist die door de verzekeraar is ingeschakeld. U kunt ook zelf een computerspecialist inhuren, maar alleen na schriftelijke toestemming van de verzekeraar.

5.4

U gaat ermee akkoord dat de verzekeraar namens u een advocaat inschakelt, voor de verdediging in rechtszaken die tegen u zijn aangespannen , als de kosten binnen de dekking en het verzekerd bedrag vallen.

5.5

U gaat ermee akkoord, dat de verzekeraar namens u, een schade rechtstreeks met een derde kan regelen en aan de derde kan uitkeren, als de schade binnen de dekking en het verzekerd bedrag valt.

## 6. Algemene bepalingen

Hieronder treft u de Algemene bepalingen aan voor Cyberhulp. De voorwaarden Cyberhulp vormen één geheel met de voorwaarden van uw inboedelverzekering. In de voorwaarden van uw inboedelverzekering staan ook de algemene bepalingen voor bijvoorbeeld premiebetaling, opzegging en herziening van tarieven. Als er verschillen zijn, gelden de polisvoorwaarden Cyberhulp.

### 6.1 Looptijd & opzegging

De looptijd van deze Cyberhulp is gelijk aan de looptijd van uw inboedelverzekering. Opzegging van Cyberhulp geschiedt door middel van opzegging van uw inboedelverzekering conform de hiervoor geldende voorwaarden, waarbij voor verzekerde en verzekeraar gelijke bevoegdheden dienen te worden gehanteerd. Indien er een afwijking bestaat in de polisvoorwaarden van de inboedelverzekering dan heeft verzekerde van Cyberhulp gelijke rechten conform de opzegmogelijkheden van verzekeraar.

### 6.2 Schorsing dekking bij wanbetaling

- Betreft het de aanvangspremie, dan wordt, zonder dat een nadere ingebrekestelling door verzekeraar en/of diens gevolmachtigde is vereist, geen dekking verleend ten aanzien van gebeurtenissen die na het verstrijken van de uiterste betaaltermijn hebben plaatsgevonden.

- Betreft het de vervolgpremie, dan wordt geen dekking verleend ten aanzien van gebeurtenissen die hebben plaatsgevonden vanaf de vijftiende dag nadat verzekeraar en/of diens gevolmachtigde u na het verstrijken van de uiterste betaaltermijn schriftelijk heeft aangemaand en betaling is uitgebleven.
- Indien u weigert de aanvangs- of vervolgpremie te betalen, wordt geen dekking verleend ten aanzien van gebeurtenissen die nadien hebben plaatsgevonden.
- De dekking wordt weer van kracht voor gebeurtenissen die hebben plaatsgevonden na de dag waarop hetgeen u verschuldigd bent voor het geheel door verzekeraar en/of diens gevolmachtigde is ontvangen.

## 6.3 Sanctiewetgeving / opschortende voorwaarde

Toetsing overeenkomstig sanctiewet of regelgeving vindt plaats conform de bepalingen van uw inboedelverzekering.

## 6.4 Opzet

U bent niet verzekerd voor de aansprakelijkheid voor schade die verband houdt met opzettelijk en tegen een persoon of zaak gericht wederrechtelijk handelen of nalaten door:

a) u of een medeverzekerde;
b) een of meer personen die behoren tot een groep personen waartoe ook u of een medeverzekerde persoon behoort. Dit geldt ook als u of uw medeverzekerde niet zelf zodanig heeft gehandeld of nagelaten.

Aan het opzettelijke karakter van het handelen of nalaten door genoemde personen doet niet af of zij zodanig onder invloed van alcohol of enige andere bedwelmende, opwekkende of soortgelijke stof verkeerden, dat zij niet in staat waren hun wil te bepalen.

## 6.5 Persoonsgegevens

6.5.1. Verwerking persoonsgegevens bij aanvraag / wijziging.
Bij de aanvraag van een verzekering of dekking vragen wij persoonsgegevens op. Wij gebruiken deze gegevens om overeenkomsten aan te gaan en uit te voeren, zoals het inschatten van risico's. Daarnaast gebruiken we ze voor fraudebestrijding, statistische analyse en wettelijke verplichtingen. Naast de informatie die wij van u krijgen, kunnen wij hiervoor informatie inwinnen bij andere partijen die wij betrouwbaar vinden. Wij kunnen ook persoonsgegevens raadplegen of laten opnemen bij de Stichting CIS te Den Haag. Hiervoor geldt het

privacyreglement van de Stichting CIS (www.stichtingcis.nl). Kijk voor meer informatie op www.nn.nl/privacy.

6.5.2. Verwerking persoonsgegevens bij schade
Bij een schademelding vragen wij persoonsgegevens op. Wij verwerken deze gegevens om de verzekeringsovereenkomst te kunnen uitvoeren, zoals het inschatten van risico's. Naast de informatie die wij van u krijgen, kunnen wij hiervoor informatie inwinnen bij andere partijen die wij betrouwbaar vinden. Wij raadplegen ook persoonsgegevens en nemen deze op bij de Stichting CIS. Hiervoor geldt het privacyreglement van de Stichting CIS.

6.5.3. Verstrekking persoonsgegevens aan derden
Wij kunnen persoonsgegevens die u ons heeft verstrekt ook ter beschikking stellen aan andere partijen. U kunt hierbij denken aan hulp en dienstverleners, experts en herstelbedrijven.

6.5.4. Toepasselijke gedragscode
Op de verwerking van deze persoonsgegevens is de gedragscode "Verwerking Persoonsgegevens Financiële Instellingen" van toepassing. Deze vindt u op www.verzekeraars.nl.

6.5.5. Toepasselijk recht
Op alle verzekeringsovereenkomsten met ons is Nederlands recht van toepassing.

6.5.6. Heeft u een klacht?
Heeft u een klacht over deze overeenkomst, stuur een brief of email aan: de directie van Aon Nederland, Postbus 518, 3000 AM Rotterdam of info@aon.nl.

Vindt u dat uw klacht niet goed is afgehandeld? Leg dan uw klacht voor aan het Klachteninstituut Financiële Dienstverlening (Kifid), Postbus 93257, 2509 AG Den Haag. Of bel: 0900-355 22 48. Doe dit binnen drie maanden nadat verzekeraars een definitief besluit hebben genomen over uw klacht. Na drie maanden wordt uw klacht door het Kifid niet meer in behandeling genomen. Uiteraard kunt u ook naar de Burgerlijke rechter gaan.

# 7. Begrippenlijst

Hieronder vindt u een uitleg van de in deze voorwaarden gebruikte begrippen.

**BKR-gegevens**
Uw kredietgegevens, zoals persoonlijke leningen, afbetalingsregelingen en betalingsachterstanden die worden vastgelegd door Stichting Bureau Krediet Registratie.

**Betrokken personen of betrokkenen**
Individuen van wie de persoonsgegevens in handen van onbevoegden zijn gekomen.

**Beveiligingsincident**
- Het falen van bestaande technische of fysieke beveiligingsmaatregelen van uw computersysteem, waardoor onbevoegden toegang tot uw computersysteem krijgen;
- Een Denial of Service aanval (DoS attack);
- Fysieke diefstal of verlies van uw computersysteem, waardoor onbevoegden toegang tot data krijgen;
- Overdracht van kwaadaardige codering (malicious code) van uw computersysteem naar het computersysteem van een derde waardoor schade kan ontstaan.

**Computerspecialist**
Een computerdeskundige die helpt vast te stellen of er sprake is van een beveiligingsincident en helpt om de functionaliteit van het computersysteem voor zover mogelijk in de staat te brengen van voor het incident.

**Computersysteem**
Elk apparaat dat u als particulier bezit met de daarop opgeslagen gegevens, dat uitsluitend gebruikt wordt voor privédoeleinden, dat verbonden kan worden met het internet en waarover u controle heeft.

Computersystemen zijn bijvoorbeeld: computers, servers, cloudinfrastructuur, microcontroller, smartphones, tablets, software of firmware, laptops, opslagmedia zoals externe harde schijven en USB-drives, Internet of Things (IoT) apparaten, smartwatches, particuliere auto's, game consoles, multimedia apparaten, met inbegrip van elk soortgelijk systeem of elke configuratie van voornoemde en met inbegrip van alle bijbehorende invoer-, uitvoer-, gegevensopslag-, netwerkapparatuur of back-upvoorziening.

Onder een computersysteem wordt niet verstaan, een apparaat dat in of op een persoon is geïmplanteerd of geïnjecteerd.

### Controle
U heeft controle over een computersysteem, als alleen u daar toegang toe heeft en onbevoegden alleen toegang kunnen krijgen door illegaal binnen te dringen.

### Cyberincident
Een cyberincident kan een privacy-inbreuk, beveiligingsincident of identiteitsfraude zijn.

### Denial of Service-Aanval (Dos attack)
Denial-of-service-aanvallen (DoS-attack) en distributed-denial-of-service-aanvallen (DDoS-attack) zijn opzettelijke en kwaadaardige pogingen door onbevoegden om een computersysteem niet of moeilijker bereikbaar te maken.

Het kan zijn dat anderen op deze manier de toegang tot uw computersysteem blokkeren. Of het kan een opzettelijke en kwaadaardige aanval zijn waarbij gebruik wordt gemaakt van uw computersysteem om hiermee de toegang tot het computersysteem van een ander te blokkeren.

### Derde of derden
- Rechtspersoon;
- Een persoon die niet een (mede-)verzekerde is.

### Effecten
Verhandelbare of niet-verhandelbare waardepapieren.

### Fraudespecialist
Een specialist die helpt bij het herstellen van informatie over u, zoals die geregistreerd stond vlak voor het moment waarop uw persoonsgegevens werden misbruikt, bij instanties zoals: kredietrapportagentschappen, kredietgevers, incassobureaus, en overheidsinstellingen.

### Frauduleuze instructie
Een instructie door een ander uit uw naam, maar waarvoor u geen toestemming of opdracht heeft gegeven;

Of een schriftelijke instructie van u die is vervalst of gewijzigd door een ander zonder uw medeweten of toestemming.

## Geld
Munten en bankbiljetten die in gebruik zijn en een nominale waarde hebben, postwissels, cheques van banken, persoonlijke cheques en reischeques, e-valuta zoals bitcoins.

## Geldmiddelen
Geld of effecten.

## Gemist loon
Loon uit dienstverband, dat u, in verband met identiteitsfraude, bent misgelopen omdat u onbetaald verlof moest opnemen om de identiteitsfraude aan te pakken. Bijvoorbeeld om te kunnen te overleggen met uw advocaat, wetshandhavingsinstanties, kredietrapportagentschappen of om verklaringen over de identiteitsfraude af te leggen.

## Identiteitsfraude
Het gebruik van uw identiteit door een derde, zonder dat hij daarvoor uw toestemming heeft of zonder dat hij dit mag op grond van de wet of een uitspraak van de rechter.

## Jailbreak
Met het uitvoeren van een jailbreak worden de door de fabrikant ingebouwde systeembeveiligingen van apparatuur omzeild. Hierdoor kan bijvoorbeeld ook software buiten app stores om op telefoons geïnstalleerd worden. Een computersysteem waarop een jailbreak is uitgevoerd is kwetsbaar voor cyberincidenten.

## Kwaadaardige codering (malicious code)
Kwaadaardige codering is een softwareprogramma, code of script dat bedoeld is om een computersysteem of data te infecteren,  te beschadigen, of te stelen. Voorbeelden zijn: Een virus, een Trojaans paard en een computerworm.

## Molest
- Gewapend conflict of cyber conflict: als staten of georganiseerde partijen elkaar (of de één, de ander), bestrijden met wapens, cybermiddelen of militaire machtsmiddelen. Hieronder valt ook het gewapend optreden van een Vredesmacht van de Verenigde Naties;
  Als de verzekeraar zich er op beroept dat een cyber conflict aan een staat kan worden toegerekend, dan berust de bewijslast daarvan bij de verzekeraar. Bij het bepalen van de toerekening zullen verzekeraar en

verzekerde rekening houden met voor hen beschikbaar bewijs dat in redelijkheid en billijkheid als objectief kan worden beschouwd. Daarvan is onder andere sprake als de overheid van de staat waarin het computersysteem dat is getrokken door het cyber conflict zich fysiek bevindt dit cyber conflict toeschrijft, formeel of officieel, aan een andere staat of aan personen die handelen op aanwijzing of onder toezicht van die staat.

- Burgeroorlog: een gewelddadige strijd tussen meerdere inwoners van eenzelfde staat;
- Opstand: georganiseerd gewelddadig verzet binnen een staat, gericht tegen het openbaar gezag;
- Binnenlandse onlusten: georganiseerde gewelddadige handelingen, op verschillende plaatsen binnen een staat;
- Oproer: een georganiseerde plaatselijke gewelddadige beweging, gericht tegen het openbaar gezag;
- Muiterij: een georganiseerde gewelddadige beweging van leden van een gewapende macht, gericht tegen het openbaar gezag.
- De definitie van de in het kader van molest gebruikte onderstaande begrippen luidt:
  **staat**: soevereine staat.
  **cyber conflict**: het gebruik van een computersysteem door, in opdracht van of onder toezicht van een staat met het oogmerk om:
  - een computersysteem te verstoren, de toegang te blokkeren of de functionaliteit ervan te verminderen en/of
  - informatie in een computersysteem te kopiëren, verwijderen, manipuleren, de toegang daartoe te ontzeggen of te vernietigen.

### Onbevoegden

Een persoon of personen, niet zijnde verzekerde, die zonder uw toestemming uw computersysteem binnendringen, of toegang hebben tot persoonsgegevens die u als particulier verwerkt, bezit of beheert, of uw persoons- en of identificatiegegevens misbruiken.

### Onderling met elkaar verband houdende incidenten

Cyberincidenten die dezelfde oorzaak hebben of waarbij een cyberincident het gevolg is van een eerder cyberincident.

### Particuliere Auto
Een personenauto waar u de eigenaar van bent, of die door u wordt geleased voor privé-gebruik.

### Peer to Peer
In een peer to peer-netwerk zijn computersystemen direct met elkaar verbonden en worden peers genoemd. Tussen deze peers kunnen bestanden direct gedeeld worden zonder dat daarvoor een centrale server nodig is. Bijvoorbeeld via bluetooth.

### Persoonsgegevens
Alle gegevens die betrekking hebben op een natuurlijk persoon. Bijvoorbeeld het woonadres, e-mail, het paspoortnummer en medische gegevens.

### Privacyregelgeving
Elke wet- of regelgeving die betrekking heeft op de controle, het gebruik of de bescherming van persoonsgegevens.

### Privacy-inbreuk
Onder privacy-inbreuk verstaan we de ongeoorloofde toegang of diefstal door onbevoegden die geen (mede-)verzekerde zijn of verlies van persoonsgegevens die u als particulier verwerkt, bezit of beheert.

### Provider
Een rechtspersoon waarmee u een schriftelijke overeenkomst heeft voor IT-dienstverlening zoals bijvoorbeeld hosting, data opslag en cloud services.

### Ransomware (losgeld)
Elk type kwaadaardige codering die wordt gebruikt om een computersysteem of netwerk te vergrendelen en zo de toegang te beperken of volledig te blokkeren, waarna er in veel gevallen losgeld wordt geëist met de belofte om de vergrendeling op te heffen.

### Rechtszaak
Een civiele rechtszaak als gevolg van een cyberincident.

### Schade
Zuivere vermogensschade van derden.

### Social engineering fraude
Bij social engineering misbruiken criminelen menselijke eigenschappen, zoals nieuwsgierigheid, vertrouwen, hebzucht, angst en onwetendheid, om iemand te misleiden. Vaak door persoonlijke informatie eerst via het internet te verzamelen. Dit met als doel om iemand frauduleus via e-mail, sms, instant messaging of de telefoon te overtuigen geld over te maken of hier aan mee te werken.

### Specialist
Deskundige op technisch, juridisch of fraude gebied, die u helpt het cyberincident op te lossen.

### Sterk wachtwoord
Een wachtwoord van minimaal 8 karakters, met minstens één hoofdletter, één kleine letter, één cijfer en een ander symbool.

### U, uw of verzekerde
De woorden ‘u’, ‘uw’ of ‘verzekerde’ betekenen de verzekerde persoon/personen zoals vermeld op uw inboedelverzekeringspolis.

### Verzekerde periode
De periode zoals aangegeven in het Dekkingsoverzicht Cyberhulp opgenomen in artikel 1.

### Verzekeraar
De verzekeraar(s) voor het onderdeel CyberHulp zoals vermeld op het polisblad van uw inboedelverzekering..