Stichting toetsing verzekeraars

Themarapportage Gedragscode Verwerking Persoonsgegevens Verzekeraars

Mei 2022

Inhoud

Samenvatting 1
1 Inleiding 2
2 Onderzoeksaanpak 3
2.1 Toetskader 3
2.2 Onderzoeksmethode 3
2.3 Onderzochte informatie en onderzoeksdag 4
2.4 Beperkingen onderzoek 5
3 Resultaten 6
3.1 Algemene resultaten 6
3.1.1 Eerste onderzoek 6
3.1.2 Vervolgonderzoek 6
3.2 onderzoeksresultaten 7
3.2.1 Artikel 2: Reikwijdte en toepassing 7
3.2.2 Artikel 3: Beginselen 8
3.2.2 Artikel 4: Doeleinden 9
3.2.3 Artikel 5: Bijzondere persoonsgegevens 11
3.2.4 Artikel 6: Rechten betrokkenen 11
3.2.5 Artikel 7: Speciale onderwerpen 14
3.2.6 Artikel 9: Naleving gedragscode 18
Bijlage 1: Onderzochte verzekeraars 21

Samenvatting

In oktober 2020 is Stichting toetsing verzekeraars (Stv) als onafhankelijk instituut gestart met het toetsen van de kerncodes klantbelang bij de leden van het Verbond van Verzekeraars (het Verbond). Dit onderzoek naar de Gedragscode Verwerking Persoonsgegevens Verzekeraars (GVPV) is het eerste onderzoek dat Stv uitvoert in dit kader. In dit onderzoek zijn 119 verzekeraars getoetst op de omgang met persoonsgegevens van klanten.

We hebben een toetskader opgesteld op basis van de GVPV. Na afstemming met enkele commissies van het Verbond hebben we het toetskader vastgesteld. De onderzoeksdagen vonden plaats in de periode september 2020 tot medio april 2021.

Aanvankelijk, na de onderzoeksdag, voldoen 50 (42%) verzekeraars aan de gedragscode. Verzekeraars die niet volledig voldoen aan een kerncode hebben een herstelmogelijkheid, waarbij ze binnen een bepaalde periode kunnen aantonen de geconstateerde tekortkomingen te hebben opgelost. Bij het toetspunt over het (uit)voeren van een beleid op het bewaren en vernietigen van persoonsgegevens bleek de gebruikelijke drie maanden hersteltermijn te kort. Voor het wegnemen van deze bevinding waren doorgaans ingrijpende systeemwijzigingen nodig. Wij hebben een voorstel van het Verbond gevolgd om de hersteltermijn voor dit specifieke toepspunt te verlengen naar twaalf maanden.

Aan het einde van de onderzoeksperiode voldoen 97 van de 119 (82%) getoetste verzekeraars aan de GVPV. Er zijn 22 verzekeraars die ook na de verlengde herstelperiode nog niet volledig voldoen aan de gedragscode.

Er zijn 64 verzekeraars die gebruik hebben gemaakt van de herstelmogelijkheid. Na de herstelperiode zijn er 134 verbeteringen opgepakt door verzekeraars.
De verbetering van deze verzekeraars is een van de belangrijke waarden van het onderzoek door Stv. We bevestigen niet alleen waar wel of niet wordt voldaan aan de verplichtingen van de zelfregulering, maar we bevorderen met de toets en de herstelmogelijkheid ook de verbetering van de dienstverlening door verzekeraars.

Na afloop van het onderzoek staan nog 38 terkortkomingen open bij 22 verzekeraars. Van de 22 verzekeraars die na afloop van het onderzoek niet voldoen aan de gedragscode gaat het in bijna alle gevallen mis op het voeren van een beleid op het bewaren en vernietigen van persoonsgegevens. Dit blijft in 21 gevallen een tekortkoming. 17 verzekeraars hebben een concreet plan van aanpak aangeleverd en zijn aan de slag met het herstellen van deze tekortkoming. Het (uit)voeren van een beleid op het bewaren en vernietigen van persoonsgegevens is een van de meest voorkomende tekortkomingen die we hebben geconstateerd bij verzekeraars in dit onderzoek.

De andere tekortkomingen die vaak voorkomen zijn:

1. De verzekeraar heeft vastgelegd dat persoonsgegevens kunnen worden verwerkt ter waarborging van de veiligheid en integriteit van de dienstverlening en de sector en informeert de betrokkenen hierover.
2. De informatie over de verwerking van persoonsgegevens is goed vindbaar en geschreven in begrijpelijke taal. De verzekeraar verwijst in zijn externe privacy statement naar de GVPV.

Voor een nadere uitleg van de resultaten verwijzen we naar hoofdstuk 3.

We adviseren het Verbond om de opvolging van de 38 tekortkomingen te monitoren bij de verzekeraars die na afloop van dit onderzoek nog niet volledig voldoen aan de eisen van de GVPV.

1 Inleiding

In oktober 2020 is Stv gestart met het toetsen van de kerncodes klantbelang. De Gedragscode Verwerking Persoonsgegevens Verzekeraars is de eerste van de tien kerncodes waarbij leden van het Verbond van Verzekeraars intensief worden getoetst door Stv als onderdeel van de zelfregulering van de verzekeringsbranche. Stv voert de onderzoeken uit als onafhankelijke partij in opdracht van het Verbond. In deze rapportage wordt het onderzoek en de uitkomst van het onderzoek toegelicht.

De Kerncode GVPV schrijft de omgang met privacygevoelige informatie voor. Het verwerken van gegevens is voor de verzekeringssector een noodzakelijkheid als het gaat om klanten en producten. De verzekeraars hebben immers verplichtingen om klanten te (leren) kennen op basis van wetgeving. Daarnaast is echter de verwerking van gegevens essentieel om producten te ontwikkelen, risico's te beoordelen en (maatschappelijke) trends te detecteren. Bij het verzamelen van gegevens wordt het aandeel persoonsgegevens steeds belangrijker.

De wijze waarop verzekeraars dienen om te gaan met persoonsgegevens is in beginsel geregeld in de Algemene verordening gegevensbescherming (AVG). In de GVPV is de AVG vertaald naar de toepassing voor de verzekeringssector. Enerzijds biedt de GVPV dus een handvat voor de verzekeringssector om invulling te geven aan de AVG. Anderzijds waarborgt de GVPV dat verzekeraars het klantbelang integreren in de omgang met persoonsgegevens. Daarbij is de reikwijdte van de GVPV logischerwijs beperkt tot klantgegevens.

In het algemeen is het doel van de kerncodes om kwaliteit, uniformiteit en klantbelang te waarborgen binnen de verzekeringssector. Het zelfreguleringstelsel geeft ook de mogelijkheid tot zelfreinigend vermogen in de sector. Sinds medio 2020 heeft het Verbond met Stv een samenwerkingsovereenkomst gesloten waarin de periodieke toetsing van de kerncodes is vastgelegd. De intensieve toetsing op de kerncodes klantbelang door Stv draagt direct bij aan het waarborgen van de uniformiteit en kwaliteit in de sector.

Dit rapport geeft het eindresultaat van het onderzoek naar de GVPV weer. In dit rapport gaan we eerst in op de onderzoeksopzet en in hoofdstuk drie presenteren we de resultaten.

2 Onderzoeksaanpak

Het onderzoek naar de Kerncode GVPV hebben we uitgevoerd in de periode september 2020 – april 2022. In bijlage 1 geven we een overzicht van de verzekeraars die aan de GVPV dienen te voldoen.

2.1 Toetskader

Voor het toetskader is de inhoud van de GVPV het uitgangspunt. Alle toetsbare bepalingen uit de gedragscode zijn in het toetskader opgenomen. Daarbij bepaalt Stv wanneer het toetspunt als voldoende of onvoldoende wordt beoordeeld.

Het toetskader is in concept besproken met de volgende commissies binnen het Verbond van Verzekeraars:

- Commissie Privacy; deze comissie beschouwen wij als de inhoudelijke commissie, die de bedoeling van bepalingen in de gedragscode kan duiden.
- Platform Klantbelang en Reputatie
- Klankbordgroep IAD
- Platform Onderlinge Verzekeraars
- Platform Grootzakelijke Verzekeraars

Deze commissies gaven feedback op het concept, waarna Stv het toetskader vaststelde.

Het toetskader voor de GVPV bevat 36 toetspunten. Stv scoort deze toetspunten met een 'ja', 'nee' of 'nvt'. Het toetskader staat bij de verschillende onderdelen in paragraaf 3.2.

2.2 Onderzoeksmethode

In september 2020 stuurden we een informatiedocument naar de verzekeraars die aan de GVPV dienen te voldoen. In het informatiedocument staat onder meer aangegeven welke documenten we voorafgaand aan de onderzoeksdag willen ontvangen. Ook staat in dat document een gespreksschema voor de interviews.
We stuurden met het informatiedocument ook het toetskader mee, zodat de verzekeraars wisten op welke punten we ons in het onderzoek zouden richten.

Het onderzoek bestond uit twee onderdelen:

1. Bureauonderzoek, naar de aangeleverde documenten en de website.
2. Onderzoeksdag met interviews. Door de coronamaatregelen hebben wij alle interviews uitgevoerd met behulp van videovergaderen.

Tijdens de onderzoeksdag met de interviews trachten we zo veel mogelijk gezamenlijk met de vertegenwoordiger(s) van de verzekeraar te komen tot een oordeel of wel of niet aan de toestpunten is voldaan. Uiteraard bepalen wij of er wel of niet is voldaan aan het toetspunt. Deze aanpak biedt als voordeel dat de verzekeraar wordt meegenomen in de beoordeling en niet verrast wordt door de uitkomst van het onderzoek. Dit bevordert het draagvlak voor eventuele bevindingen van Stv.

Stv stelt direct na de onderzoekdag een conceptrapport op. De verzekeraar heeft twee weken de tijd om daarop te reageren, daarna is het rapport definitief.

Voor een positieve uitkomst van het onderzoek dient een verzekeraar aan alle 36 toetspunten te voldoen.

In overleg tussen Stv en het Platform Onderlinge Verzekeraars is besloten om verzekeraars met een relatief klein premievolume (lager dan vijf miljoen euro) op proportionele wijze te toetsen. Bij deze verzekeraars is een select aantal documenten

opgevraagd en zijn maximaal twee interviews gepland. Op deze manier heeft Stv op een proportionele wijze kunnen toetsen of verzekeraars voldeden aan alle toetspunten. In totaal zijn er 23 verzekeraars op deze manier getoetst.
Daarnaast is er een groep kleine verzekeraars (premievolume minder dan één miljoen euro) die lid is van het Verbond. Deze groep is getoetst door middel van een self assessment. We hebben deze groep getoetst door het schriftelijk stellen van enkele gerichte vragen. Deze verzekeraars hebben schriftelijk gereageerd en daarbij bewijsstukken meegestuurd. Er zijn 16 verzekeraars op deze wijze getoetst.

Als de verzekeraar niet volledig aan een Kerncode voldoet, dan heeft de verzekeraar tot drie maanden na het uitbrengen van de definitieve rapportage de tijd om verbeteringen door te voeren en opnieuw een toets te laten uitvoeren. Dit noemen we een vervolgonderzoek.

In dit onderzoek konden verzekeraars met een bevinding op toetspunt 29, omtrent het (uit)voeren van een beleid op het bewaren en vernietigen van persoonsgegevens, gebruik maken een verlengde hersteltermijn (tot twaalf maanden). De hersteltermijn van drie maanden bleek op dit punt niet realistisch te zijn omdat hiervoor doorgaans systeemaanpassingen nodig waren. De hersteltermijn waarna Stv een vervolgonderzoek uitvoert, is verlengd naar twaalf maanden. Dit betrof uitsluitend een bevinding bij toetspunt 29, voor andere bevindingen gold de herstelperiode van drie maanden. De verlengde hersteltermijn is ingevoerd op initiatief van het Verbond om verzekeraars een realistische kans te geven om de bevinding op te pakken. Het Verbond heeft de verzekeraars hierover in juli 2021 geïnformeerd.

2.3 Onderzochte informatie en onderzoeksdag

Wij hebben de verzekeraars gevraagd om documenten en informatie bij ons aan te leveren. Het ging onder meer om:

- privacybeleid;
- het privacystatement van de verzekeraar;
- een volmachtovereenkomst en intermediairovereenkomst;
- procedures of werkinstructies voor het verwerken van een verzoek tot heroverweging van een betrokkene bij volledig geautomatiseerde verwerking van persoonsgegevens;
- procedures of werkinstructies waaruit de omgang met medische gegevens blijkt;
- procedures of werkinstructies over de omgang van (informatie)verzoeken van betrokkenen in het kader van persoonsgegevens;
- het (informatie)beveiligingsbeleid;
- een procedure of werkinstructie voor het melden van een datalek;
- een procedure of werkinstructie voor het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA);
- een recent uitgevoerde DPIA;
- een verwerkingsovereenkomst;
- het meest recent uitgevoerde interne onderzoek naar de naleving van de GVPV.

Daarnaast hebben wij op de website van de deelnemende verzekeraars onderzocht of het privacystatement op de website stond en wat hierin werd vermeld.

Tijdens de onderzoeksdag bij de verzekeraar spraken we met de volgende functionarissen:

- directie of management met verantwoordelijkheid voor privacybeleid;
- privacy-officer of functionaris gegevensbescherming;
- interne auditor of de verantwoordelijke voor de periodieke interne controle;
- medewerkers die verzoeken van klanten voor inzage en correctie verwerken;

- medewerkers die bezwaren behandelen van klanten over verwerking persoonsgegevens.

2.4 Beperkingen onderzoek

Stv heeft bij de onderzoeken geen inzage gehad in de ICT systemen van verzekeraars. Het onderzoek van Stv is dus in zeker opzicht beperkt tot het toetsen van opzet en bestaan. De werking kan in dit onderzoek niet volledig worden vastgesteld. Deze beperking komt met name terug in de toetspunten omtrent het verwijderen van persoonsgegevens na het verstrijken van de bewaartermijn, de reactietermijnen omtrent verzoeken van betrokkenen en het tijdig melden van datalekken aan de Autoriteit Persoonsgegevens (AP).
Desondanks stelt Stv dat er door de gekozen aanpak, om zoveel mogelijk samen met de verzekeraar de toetspunten door te nemen, wel relevante bevindingen boven water komen. De verzekeraars waren heel open in het aanleveren van de gevraagde informatie en de vertegenwoordigers van de verzekeraars waren ruimhartig in het geven van antwoorden op de gestelde vragen tijdens de onderzoeksdagen.
Wij menen dan ook dat de rapportage een goed beeld geeft van de geconstateerde tekortkomingen bij diverse verzekeraars.

3 Resultaten

In dit hoofdstuk staan de resultaten van het kerncodeonderzoek naar de GVPV beschreven. Er zal eerst een algemeen beeld worden geschetst. Vervolgens zal steeds dieper op de resultaten worden ingegaan.

3.1 Algemene resultaten

3.1.1 Eerste onderzoek

Van de in totaal 119 onderzoeken die door Stv zijn uitgevoerd, is 50 keer direct een positief resultaat behaald. Dat is 42%. Bij 69 verzekeraars scoorden we op één of meerdere toetspunten een 'nee' tijdens het eerste onderzoek. Daarmee heeft 58% van de verzekeraars tijdens het eerste onderzoek een nee-score behaald op één of meerdere toetspunten.

In de 69 onderzoeken met een negatief resultaat is in totaal 172 keer een nee-score toegewezen. Dat betekent dat er per onderzoek gemiddeld 2,5 keer een nee-score is toegekend. De onderzoeken met een negatieve uitslag resulteren in 47 gevallen (68%) in één of twee nee-scores. Bij twaalf onderzoeken (17%) zijn er drie nee-scores geconstateerd. In de overige tien onderzoeken zijn meer dan drie nee-scores behaald, met een maximum van 15 nee-scores. In het grootste deel (86%) van de onderzoeken met een negatieve uitkomst zijn dus drie of minder nee-scores geconstateerd op een totaal van 36 toetspunten.

De resultaten van de onderzoeken laten zien dat op de volgende drie toetspunten het meest frequent een bevinding is gedaan:

- De verzekeraar heeft een beleid voor het bewaren en vernietigen van persoonsgegevens.
- De verzekeraar heeft vastgelegd dat persoonsgegevens kunnen worden verwerkt ter waarborging van de veiligheid en integriteit van de dienstverlening en de sector en informeert de betrokkenen hierover.
- De informatie over de verwerking van persoonsgegevens is goed vindbaar en geschreven in begrijpelijke taal. De verzekeraar verwijst in zijn externe privacy statement naar de GVPV.

In paragraaf 3.2 wordt verder ingegaan op deze toetspunten.

Voor de herstelmogelijkheid die wij als onderdeel van het toetsingsproces aanbieden, komen 69 verzekeraars in aanmerking. In totaal moeten 172 herstelacties worden uitgevoerd. In de volgende paragraaf worden de resultaten van de vervolgonderzoeken beschreven, voordat in meer detail wordt ingegaan op de resultaten.

3.1.2 Vervolgonderzoek

Van de 69 verzekeraars hebben er 64 gebruik gemaakt van de herstelmogelijkheid. We hebben dus bij 64 verzekeraars een vervolgonderzoek uitgevoerd. Deze verzekeraars hebben op basis van onze rapportage met de tekortkoming(en), aanpassingen verricht in hun werkwijze, IT systemen, documenten of website.
Voor het vervolgonderzoek konden de verzekeraars bewijsstukken uploaden. De bewijsstukken zijn door Stv beoordeeld. Om te voldoen aan het vervolgonderzoek gelden dezelfde criteria als voor de eerste toets.

De 64 verzekeraars hebben in totaal 112 bevindingen opgelost binnen de daarvoor gestelde hersteltermijn van drie maanden. Van de 64 vervolgonderzoeken binnen drie maanden zijn er 25 afgerond met een positief resultaat. Een positief resultaat betekent dat de verzekeraar alle bevindingen heeft hersteld. Er zijn 39 verzekeraars die niet alle tekortkomingen konden herstellen binnen de herstelperiode. Zij voldoen daarmee na het

vervolgonderzoek nog niet volledig aan de GVPV. Deze verzekeraars hebben allemaal een openstaande bevinding over de verwijdering van persoonsgegevens. In totaal blijven na het eerste vervolgonderzoek 41 bevindingen openstaan bij de verzekeraars die gebruik hebben gemaakt van de herstelperiode. Deze verzekeraars hebben allen een plan van aanpak aangeleverd waarin zij aangeven hoe en binnen welke termijn zij de bevindingen oplossen.

Zoals eerder aangegeven in paragraaf 2.2 konden de verzekeraars met een bevinding op toetspunt 29 gebruik maken van een verlengde herstel termijn. Tijdens de verlengde herstel termijn hebben 22 verzekeraars de bevinding opgelost.

Daarnaast zijn er vijf verzekeraars die geen gebruik hebben gemaakt van de herstelperiode. Zij konden daarmee ook geen gebruik maken van de verlengde herstel termijn. Deze verzekeraars hebben gezamenlijk negentien bevindingen. Logischerwijs blijven deze bevindingen gehandhaafd omdat we tijdens de onderzoeksperiode niet hebben kunnen vaststellen dat deze bevindingen zijn opgelost.

Daarmee stellen we vast dat 97 verzekeraars (82%) na afloop van de onderzoeksperiode volledig voldoen aan de GVPV.

3.2 onderzoeksresultaten

In deze paragraaf worden per onderzoeksonderdeel de resultaten gedetailleerder uiteengezet. Per onderdeel van de gedragscode worden de resultaten van de onderzochte toetspunten beschreven. Voor elk toetspunt wordt in de tekst een verwijzing gemaakt naar het bijbehorende artikel uit de GVPV. Elke paragraaf eindigt met een overzicht van de toetspunten en het aantal bevindingen op dit toetspunt.

3.2.1 Artikel 2: Reikwijdte en toepassing

In dit onderdeel van de GVPV wordt de reikwijdte en toepassing van de gedragscode uiteengezet. We toetsen in dit onderdeel of verzekeraars, bij uitbesteding van taken aan gevolmachtigden of andere dienstverleners, de naleving van deze code dwingend opleggen in een overeenkomst (art. 2.1.1). Onder andere dienstverleners verstaan we bijvoorbeeld een Arbodienst of rechtsbijstandsverleners.

Om dit toetspunt te beoordelen, hebben we bij iedere verzekeraar een (format) samenwerkingsovereenkomst opgevraagd. In de overeenkomst verwachtten wij op zijn minst een passage aan te treffen waarin de naleving van de kerncodes van het Verbond van Verzekeraars dwingend werd opgelegd. Het was dus niet verplicht om een concrete verwijzing naar de GVPV op te nemen, als de naleving bleek uit een algemene verwijzing. We zien dat veel verzekeraars het model samenwerkingsovereenkomst van het Verbond en de Nederlandse Vereniging van Gevolmachtigde Assurantiebedrijven (NVGA) volgen, waarin ook op algemene wijze de naleving van de kerncodes wordt opgelegd en in de bijlage een lijst met toepasselijke kerncodes is opgenomen.

In totaal is in zeven onderzoeken (6%) geconstateerd dat een verzekeraar in zijn samenwerkingsovereenkomst de GVPV niet dwingend oplegt. De zes verzekeraars die gebruik hebben gemaakt van de hersteltermijn hebben de bevinding alle naar behoren opgelost. Één verzekeraar heeft geen gebruik gemaakt van de hersteltermijn en daarmee blijft er een bevinding openstaan op dit punt.

	Toetspunten bij Reikwijdte en toepassing	Aantal verzekeraars met een bevinding na de onderzoeksdag	Aantal verzekeraars met een bevinding na afloop onderzoeks-periode
1	De verzekeraar legt bij uitbesteding van taken aan gevolmachtigden of andere dienstverleners, de naleving van de GVPV dwingend op in een onderlinge overeenkomst.	7	1

3.2.2 Artikel 3: Beginselen

De beginselen worden uiteengezet in artikel 3 van de GVPV. Dit artikel schrijft onder andere voor dat een verzekeraar een privacybeleid moet hebben. In dit privacybeleid moeten verschillende onderdelen worden opgenomen. Zo moet de verzekeraar beschrijven hoe gegevens worden verzameld en voor welke doeleinden de gegevens worden verzameld. Daarnaast moet de verzekeraar een beleid hebben voor de juistheid van gegevens, de bewaartermijnen, het vastleggen van verwerkingen in een verwerkingsregister en de verwijdering van gegevens.

In beginsel moeten verzekeraars een beleid hebben opgesteld voor de verwerking van persoonsgegevens (art. 3.3.1 & 4.1.1). Uit het onderzoek blijkt dat alle onderzochte verzekeraars een beleid hebben vastgesteld. Op dit punt zijn dus geen bevindingen naar voren gekomen. Er zijn wel bevindingen gedaan op de inhoud van het beleid in de overige toetspunten.

In het beleid moeten verzekeraars de doeleinden voor het verwerken van persoonsgegevens hebben vastgelegd (art. 3.3.1 & 4.1.1). Dit mocht ook blijken uit een concrete verwijzing in het beleid naar het verwerkingsregister. Daarnaast is in het onderzoek vastgesteld of de verzekeraar alle doeleinden heeft beschreven. Er zijn minstens vier concrete doeleinden die, indien van toepassing, moeten worden beschreven door verzekeraars. Uit ons onderzoek is op dit punt één bevinding gedaan waarbij een verzekeraar niet alle doeleinden had beschreven. Na het vervolgonderzoek is de bevinding op dit punt opgelost.
Daarnaast is beoordeeld of de verzekeraar in zijn beleid heeft beschreven hoe persoonsgegevens worden verzameld (art. 3.3.1 & 4.1.1). Het gaat daarbij om de bronnen van de persoonsgegevens. Op dit onderdeel zijn geen bevindingen gedaan. Alle onderzochte verzekeraars voldoen dus op dit punt.

Het laatste element betreft het hebben van beleid op verschillende aspecten (art. 3.4.1). Het gaat daarbij om de aspecten: juistheid van gegevens, de bewaartermijnen, het vastleggen van verwerkingen in een verwerkingsregister en de verwijdering van persoonsgegevens. In drie onderzoeken is er een bevinding gedaan op dit punt.

In alle drie de onderzoeken blijkt dat de verzekeraar geen beleid voert op bewaartermijnen. In twee van deze onderzoeken komt naar voren dat de verzekeraar geen beleid voert op het vastleggen van verwerkingen in een verwerkingsregister en de verwijdering van gegevens. In één onderzoek constateren we dat er geen beleid wordt gevoerd op de juistheid van persoonsgegevens. Na afloop van de hersteltermijn zijn alle bevindingen op dit punt opgelost.

Er zijn drie verzekeraars (3%) die in totaal vier tekortkomingen noteren bij dit onderdeel over de beginselen. Na de vervolgonderzoeken voldoen alle verzekeraars aan dit onderdeel van de gedragscode.

	Toetspunten bij Beginselen	Aantal verzekeraars met een bevinding na de onderzoeksdag	Aantal verzekeraars met een bevinding na afloop onderzoeks-periode
2	De verzekeraar heeft een privacybeleid voor de verwerking van persoonsgegevens.	0	0
3	In het beleid beschrijft de verzekeraar de concrete doeleinden voor het verzamelen en verwerken van persoonsgegevens.	1	0
4	In het beleid beschrijft de verzekeraar hoe hij de persoonsgegevens verzamelt.	0	0
5	De verzekeraar heeft een beleid voor de noodzakelijkheid en juistheid van de te verwerken persoonsgegevens, de bewaartermijnen, het vastleggen van verwerkingen in een daartoe bestemd verwerkingsregister en de verwijdering van persoonsgegevens.	3	0

3.2.2 Artikel 4: Doeleinden

Dit onderdeel van de GVPV zet de lijnen uit voor de verschillende doeleinden waarvoor verzekeraars persoonsgegevens kunnen verzamelen. Dit onderzoek richt zich op de doelstellingen: volledig geautomatiseerde besluitvorming bij het aangaan en uitvoeren van verzekeringen, de analyse van gegevens en marketingactiviteiten en relatiemanagement. Hierbij is gekeken naar het privacybeleid, de communicatie via het privacystatement richting betrokkenen en de procedures.

De gedragscode geeft betrokkenen bij volledig geautomatiseerde verwerking van persoonsgegevens tijdens het aangaan en uitvoeren van een verzekering het recht op menselijke heroverweging (art. 4.2.2). De verzekeraar moet dit beleidsmatig hebben belegd en een proces hebben ingericht om te voldoen aan een verzoek op heroverweging. Op dit toetspunt is twee keer een bevinding gedaan. In beide gevallen bleek dat de verzekeraar het recht op heroverweging niet had opgenomen in het beleid en in een procedure. Ook wezen beide verzekeraars de klant niet op dit recht in het privacystatement. Beide bevindingen zijn opgelost na de herstelperiode.

Een ander doel waar de gedragscode zich op richt, is marketingactiviteiten en relatiebeheer. Het kan voorkomen dat verzekeraars persoonsgegevens verzamelen voor marketingdoeleinden en deze gegevens niet direct van de betrokkenen hebben verkregen, maar van een derde partij. Als een verzekeraar dit doet, dan moet de verzekeraar de betrokken hierover informeren (art. 4.4.1). Uit het onderzoek komen op dit onderdeel geen bevindingen naar voren bij verzekeraars. Alle verzekeraars informeren betrokkenen hier dus over.

Daarnaast kunnen verzekeraars gebruik maken van direct marketing om klanten te benaderen. Als verzekeraars dit via automatische systemen doen, dan moeten zij betrokkenen om toestemming vragen door een zogehete ‘opt-in’ mogelijkheid. Bij andere technieken zoals (elektronische) post moet de verzekeraar waarborgen dat er een ‘opt-out’ mogelijkheid is waarmee de klant zich makkelijk kan uitschrijven (art. 4.5.3). Op dit onderdeel zijn geen bevindingen gedaan.

Als laatste bij dit onderdeel dient de verzekeraar betrokkenen te informeren over het feit dat persoonsgegevens kunnen worden verwerkt ter waarborging van de veiligheid en integriteit van de dienstverlening en de sector (art. 4.5.3). Om dit vast te stellen, is in eerste instantie het privacystatement beoordeeld.
Op dit punt is 24 keer een bevinding gedaan tijdens het onderzoek. Daarmee communiceerden 24 verzekeraars dit doel van gegevensverwerking onvoldoende of helemaal niet aan betrokkenen.
Alle verzekeraars die gebruik hebben gemaakt van de herstelperiode hebben dit punt opgelost. Bij vier verzekeraars die hier geen gebruik van hebben gemaakt, blijft de bevinding op dit punt gehandhaafd. Dat betekent dat er na afloop van het onderzoek nog vier verzekeraars zijn die betrokkenen niet informeren over dit doel van gegevensverwerking.

Er zijn 26 verzekeraars (22%) die in totaal 26 tekortkomingen noteren bij dit onderdeel over doeleinden. Na afloop van de onderzoeksperiode voldoen er nog vier verzekeraars (3%) niet aan dit onderdeel van de gedragscode.

	Toetspunten bij Doeleinden	**Aantal verzekeraars met een bevinding na de onderzoeksdag**	**Aantal verzekeraars met een bevinding na afloop onderzoeks-periode**
6	Als een verzekeraar volledig geautomatiseerde verwerkingen verricht (bijvoorbeeld voor het aangaan van de verzekering of het behandelen van schades) waaruit rechtsgevolgen voortvloeien, dan kan betrokkene verzoeken het besluit te laten heroverwegen door een medewerker.	2	0
7	De verzekeraar informeert de betrokkene bij verwerking van persoonsgegevens voor marketingdoeleinden die de verzekeraar niet direct bij betrokkene heeft verzameld.	0	0
8	Bij gebruik van automatische oproepsystemen of elektronische berichten benadert de verzekeraar klanten alleen als klanten contactgegevens hebben gegeven voor afsluiten verzekering of door voorafgaande toestemming (‘opt-in’). Bij gebruik van andere technieken zoals post voor direct marketing heeft de klant een ‘opt-out’ mogelijkheid door aan te geven dat hij die marketing niet wenst te ontvangen.	0	0
9	De verzekeraar heeft vastgelegd dat persoonsgegevens kunnen worden verwerkt ter waarborging van de veiligheid en integriteit van de dienstverlening en de sector en informeert de betrokkenen hierover.	24	4

3.2.3 Artikel 5: Bijzondere persoonsgegevens

In dit onderdeel van de GVPV is de omgang met bijzondere persoonsgegevens onderzocht. Daarbij is onderzocht of verzekeraars medische en strafrechtelijke gegevens verwerken conform de criteria en voorwaarden in de gedragscode.

Met betrekking tot de verwerking van medische gegevens zijn twee punten onderzocht. Namelijk of medische gegevens conform de eisen in artikel 5.1 worden verwerkt (art. 5.1.1) en of de verzekeraar waarborgt dat medische gegevens alleen door de medisch adviseur en zijn medewerkers worden verwerkt voor het opstellen van medisch advies (art. 5.1.3). Op deze punten zijn tijdens het onderzoek geen bevindingen gedaan. Alle verzekeraars die medische gegevens verwerken, doen dit dus volgens de eisen uit de GVPV.

Daarnaast is onderzocht of verzekeraars strafrechtelijke gegevens verwerken conform de cirteria en voorwaarden van arikel 5.2 van de GVPV (art. 5.2.1). Daarop is één bevinding gedaan tijdens het onderzoek. Deze bevinding is tijdens de herstelperiode opgelost door de betreffende verzekeraar.

Toetspunten bij Bijzondere persoonsgegevens		**Aantal verzekeraars met een bevinding na de onderzoeksdag**	**Aantal verzekeraars met een bevinding na afloop onderzoeks-periode**
10	De verzekeraar verwerkt gezondheidsgegevens conform de criteria en voorwaarden van artikel 5.1 van de GVPV.	0	0
11	Alleen de medisch adviseur en zijn medewerkers mogen gezondheidsgegevens verwerken voor het opstellen van een medisch advies.	0	0
12	De verzekeraar verwerkt strafrechtelijke gegevens conform de criteria en voorwaarden van artikel 5.2 van de GVPV.	1	0

3.2.4 Artikel 6: Rechten betrokkenen

Dit onderdeel van de GVPV ziet toe op de informatieverstrekking van verzekeraars aan betrokkenen over de (mogelijke) verwerking van persoonsgegevens. Zo kunnen betrokkenen beoordelen of zij het eens zijn met deze verwerkingen en gebruik willen maken van de rechten die zij hebben in dit kader. Betrokkenen hebben het recht op inzage, correctie, bezwaar en verwijdering van hun persoonsgegevens. In totaal zijn 23 bevindingen gedaan op de 11 punten waarop getoetst is in dit onderdeel van de GVPV.

In het kader van informatieverstrekking is in dit onderzoek beoordeeld of de verzekeraar een privacystatement op de website heeft staan (art. 6.1.1). Alle verzekeraars hebben een privacystatement op de website staan. Hieruit zijn dus geen onderzoeksbevindingen voortgekomen.

Daarnaast is in het onderzoek beoordeeld of het privacystatement van de verzekeraar goed vindbaar is, in begrijpelijke taal is geschreven en of de verzekeraar verwijst naar de

GVPV (art. 6.1.3). Op dit punt zijn 21 bevindingen gedaan. Alle bevindingen zien toe op het feit dat er geen verwijzing naar de GVPV wordt gemaakt in het privacystatement van de verzekeraar. Dat betekent dat alle privacystatements in duidelijke taal zijn geschreven en goed vindbaar zijn op de website. Het aantal bevindingen op dit toetspunt is te verklaren doordat deze verplichting niet direct voortvloeit uit de AVG. Het betreft een punt dat specifiek is toegevoegd aan de GVPV.
Alle verzekeraars die gebruik hebben gemaakt van de herstelperiode, hebben een verwijzing naar de GVPV opgenomen in het privacystatement. Na afloop van de onderzoeksperiode blijven er drie bevindingen op dit punt openstaan bij de verzekeraars die geen gebruik hebben gemaakt van de herstelperiode.

Een andere verplichting in het kader van informatieverstrekking is dat verzekeraars betrokkenen voorafgaand aan een verwerking voor een ander doel dan waarvoor de verzekeraar gegevens heeft verzameld, moet informeren (art. 6.1.4). Op dit punt zijn geen bevindingen gedaan in het onderzoek.

Als laatste hebben we in het kader van informatieverstrekking onderzocht of verzekeraars bij het nemen van besluiten gebaseerd op automatische verwerking van persoonsgegevens, betrokkenen informeert over het bestaan, het belang, de logica en de te verwachten gevolgen (art. 6.1.5). Hierbij hebben we gekeken naar het privacystatement van de verzekeraar. Op dit punt zijn vier bevindingen gedaan.
Bij twee verzekeraars stond er geen informatie over geautomatiseerde verwerkingen in het privacystatement. Bij de overige twee verzekeraars ontbraken één of meerdere elementen in de beschrijving in het privacystatement. Na de herstelperiode zijn alle bevindingen door de verzekeraars opgelost.

Vervolgens gaat de gedragscode in op het recht op inzage. De verzekeraar dient de betrokkenen desgevraagd inzage te verlenen in de persoonsgegevens die worden verwerkt (art. 6.2.1). Hiervoor is beoordeeld of verzekeraars een werkinstructie hebben ingericht en of deze in de praktijk ook wordt gevolgd door medewerkers. Op dit punt is bij drie verzekeraars een bevinding geconstateerd. Bij alle drie waren geen werkinstructies of procesbeschrijvingen opgesteld om te voldoen aan een verzoek tot inzage van een betrokkene. In de herstelperiode hebben alle verzekeraars een werkinstructie of procedure aangeleverd waarmee dit punt adequaat is opgepakt.

Daarnaast legt de code de verplichting op om binnen een maand het gevraagde overzicht aan te leveren (art. 6.2.2). Daarvoor is onderzocht hoe verzekeraars waarborgen dat een overzicht binnen een maand wordt aangeleverd. De verzekeraar moet ook monitoren op de doorlooptijden. Bij één verzekeraar is vastgesteld dat er geen monitoring op dit proces plaatsvindt. Deze verzekeraar heeft hier tijdens de herstelperiode invulling aan gegeven en voldoet na het vervolgonderzoek.

Voordat de verzekeraar een verzoek van een betrokkene inwilligt, verplicht de gedragscode de verzekeraar om de identiteit van de betrokkene vast te stellen (art. 6.2.4 & 6.3.3). Dit kan de verzekeraar doen door de betrokkene te verzoeken zich te legitimeren. Hiervoor zijn verschillende mogelijkheden denkbaar. Uit het onderzoek blijkt dat één verzekeraar niet altijd de identiteit van de betrokkene vaststelt. Deze bevinding is opgelost gedurende de herstelperiode.

Vervolgens gaat de gedragscode in op de overige rechten van betrokkenen. Deze rechten zijn het verzoek om correctie, bezwaar, beperking en verwijdering. Daarbij hebben we onderzocht of de verzekeraar op het verzoek reageert binnen de daarvoor gestelde termijn uit de gedragscode.
Bij verzoeken van betrokkenen om correctie van persoonsgegevens (art. 6.3.1), of bij het maken van bezwaar (art. 6.3.2) moeten verzekeraars binnen een maand reageren. Hierbij is beoordeeld of verzekeraars dit in de praktijk doen en of ze de termijnen monitoren. Voor zowel het verzoek om correctie als het verzoek op bezwaar is er bij één

verzekeraar geconstateerd dat er geen monitoring plaatsvindt op de termijn. De verzekeraar bij wie deze bevindingen zijn geconstateerd, heeft deze bevindingen opgelost tijdens het vervolgonderzoek.

Als een betrokkene bezwaar maakt tegen de verwerking van zijn persoonsgegevens voor marketingdoeleinden, dan moet de verzekeraar onmiddellijk stoppen met het verwerken van deze persoonsgegevens (art. 6.3.2). De verzekeraar moet daarvoor een intern register hebben waarin hij bezwaren vastlegt. Ook moet hij regelmatig het Bel-me-niet register raadplegen. We hebben bij één verzekeraar geconstateerd dat er geen intern register is waar bezwaren in worden bewaard en daarbij werd ook niet regelmatig het Bel-me-niet register geraadpleegd door deze verzekeraar. De verzekeraar heeft de tekortkomingen op dit punt tijdens de herstelperiode opgelost.

Als laatste dienen verzekeraars betrokkenen te helpen met het verhuizen van persoonsgegevens (art. 6.4.1). Het verhuizen van persoonsgegevens wordt in de gedragscode een verzoek tot dataportabiliteit genoemd. Op dit punt gaf één verzekeraar aan niet te voldoen aan een verzoek tot dataportabiliteit. Tijdens het onderzoek merken we op dat verzoeken tot dataportabiliteit niet tot nauwelijks voorkomen in de praktijk.

Er zijn 23 verzekeraars (19%) die in totaal 34 tekortkomingen noteren bij dit onderdeel over de rechten van betrokkenen. Na afloop van de onderzoeksperiode voldoen er nog drie verzekeraars (3%) niet aan dit onderdeel van de gedragscode.

	Toetspunten bij Rechten betrokkenen	**Aantal verzekeraars met een bevinding na de onderzoeksdag**	**Aantal verzekeraars met een bevinding na afloop onderzoeks-periode**
13	De verzekeraar geeft uitdrukking aan de informatieplicht, in ieder geval door een extern privacybeleid (zoals een privacystatement) op de website te plaatsen.	0	0
14	De informatie over de verwerking van persoonsgegevens is goed vindbaar en geschreven in begrijpelijke taal. De verzekeraar verwijst in zijn externe privacystatement naar de GVPV.	21	3
15	De verzekeraar informeert de betrokkene voorafgaand aan een verwerking voor een ander doel dan waarvoor hij de gegevens heeft verzameld.	0	0
16	Als de verzekeraar een besluit neemt (bijvoorbeeld acceptatie of claimbehandeling) gebaseerd op geautomatiseerde verwerking van persoonsgegevens, dan meldt de verzekeraar het bestaan, het belang, de logica en de te verwachten gevolgen van deze verwerking.	4	0
17	De verzekeraar verstrekt op verzoek van betrokkene een overzicht van de persoonsgegevens die van hem/haar worden	3	0

	verwerkt en de aanvullende informatie zoals vermeld in artikel 6.2.1.		
18	De verzekeraar verstrekt dit overzicht (zie artikel 6.2.1) binnen een maand na de datum van ontvangst van het verzoek aan de betrokkene.	1	0
19	De verzekeraar stelt de identiteit van de betrokkene vast, om zeker te stellen dat de juiste persoon toegang krijgt tot de eigen persoonsgegevens.	1	0
20	De verzekeraar reageert binnen een maand op het verzoek van een betrokkene om correctie van zijn persoonsgegevens.	1	0
21	De verzekeraar reageert binnen een maand op het bezwaar van een betrokkene tegen de verwerking van zijn persoonsgegevens.	1	0
22	De verzekeraar stopt onmiddellijk met de verwerking van persoonsgegevens voor marketingdoeleinden wanneer de betrokkene bezwaar hiertegen maakt.	1	0
23	De verzekeraar helpt een betrokkene op diens verzoek met het verhuizen van persoonsgegevens.	1	0

3.2.5 Artikel 7: Speciale onderwerpen

Dit onderdeel van de GVPV beschrijft hoe verzekeraars om dienen te gaan met speciale onderwerpen. In dit onderzoek zijn negen onderwerpen getoetst. Het gaat daarbij om de onderwerpen: verzamelen van gegevens via apparatuur van betrokkkenen, beveiliging, datalekken, gegevensbeschermingsbeoordeling (hierna: DPIA), beleid bewaren persoonsgegevens, pseudonimisering, vastleggen elektronische communicatie, cameratoezicht en verwerkersovereenkomst.

Voor het onderwerp 'verzamelen van gegevens via apparatuur van betrokkenen' is beoordeeld of verzekeraars gegevens verzamelen via methodes zoals cookies, Google Pixel of bijvoorbeeld device fingerprints. Indien verzekeraars gebruik maken van dergelijke methodes voor gegevensverzameling, moeten zij betrokkenen hierover informeren (art. 7.1.1). Bij één verzekeraar constateerden we dat hij betrokkenen niet vooraf informeert terwijl er wel gegevens worden verzameld van de betrokkenen via tracking cookies. De verzekeraar heeft de bevinding opgelost tijdens de herstelperiode.

Over het onderwerp 'beveiliging' zijn verzekeraars verplicht om een beveiligingsbeleid op te stellen. In dit beveiligingsbeleid moet concreet staan beschreven welke organisatorische en technische maatregelen zijn genomen om persoonsgegevens te beschermen (art. 7.2.1). Om dit te beoordelen, is bij alle onderzochte verzekeraars het beveiligingsbeleid opgevraagd. Bij twee verzekeraars is geconstateerd dat zij geen beveiligingsbeleid hadden opgesteld. Tijdens de hersteltermijn heeft één verzekeraars een beveiligingsbeleid opgesteld waarin concreet organisatorische en technische maatregelen staan beschreven. De andere verzekeraar heeft geen reactie gegeven op deze bevinding. Daarmee blijft er na de herstelperiode één verzekeraar met een bevinding op dit punt.

De gedragscode verplicht verzekeraars onder het onderwerp 'datalek' om een meldingsplichtig datalek binnen 72 uur na kennisname te melden aan de AP (art. 7.3.1). In het onderzoek is beoordeeld of verzekeraars een proces hebben ingericht om datalekken te melden. Daarnaast is ook besproken met verzekeraars in hoeverre dit proces als uitkomst heeft dat meldplichtige datalekken gemeld worden binnen 72 uur. Tijdens het onderzoek zijn géén bevindingen gedaan op dit onderwerp. Alle onderzochte verzekeraars voldoen aan de eisen voor het onderwerp datalekken.

Bij het onderwerp DPIA stelt de GVPV eisen over het moment dat een DPIA moet worden uitgevoerd (art. 7.4.1) en over welke elementen de DPIA moet bevatten (art. 7.4.2). Verzekeraars moeten een DPIA uitvoeren wanneer een nieuwe of bestaande verwerking waarschijnijk een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen. Daarbij moet de verzekeraar rekening houden met de aard, de omvang, de context en doeleinden van de verwerking (art. 7.4.1).
Door recente DPIA's op te vragen en in gesprek te gaan met de functionaris gegevensbescherming (FG) is tijdens het onderzoek vastgesteld of verzekeraars DPIA's uitvoeren als dit verplicht is. De verzekeraar moet beleidsmatig vastleggen wanneer een DPIA moet worden uitgevoerd. Daarbij is tijdens de onderzoeksdag met de verzekeraar besproken hoe het proces eruitziet rondom het uitvoeren van een DPIA. Dit proces moet in ieder geval resulteren in inzicht wanneer en voor welke verwerkingen DPIA's moeten worden uitgevoerd en hoe een DPIA uit wordt gevoerd door verzekeraars.
Tijdens het onderzoek is bij zeven verzekeraars een tekortkoming vastgesteld op dit punt. Drie verzekeraars hadden niet (beleidsmatig) vastgelegd wanneer een DPIA moet worden uitgevoerd. Bij één verzekeraar is geconcludeerd dat er geen overzicht bestond of/en welke DPIA's moeten worden uitgevoerd. Bij de overige drie verzekeraars is geconcludeerd dat zij ten onrechte geen DPIA hadden uitgevoerd, terwijl dit wel verplicht was geweest. Zes verzekeraars hebben de bevinding tijdens de herstelperiode opgelost. Een verzekeraar die ten onrechte geen DPIA had uitgevoerd, heeft geen gebruik gemaakt van de herstelperidoe. Daarmee blijft er na de herstelperiode één verzekeraar over met bevinding op dit punt.

Op basis van de uitgevoerde DPIA is tijdens het onderzoek tevens vastgesteld of verzekeraars alle vereiste elementen die voort komen uit de gedragscode ook hebben beoordeeld. In de DPIA moet in ieder geval staan: een analyse van de beoogde verwerking, doeleinden, noodzaak, grondslagen, mogelijke risico's voor betrokkenen, de waarborgen die de verzekeraar treft om risico's te mitigeren en er moet advies zijn ingewonnen bij de FG.
Bij drie verzekeraars is er een bevinding gedaan op de elementen die zij meenamen in de uitgevoerde DPIA. Bij één verzekeraar waarborgde de instructie om een DPIA uit te voeren niet dat alle elementen werden meegenomen. Bij een andere verzekeraar kon geen oordeel worden gegeven op dit punt omdat er onterecht nog geen DPIA was uitgevoerd. Bij de laatste verzekeraar is geconstateerd dat niet in alle gevallen advies ingewonnen werd bij de FG tijdens het uitvoeren van een DPIA.
Tijdens de herstelperiode hebben de drie verzekeraars de bevinding opgelost.

Het volgende speciale onderwerp in de GVPV is 'Beleid bewaren persoonsgegevens'. Verzekeraars moeten een beleid opstellen voor het bewaren en vernietigen van persoonsgegevens (art. 7.5.1). Persoonsgegevens worden op basis hiervan bewaard met een specifiek doel tot aan de gestelde bewaartermijn. Na het verstrijken van de bewaartermijn dienen verzekeraars persoonsgegevens te vernietigen, te anonimiseren of te pseudonimiseren.

Tijdens het onderzoek is beoordeeld of verzekeraars een dergelijk beleid hebben vastgesteld, waarin ze concreet de bewaartermijnen benoemen. Het kan zijn dat verzekeraars de bewaartermijnen vast hebben gelegd in het verwerkingsregister. Maar er

moet wel een beleid zijn voor het bewaren en verwijderen van gegevens. Ook is beoordeeld of verzekeraars hun eigen beleid in de praktijk uitvoeren.
Hiervoor is het beleid bewaren persoonsgegevens opgevraagd bij verzekeraars. In de gesprekken tijdens de onderzoeksdag is onderzocht of het beleid ook uit wordt gevoerd in de praktijk.
De uitkomst van het onderzoek is dat 48 verzekeraars niet voldeden op dit punt na het eerste onderzoek. We zien dat er drie verschillende redenen zijn waarom verzekeraars niet voldoen aan dit toetspunt.
Bij de grootste groep (40 verzekeraars) concluderen we dat we dat er wel een beleid is vastgesteld voor het bewaren en verwijderen van persoonsgegevens, maar dat zij het beleid niet uitvoeren in de praktijk.
Bij een klein gedeelte (zeven verzekeraars) concluderen we dat er geen beleid over het bewaren en vernietigen van persoonsgegevens is vastgesteld.
Bij één verzekeraar troffen we de situatie aan waarin er geen beleid was vastgesteld, maar de gegevens wel werden verwijderd in de praktijk.

Zoals eerder toegelicht in paragraaf 2.2 is er voor dit toetspunt naast de initiele herstelperiode, een verlengde herstelperiode ingevoerd. Hieronder beschrijven we de resultaten van beide herstelperiodes.

Tijdens de eerste herstelperiode hebben vijf verzekeraars de bevinding op dit toetspunt op kunnen lossen. Dat betekent dat 43 verzekeraars de bevinding niet hebben opgelost binnen de herstelperiode van drie maanden. Van deze 43 verzekeraars hebben vier verzekeraars geen gebruik gemaakt van de eerste herstelperiode. Daarmee konden zij ook geen gebruik maken van de verlengde herstelperiode.
De 39 verzekeraars die wel gebruik hebben gemaakt van de eerste herstelperiode hebben bij ons een plan van aanpak aangeleverd. In dit plan van aanpak hebben zij aangegeven hoe en binnen welke termijn zij de bevinding op kunnen lossen. In alle 39 gevallen was het uitvoeren van het beleid in de praktijk nog niet mogelijk. De reden hiervoor is dat de projecten die verzekeraars hebben opgezet om verwijdering uit de IT-systemen te realiseren niet haalbaar waren binnen drie maanden.

Binnen de verlengde herstelperiode hebben 23 verzekeraars zich gemeld voor een vervolgonderzoek. Voor het vervolgonderzoek hebben we verzekeraars gevraagd om eventueel aanvullend bewijs aan te leveren en hebben we een nieuw interview ingepland met de betreffende verzekeraar om vast te stellen dat de bevinding op toetspunt 29 was opgelost.
In totaal hebben we 23 onderzoeken uitgevoerd binnen de verlengde herstelperiode. Van de 23 onderzoeken zijn er 22 met een positief resultaat afgerond.
Er waren zestien verzekeraars die de bevinding niet konden oplossen binnen de verlengde hersteltermijn, omdat het project om de verwijdering van persoonsgegevens te realiseren nog niet gereed was. Zoals eerder aangegeven hebben vier verzekeraars geen gebruik gemaakt van de initiële hersteltermijn. Daarmee zijn er nog 21 verzekeraars die een bevinding open hebben staan op dit toetspunt.

Als verzekeraars gebruik maken van het pseudonimiseren van persoonsgegevens moeten ze maatregelen treffen om ongeoorloofde re-identificatie te voorkomen (art. 7.6.1). Met pseudonimisering vervangen verzekeraars direct identificerende gegevens van een betrokkene door andere identificatiemiddelen, zoals een IP-adres, gebruikersnaam of klantnummer. Verzekeraars moeten maatregelen nemen om re-identificatie van de gepseudonnimiseerde gegevens te voorkomen. Verzekeraars moeten de dataset met gepseudonimiseerde gegevens apart bewaren van de originele dataset. Ook dienen verzekeraars de toegang tot de originele dataset te beperken.

Tijdens dit onderzoek is beoordeeld of verzekeraars deze maatregelen hebben vastgelegd en of de maatregelen worden toegepast in de praktijk. Bij twee verzekeraars is tijdens het onderzoek geconstateerd dat zij geen maatregelen nemen om re-identificatie van

gepseudonimiseerde persoonsgegevens te voorkomen. We hebben bij één verzekeraar een vervolgonderzoek uitgevoerd en hgeconstateerd dat de bevinding was opgelost. De andere verzekeraar heeft geen gebruik gemaakt van de herstelperiode. Dat betekent dat één verzekeraar geen maatregelen neemt om re-identificatie van gepseudonimiseerde persoonsgegevens te voorkomen.

Verzekeraars die elektronische communicatie registreren, moeten volgens de GVPV voldoen aan voorwaarden bij het vastleggen van deze communicatie (art. 7.7.2). De GVPV schrijft voor dat verzekeraars een strikte bewaartermijn hanteren, passende beveiliging hebben en kenbaar maken aan betrokkenen dat elektronische communicatie wordt vastgelegd. Tijdens dit onderzoek is beoordeeld of verzekeraars deze eisen hebben vastgelegd in beleid, en of ze deze eisen in de praktijk toepassen.

Zestien verzekeraars voldeden niet aan één of meerdere van de eisen die de GVPV voorschrijft voor het vastleggen van elektronische communicatie. Bij één verzekeraar constateren we dat zowel beleidsmatig als in de praktijk geen invulling wordt gegeven aan de drie vereisten. Bij negen verzekeraars constateren we dat alleen beleidsmatig één of meerdere elementen ontbreken. In zes gevallen constateren we dat verzekeraars geen uitvoering geven aan één of meerdere vereisten in de praktijk.
In totaal zijn er twaalf vervolgonderzoeken uitgevoerd. Tijdens alle vervolgonderzoeken is vastgesteld dat de verzekeraar voldoet aan de eisen voor het vastleggen van elektronische communicatie. Vier verzekeraars met een bevinding op dit punt hebben geen gebruik gemaakt van de herstelperiode.

Verzekeraars kunnen gebruik maken van cameratoezicht als dat noodzakelijk is. Die noodzaak kan zich voordoen bij objectbeveiliging of om strafbare feiten te voorkomen, vast te stellen of te onderzoeken. De GVPV geeft criteria voor de inzet van cameratoezicht (art. 7.8.2). De criteria zien toe op: selectiviteit, bewaartermijnen, passende beveiligng en kenbaarheid. In dit onderzoek is beoordeeld of de verzekeraar deze criteria heeft vastgelegd in beleid en of hij uitvoering geeft aan deze criteria in de praktijk.
We hebben bij twee verzekeraars geconstateerd dat zij één of meerdere criteria niet hebben vastgelegd in beleid. Bij beide verzekeraars is een vervolgonderzoek uitgevoerd met een positieve uitkomst.

Verzekeraars die persoonsgegevens laten imlementeren door verwerkers moeten in een overeenkomst met de betreffende verwerker alle verplichtingen vastlegggen op grond van geldende wet- en regelgeving (art. 7.9.1). In dit onderzoek is bij één verzekeraar geconstateerd dat dit niet het geval was. Deze verzekeraar heeft deze bevinding tijdens de herstelperiode opgelost.

Er zijn 63 verzekeraars (53%) die in totaal 82 tekortkomingen noteren bij dit onderdeel over speciale onderwerpen. Na afloop van de onderzoeksperiode zijn er nog 21 verzekeraars (18%) die niet voldoen aan dit onderdeel van de gedragscode.

	Toetspunten bij Speciale onderwerpen	**Aantal verzekeraars met een bevinding na de onderzoeksdag**	**Aantal verzekeraars met een bevinding na afloop onderzoeks-periode**
24	Verzekeraars plaatsen gegevens, waaronder cookies, op de apparatuur van betrokkene om gegevens te verzamelen. In andere gevallen	1	0

	zal een verzekeraar gegevens pas verzamelen nadat betrokkene is geïnformeerd.		
25	Verzekeraar heeft een beveiligingsbeleid waarin concreet wordt aangegeven welke organisatorische en technische maatregelen zijn genomen om de persoonsgegevens te beschermen.	2	1
26	De verzekeraar meldt een meldingsplichtig datalek indien mogelijk binnen 72 uur na kennisname aan de AP.	0	0
27	De verzekeraar voert een DPIA uit wanneer een nieuwe verwerking of de aanpassing van een bestaande verwerking gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van de betrokkene.	7	1
28	Een DPIA bevat alle elementen van artikel 7.4.2. De verzekeraar wint daarnaast advies in van de functionaris gegevensbescherming (FG).	3	0
29	De verzekeraar heeft een beleid voor het bewaren en vernietigen van persoonsgegevens.	48	21
30	De verzekeraar treft na pseudonimisering van persoonsgegevens maatregelen om ongeoorloofde re-identificatie te voorkomen.	2	1
31	Bij het vastleggen van elektronische communicatie voldoet de verzekeraar aan de voorwaarden van artikel 7.7.2.	16	4
32	Bij de inzet van cameratoezicht voldoet de verzekeraar aan de voorwaarden van artikel 7.8.2.	2	0
33	Bij het inschakelen van een verwerker die op instructie persoonsgegevens verwerkt, sluit de verzekeraar een verwerkersovereenkomst met deze partij. In de overeenkomst legt de verzekeraar alle verplichtingen vast waaraan een verwerker moet voldoen.	1	0

3.2.6 Artikel 9: Naleving gedragscode

In het laatste onderdeel van de GVPV dat is getoetst in dit onderzoek staan de vereisten over het zelfreinigend vermogen waarmee verzekeraars waarborgen dat zij voldoen aan de GVPV. Verzekeraars stellen een functionaris gegevensbescherming (FG) aan die voldoet aan de vereisten van deskundigheid en onafhankelijkheid. Daarnaast moeten verzekeraars periodiek onderzoeken of zij voldoen aan de eisen uit de GVPV. Als laatste

richten verzekeraars een klachtprocedure in waarmee betrokkene een klacht in kan dienen bij de verzekeraar als de betrokkene van mening is dat de verzekeraar in strijd handelt met de GVPV of AVG.

De GVPV schrijft voor dat de verzekeraar een FG aanstelt die deskundig en onafhankelijk is (art. 9.1.1). Het aanstellen van een FG is niet voor iedere verzekeraar verplicht. Het kan bijvoorbeeld zijn dat door de aard van de dienstverlening of het type product het niet verplicht is een FG aan te stellen. Bij de verzekeraars die wel een FG moeten aanstellen, hebben we in geen enkel geval geconstateerd dat de FG niet deskundig was of niet onafhankelijk kon optreden in zijn of haar functie.

De GVPV verplicht verzekeraars om intern onderzoek uit te voeren naar de naleving van de kerncode en geldende wetgeving (art. 9.2.1). Bij elf verzekeraars is geconstateerd dat zij niet periodiek intern onderzoek uitvoeren. Om deze bevinding op te lossen, moesten verzekeraars aan kunnen tonen op welke wijze zij waarborgen dat er periodiek onderzoek wordt uitgevoerd naar de naleving van de GVPV en geldende wetgeving. Het was niet vereist om een dergelijk onderzoek binnen drie maanden uit te voeren.
Alle verzekeraars die gebruik hebben gemaakt van de hersteltermijn en een vervolgonderzoek hebben laten uitvoeren, hebben deze bevinding naar behoren opgepakt.
Twee verzekeraars hebben geen gebruik gemaakt van de mogelijkheid op een vervolgonderzoek. Bij deze verzekeraars hebben we dus niet kunnen vaststellen of zij intern onderzoek uitvoeren of zullen gaan uitvoeren. Er blijft dus bij twee verzekeraars een bevinding openstaan na afloop van de onderzoeksperiode.

Als laatste is getoetst of verzekeraars hun klachtprocedures zo hebben ingericht dat zij betrokkenen, na het doorlopen hebben van de interne klachtprocedure (IKP), wijzen op de mogelijkheid om hun klacht in te dienen bij de bevoegde rechter, het Kifid of de AP (art. 9.3.1). Daarbij is niet alleen naar verzekeraars definitieve reactie op de klacht gekeken, maar ook naar zijn mededelingen in dat verband op de website (bijvoorbeeld in het privacystatement of onder de rubriek 'klachtprocedure'). Een dergelijke mededeling op de website volstaat als sluitstuk van de IKP.
Bij zes verzekeraars is geconstateerd dat zij betrokkenen niet wijzen op de mogelijkheid om een klacht in te dienen bij het Kifid of de bevoegde rechter. Alle verzekeraars hebben deze bevinding opgelost tijdens de herstelperiode

Er zijn vijftien verzekeraars (13%) die in totaal zeventien tekortkomingen noteren bij dit onderdeel over speciale onderwerpen. Na afloop van de onderzoeksperiode zijn er nog twee verzekeraars die niet voldoen aan dit onderdeel van de gedragscode.

	Toetspunten bij Naleving gedragscode	**Aantal verzekeraars met een bevinding na de onderzoeksdag**	**Aantal verzekeraars met een bevinding na afloop onderzoeks-periode**
34	De verzekeraar heeft een FG aangesteld. De FG is een deskundige, onafhankelijke professional.	0	0
35	De verzekeraar onderzoekt periodiek intern de naleving van de GVPV.	11	2
36	De verzekeraar wijst de betrokkene op de mogelijkheid dat -nadat hij de interne klachtenprocedure heeft doorlopen- de	6	0

	betrokkene zijn klacht in het kader van GVPV ook kan indienen bij het Kifid of zich kan wenden tot het AP of de bevoegde rechter. Dit moet zijn opgenomen in de klachtbrief van de verzekeraar.		

Bijlage 1: Onderzochte verzekeraars

- ABN AMRO Levensverzekering N.V.
- ABN AMRO Schadeverzekering N.V.
- ACE Europe life Limited
- Achmea Pensioen-en Levensverzekering
- Achmea Schadeverzekeringen N.V.
- AEGON Nederland N.V. Leven
- AEGON Nederland N.V. Schade
- AEGON Nederland N.V. Spaarkas
- AgriVer Onderlinge Hagelverzekering Maatschappij B.A.
- AIG Europe S.A., Netherlands Branch
- Allianz Benelux NV
- Allianz Global Corporate Specialty (AGCS)
- Amlin Insurance S.E.
- Anker Insurance Company n.v.
- Ansvar Verzekeringsmaatschappij
- ARAG SE
- ASR Levensverzekering NV
- ASR Schadeverzekering NV
- Atradius Crédito y Caución S.A. de Seguros
- Avipol B.A., Onderlinge Waarborgmaatschappij
- AWP P&C S.A. - Dutch Branch
- AXA XL
- Baloise Belgium N.V.
- BNP Paribas Cardif Levensverzekering
- BNP Paribas Cardif Schadeverzekering
- Bos Fruit Aardappelen Onderlinge Verz. BFAO UA
- Centramed B.A., Onderlinge Waarborgmaatschappij
- Chubb European Group SE
- CNA Hardy
- Coface Nederland
- Credit Life AG
- DAS Nederlandse Rechtsbijstand Verzekeringmaatschappij N.V.
- De Burcht, N.V. Verzekeringsmaatschappij
- De Laatste Eer U.A., Onderlinge Uitvaartverzekering
- De Luchtvaart Onderlinge WA
- DELA Natura- en levensverzekeringen N.V.
- Donatus Verzekeringen
- EFO Paardenverzekering
- EOC Verzekeringen
- EULER HERMES Europe S.A.
- Gartenbau-Versicherung VVaG
- Goudse Leven N.V., De
- Goudse Schade N.V., De
- Hagelunie N.V.
- HDI Global SE
- Hiscox SA
- If P&C Insurance Ltd. (publ.)
- JUWON Onderlinge Schade Maatschappij U.A.
- Klaverblad Verzekeringen U.A., Coöperatie
- Lifetri Uitvaartverzekeringen N.V.
- Lifetri Verzekeringen N.V.
- Markel Insurance SE
- MediRisk B.A., Onderlinge Waarborgmaatschappij voor Instellingen in de Gezondheidszorg

Bijlage 1: Onderzochte verzekeraars (vervolg)

- Mercurius Schadeverzekeringen NV
- Midglas Glasassurantie Maatschappij N.V.
- Monuta Verzekeringen NV
- MSIG Insurance Europe AG
- MUNIS U.A., Onderlinge verzekeringsmaatschappij
- N.V. Schadeverzekering-Maatschappij Bovemij
- Nationale-Nederlanden Levensverzekering Maatschappij N.V.
- Nationale-Nederlanden Schadeverzekering Maatschappij N.V.
- Nh1816 Verzekeringen, Levensverzekeringsmaatschappij NV
- Nh1816 Verzekeringen, Schadeverzekeringsmaatschappij NV
- Noord Holland U.A., OBM
- OBV "Steenwijkerwold" WA
- OBV Giethoorn
- Onderling Verzekerd UA
- Onderlinge Levensverzekering Maatschappij s-Gravenhage U.A.
- Onderlinge Steenwijk Verzekeringen
- Onderlinge van 1719
- Onderlinge Verzekeringen OVM UA
- Onderlinge Waarborg Maatschappij Achterhoek U.A.
- ONVZ Aanvullende Verzekering N.V.
- ONVZ ziektekosten verzekering NV
- OOM Verzekeringen
- OVM Twente
- OVM Vinkeveen & Omstreken
- Patronale Life NV
- Proteq Levensverzekeringen NV (Vivat)
- Quantum Leben AG
- Rheinland Versicherungs AG
- Rijn en Aar U.A., Onderlinge Verzekerings Maatschappij
- Robein Leven N.V.
- RSA Luxembourg S.A., Netherlands branch
- Samenwerking Glasverzekering N.V.
- SAZAS U.A., Onderlinge waarborgmaatschappij
- Schadeverzekeringsmaatschappij Maas Lloyd
- Scildon N.V.
- SI Insurance (Europe) SA
- Sliedrecht Onderling Fonds BA
- SOM U.A., Onderlinge Verzekeringmaatschappij
- Squarelife Lebensversicherungs-Aktiengesellschaft
- SRLEV N.V. (Vivat)
- The Prudential Assurance Company Ltd.
- Tokio Marine Europe SA
- TVM U.A., Coöperatie
- Uitvaartverzekering Twenthe NV
- Univé Dichtbij Brandverzekeraar N.V.
- Univé Het Groene Hart N.V.
- Univé Noord-Holland Brandverzekeraar N.V.
- Univé Noord-Nederland
- Univé Oost Brandverzekeraar N.V.
- Univé Samen U.A., Onderlinge Verzekeringsmaatschappij
- Univé Schade N.V.
- Univé Stad en Land Brandverzekeraar N.V.
- Univé Zuid-Nederland
- UVM Verzekeringen
- Veenhoop U.A., Onderlinge Verzekeringsmaatschappij De

Bijlage 1: Onderzochte verzekeraars (vervolg)

- Vereende N.V., De
- Vereinigte Hagel VVaG
- Verzekeringsbedrijf Groot Amsterdam (VGA) N.V.
- VvAA Groep B.V.
- Waard Leven N.V.
- Waard Schade N.V.
- Waterland en Omstreken U.A., Onderlinge Verzekeringsmaatschappij
- Yarden Uitvaartverzekeringen N.V.
- Zevenwouden
- ZLM Verzekeringen
- Zurich Insurance plc