Themarapportage Module Kwaliteitsverbetering Gedragscode Verwerking Persoonsgegevens Verzekeraars

November 2022

Inhoud rapportage Module Kwaliteitsverbetering

Samenvatting

Introductie

Stichting toetsing verzekeraars (hierna: Stv) toetst de naleving van de zelfregulering in opdracht van het Verbond van Verzekeraars.

Het eerste kerncode-onderzoek: de Gedragscode Verwerking Persoonsgegevens Verzekeraars (hierna: GVPV) is getoetst bij alle leden van het Verbond van Verzekeraars.

In aanvulling op het kerncode-onderzoek zijn wij met de aanvullende Module Kwaliteitsverbetering dieper ingegaan op het onderwerp privacy.

Wij hebben het onderzoek met de Module Kwaliteitsverbetering uitgevoerd bij negen verzekeraars.

Resultaat

Op de gedeelde eerste plaats van de benchmark staan ABN AMRO Verzekeringen en Nationale–Nederlanden Schade met een score van 97%.

Rechtsbijstandverzekeraar DAS volgt op de derde plaats met een score van 96%.

De gemiddelde score over negen verzekeraars is 90%.

Verbetermogelijkheden

Tijdens ons onderzoek hebben we ondanks de hoge scores een aantal verbetermogelijkheden gesignaleerd. De belangrijkste verbetermogelijkheden zijn:

- Uitvoering geven aan het beleid voor het bewaren en verwijderen van persoonsgegevens. Niet alle verzekeraars zijn in staat om volledig uitvoering te geven aan het beleid voor het bewaren en vernietigen van persoonsgegevens.
- Het geven van trainingen over privacy. Een deel van de verzekeraars geeft (nieuwe) medewerkers geen basistraining privacy of herhaalt deze vervolgens niet periodiek, bijvoorbeeld eens in de drie jaar.
- Het uitwerken van beleid voor het bewaren en verwijderen van e-mails en opgenomen telefoongesprekken. En vervolgens het waarborgen van de periodieke verwijdering hiervan. Een deel van de deelnemende verzekeraars heeft hier geen duidelijk beleid voor en waarborgt onvoldoende de periodieke verwijdering hiervan.
- Het geven van informatie in het privacystatement over het opnemen/registreren van telefoongesprekken en chatsessies. Een deel van de verzekeraars heeft in het privacystatement niet of onvoldoende beschreven of het telefoongesprekken en chatsessies opneemt/registreert en waar ze dit vervolgens voor gebruiken.

Goede praktijkvoorbeelden

Verzekeraars kunnen de goede praktijk-voorbeelden die wij hebben gezien tijdens ons onderzoek gebruiken om zich op onderdelen nog verder te verbeteren. Enkele voorbeelden:

- Sommige verzekeraars hebben (een deel van) het verwerkingsregister openbaar gemaakt en gedeeld op de website. Een best practice hierbij zien we bij een van de deelnemers aan de Module Kwaliteitsverbetering: De verzekeraar linkt vanuit het privacystatement naar het verwerkingsregister. Het verwerkingsregister is voor zowel intern als extern gebruik gelijk en geeft op een overzichtelijke manier informatie.
- Een software tool voor het verwerkingsregister geeft de mogelijkheid om een periodieke uitvraag aan de business in te regelen. Dit om te verifiëren of verwerkingen nog actueel zijn. Ook helpt een software tool om risico’s bloot te leggen, de informatieflow en verbanden inzichtelijk te maken en zet het desgewenst de Data Protection Impact Assessment (hierna: DPIA) in gang.
- Een aantal verzekeraars heeft ook een DPIA op bestaande processen met een hoog risico uitgevoerd. Een enkeling heeft zelfs op ieder bestaand en nieuw proces een DPIA uitgevoerd. Een goed uitgevoerde DPIA is een waardevol middel om mogelijke risico’s in kaart te brengen.

1. Inleiding

Rapportage
In dit rapport geven we inzicht in de uitkomsten van het onderzoek naar de Module kwaliteits-verbetering bij de GVPV.

Dit rapport is een aanvulling op het onderzoeks-rapport van het kerncode-onderzoek uitgevoerd bij alle leden van het Verbond van Verzekeraars. Het rapport van het kerncode-onderzoek staat op de website van Stv.

Inhoud onderzoek
In dit onderzoek hebben wij onderzocht hoe verzekeraars omgaan met het verwerken van persoonsgegevens.

In de periode van oktober 2020 tot en met maart 2021 heeft Stv 112 verzekeraars getoetst op de kerncode GVPV.

Negen verzekeraars namen ook deel aan de Module Kwaliteitsverbetering.

Onderzoek op afstand
Door de uitbraak van het coronavirus konden de fysieke bedrijfsbezoeken voor het onderzoek GVPV niet doorgaan.
De bedrijfsbezoeken zijn dan ook uitgevoerd op afstand met behulp van videovergaderen.

Nieuw stelsel zelfregulering
Het onderzoek naar de kerncode GVPV is het eerste onderzoek voor het nieuwe stelsel van zelfregulering.

Stv toetst bij alle leden van het Verbond van Verzekeraars of er wordt voldaan aan de gedragscodes. Bij tien zogenoemde Kerncodes Klantbelang toetsen we elke drie jaar intensief de naleving daarvan.

In aanvulling op kerncode-onderzoeken biedt Stv de Module Kwaliteitsverbetering aan.

Normenkader en benchmark
Het normenkader voor het onderzoek GVPV met de Module Kwaliteitsverbetering bestaat uit drie onderdelen:

I. Beleid en praktijk
II. Mensen en middelen
III. Communicatie naar de klant

De resultaten van de verzekeraars vertalen wij naar een score, waarmee we een benchmark opstellen. Hiermee zien verzekeraars hoe zij presteren ten opzichte van andere verzekeraars.

Daarnaast geven we per onderdeel een marktbeeld terug wat is opgedaan bij het kerncode-onderzoek.

Drijfveer Stv
Stv heeft als missie het bijdragen aan het bevorderen van een duurzaam vertrouwen van de consument in de verzekeringssector. Stv toetst hiervoor het nieuwe stelsel van zelfregulering.

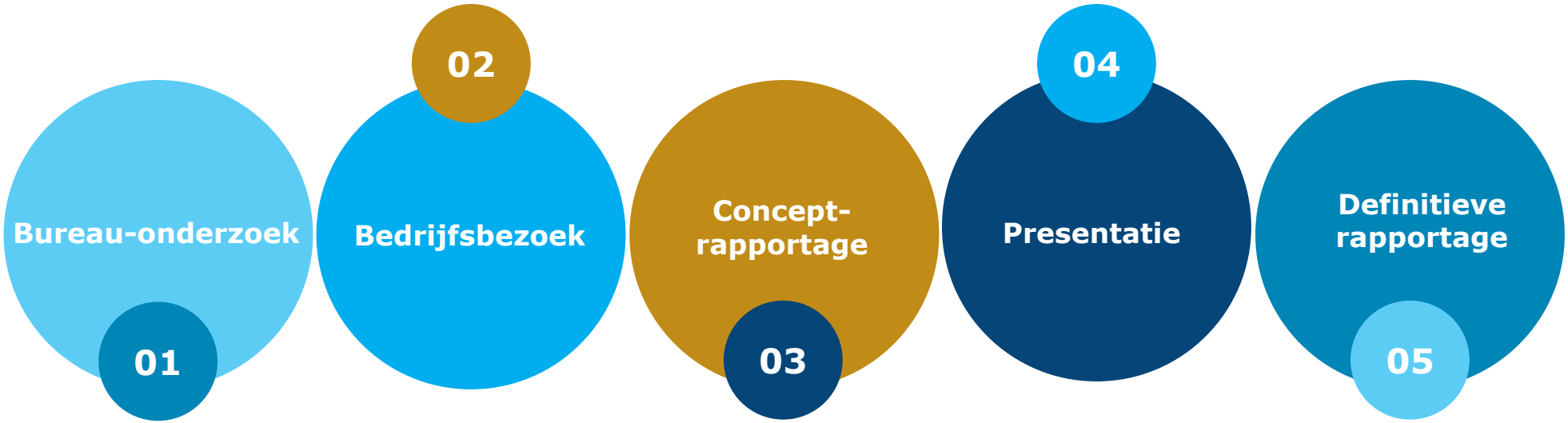
Iedere verzekeraar ontvangt een eigen rapport met aanbevelingen en adviezen waarmee hij zich kan verbeteren.

Daarnaast stellen we een themarapportage op waarin we de resultaten over alle verzekeraars presenteren. Daarin staan ook de goede praktijkvoorbeelden en aanbevelingen met een algemeen karakter.

Met onze audits en themarapportages dragen wij bij aan het verder verbeteren van de klantgerichtheid van verzekeraars.

2. Onderzoeksaanpak

De onderzoeksaanpak door Stv bestaat voor iedere verzekeraar uit vijf stappen.



Bureau-onderzoek

De Stv-auditors bestuderen de website, beleidsstukken en verschillende documenten over het verwerken van persoonsgegevens:

- privacybeleid;
- privacystatement;
- werkinstructies;
- intern onderzoek;
- opleidings- en trainingsprogramma;
- samenwerkings-overeenkomsten.

Bedrijfsbezoek

De Stv-auditors komen (virtueel) op bezoek en hebben interviews met de directeur, managers en medewerkers die zich bezighouden met het verwerken van persoonsgegevens.

Concept-rapportage

De verzekeraar ontvangt een conceptrapportage met pluspunten, bevindingen, aanbevelingen en adviezen.

Presentatie

De Stv-auditor bespreekt de conceptrapportage met het management van de verzekeraar.

Definitieve rapportage

De verzekeraar ontvangt de definitieve rapportage.

3. Normenkader

Het normenkader GVPV met de Module Kwaliteitsverbetering bestaat uit drie onderdelen:

I. Beleid en praktijk

De verzekeraar heeft beleid en procedures vastgesteld om te voldoen aan de eisen van de GVPV. Hiermee legt de verzekeraar de basis voor een zorgvuldige omgang in de organisatie met de persoonsgegevens van zijn klanten en voor het nakomen van de rechten van de klant, zoals die in de GVPV zijn vastgelegd.

II. Mensen en middelen

Om de GVPV goed te kunnen naleven, moet de verzekeraar de vereiste taken duidelijk beleggen bij medewerkers. De medewerkers moeten beschikken over voldoende tijd en kennis. Ook moet de verzekeraar de medewerkers faciliteren met middelen en instrumenten waarmee ze hun taken goed kunnen uitoefenen en hun handelingen waar nodig aantoonbaar vast kunnen leggen.

III. Communicatie naar de klant

De verzekeraar heeft als uitgangspunt dat de klant recht heeft op een open, complete en juiste communicatie over de werkwijze van de verzekeraar bij de verwerking van persoonsgegevens, alsmede over de rechten van de klant daarbij. Ook wil hij aanspreekbaar zijn als de klant verzoeken heeft over de verwerking van zijn eigen persoonsgegevens.

Werkprogramma

Het normenkader dat is gebruikt voor de Module Kwaliteitsverbetering is een aanvulling op het normenkader dat gebruikt is voor de kerncode GVPV.
Het reguliere kerncode-onderzoek bestaat uit 36 toetspunten, het onderzoek Module Kwaliteitsverbetering bestaat uit 90 toetspunten.

Opbouw scores

Ieder toetspunt heeft een scoremogelijkheid van 0, 5 of 10 punten. Toetspunten die gelijk zijn aan het reguliere kerncode-onderzoek kennen enkel de scoremogelijkheid 0 of 10 punten.

De drie onderdelen van het normenkader zijn ieder opgebouwd uit meerdere toetspunten. Om te komen tot een score per onderdeel is er gekeken naar de behaalde score per onderdeel ten opzichte van de maximaal haalbare score en vervolgens uitgedrukt in een percentage. Hierbij is rekening gehouden met toetspunten die mogelijk voor een verzekeraar niet van toepassing zijn.
De totale score van de verzekeraar is de behaalde score over de drie onderdelen ten opzichte van de maximaal haalbare score.

Minimale score

Bij deelname aan de Module Kwaliteitsverbetering geldt geen minimale score. Het doel is namelijk kwaliteitsverbetering.
Net als iedere verzekeraar moeten de deelnemers aan de kwaliteitsmodule wel voldoen aan de kerncode GVPV.

4. Benchmark

Benchmarkscore
De benchmarkscore van iedere verzekeraar is de gemiddelde score die hij behaald heeft over de drie onderdelen.

Op de gedeelde eerste plaats van de benchmark staan ABN AMRO Verzekeringen en Nationale–Nederlanden Schade met een score van 97%.

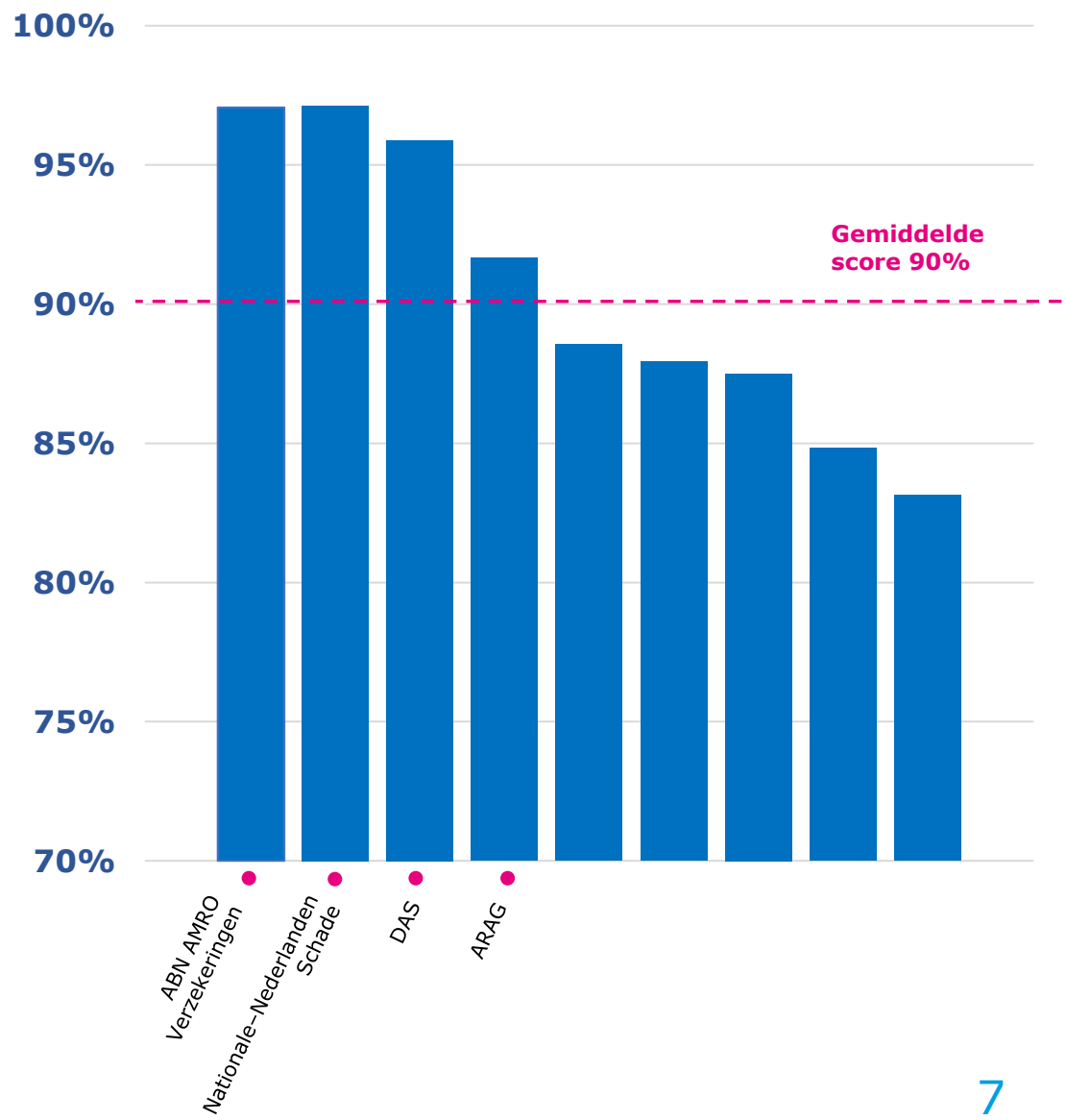
Rechtsbijstandverzekeraar DAS volgt op de derde plaats met een score van 96%.

De gemiddelde score over 9 verzekeraars is 90%.

De verklaring voor dit goede resultaat is dat de verwerking van persoonsgegevens al enkele jaren een belangrijk onderwerp is en bij veel deelnemende verzekeraars hoog op de agenda staat.

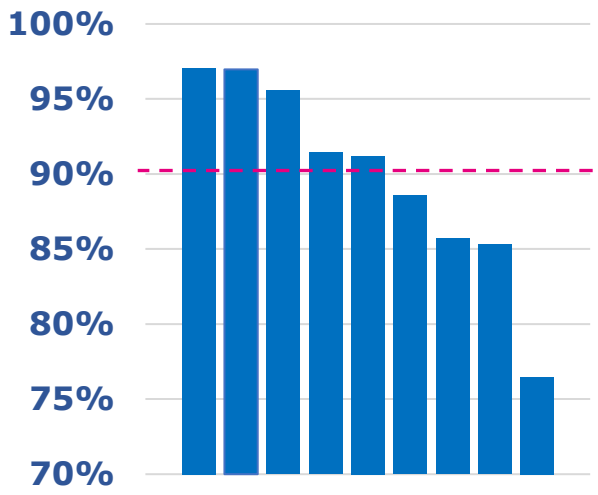
Ondanks de hoge gemiddelde score hebben we alle verzekeraars in hun individuele rapport verbeterpunten of aanbevelingen gegeven om te komen tot nog betere prestaties.

Resultaten per onderdeel
Op de volgende pagina's gaan we in op de resultaten in de drie verschillende onderdelen van het normenkader. Wat zijn de scores per onderdeel, wat gaat opvallend goed en wat kan beter?



5. Resultaten

I. Beleid en praktijk



Benchmarkscore
In het onderdeel Beleid en praktijk scoren verzekeraars gemiddeld 90%.

Marktbeeld
In de markt zien we op dit onderdeel dat verzekeraars veel moeite hebben met het volledig uitvoering geven aan beleid voor het bewaren en verwijderen van persoonsgegevens.

Verder viel op dat veel verzekeraars met name tijdens de invoering van de AVG veel aandacht hebben besteed aan bewustwording van de privacywetgeving maar dat dit inmiddels weer opnieuw aandacht nodig heeft.

Algemeen beeld en wat gaat goed

Privacybeleid
Alle deelnemende verzekeraars hebben een privacybeleid. In bijna alle gevallen (89%) is dit ook volledig, vastgesteld door directie en gecommuniceerd met de organisatie.

De opzet en uitwerking van het privacybeleid verschilt behoorlijk tussen de verzekeraars. We zagen beleidsstukken van tien maar ook van honderd pagina's.

Uitvoeren van DPIA's
Alle deelnemende verzekeraars hebben wanneer nodig een DPIA uitgevoerd. Deze DPIA's bevatten ook de vereiste elementen zoals voorgeschreven in de GVPV/AVG.

78% van de verzekeraars heeft een duidelijk overzicht van uitgevoerde DPIA's, bijvoorbeeld door deze op te nemen in een registratie.

Datalekken
Bij alle deelnemende verzekeraars heerst er een cultuur waarin medewerkers zich vrij voelen om een datalek te melden.

Daarnaast is bij alle verzekeraars een meldingsplichtig datalek tijdig gemeld bij de Autoriteit Persoonsgegevens.

Wel zien we nog grote verschillen tussen het aantal datalekken dat verzekeraars weten waar te nemen. Dit ligt mogelijk aan het bewustzijn van medewerkers over wat een (potentieel) datalek inhoudt en het gemak waarmee medewerkers een datalek kunnen melden.

Beveiligingsbeleid
Alle deelnemende verzekeraars hebben een uitgebreid beveiligingsbeleid. Ook toetst iedere verzekeraar periodiek de werking van de technische beveiligingsmaatregelen.

I. Beleid en praktijk

Wat kan beter?

Het periodiek herzien van het privacybeleid en het privacystatement
Uit ons onderzoek komt naar voren dat alle deelnemende verzekeraars een privacybeleid hebben. Het privacybeleid is bij alle verzekeraars actueel, maar iets meer dan de helft (56%) van de verzekeraars waarborgt het periodiek controleren op actualiteit en herzien van het privacybeleid.

Hetzelfde zien we ook bij het privacystatement, iets meer dan de helft (56%) heeft het controleren op actualiteit bijvoorbeeld belegd in de jaarplanning van de functionaris gegevensbescherming (hierna: FG).

Het in de praktijk uitvoering geven aan het beleid voor het bewaren en vernietigen van persoonsgegevens
Uit ons onderzoek komt naar voren dat iets minder dan de helft van de deelnemende verzekeraars (44%) in staat is om volledig uitvoering te geven aan het beleid voor het bewaren en vernietigen van persoonsgegevens.

Verzekeraars lopen hierbij veelal tegen beperkingen aan in administratiesystemen waardoor (automatische) verwijdering niet, of slechts beperkt mogelijk is. Bij al deze verzekeraars staat het maken van aanpassingen in de systemen om het verwijderen van persoonsgegevens mogelijk te maken hoog op de agenda.

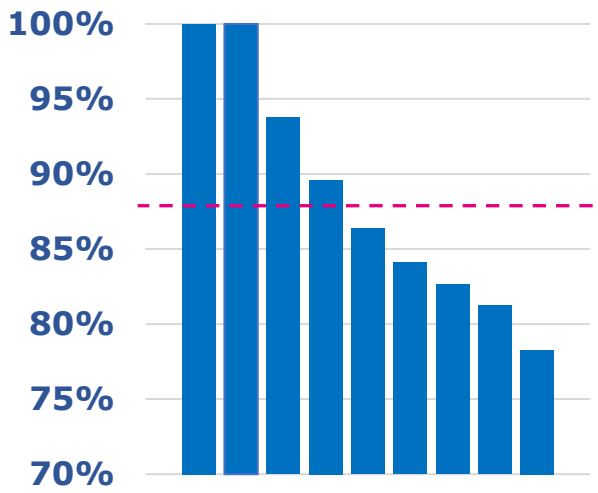
Het periodiek herhalen van uitgevoerde DPIA's
Een derde van de verzekeraars heeft gewaarborgd dat het een uitgevoerde DPIA periodiek herhaalt, bijvoorbeeld door dit vast te leggen in de procedure en de DPIA registratie. Een derde van de verzekeraars herhaalt in de praktijk periodiek uitgevoerde DPIA's maar heeft dit onvoldoende vastgelegd.

Verder zagen we dat niet iedere verzekeraar even duidelijk rapporteert over de uitgevoerde DPIA's. Bijvoorbeeld door deze te voorzien van een managementsamenvatting met daarin de belangrijkste uitkomsten.

Tweedelijns beheersmaatregelen op de naleving van de GVPV/AVG en periodiek onderzoek vanuit de derde lijn
Een derde van de deelnemende verzekeraars heeft een uitgebreid risico control framework met daarin aandacht voor privacy risico indicatoren. Dit helpt verzekeraars om de naleving van de GVPV/AVG te monitoren en tijdig bij te sturen op eventuele risico's.
Meer dan de helft van de verzekeraars (67%) heeft geen of in beperkte mate tweedelijns beheersmaatregelen ingericht en is druk bezig met het verder uitwerken van het risico control framewerk door hier privacy controls in op te nemen.

Een derde van de deelnemende verzekeraars heeft in de afgelopen drie jaar een volledig derdelijns intern onderzoek uitgevoerd op de naleving van de GVPV/AVG. Iets meer dan de helft (56%) van de verzekeraars heeft wel een onderzoek uitgevoerd maar zich daarin beperkt tot opzet en/of bestaan en niet de werking getoetst van bijvoorbeeld het privacybeleid.

II. Mensen en middelen



Benchmarkscore
In het onderdeel Mensen en middelen scoren verzekeraars gemiddeld 88%.

Marktbeeld
Bijna iedere verzekeraar heeft een verwerkingsregister. De opzet en inhoud daarbij kennen grote verschillen.
Verzekeraars zijn zich niet altijd bewust van de verwerking van persoonsgegevens buiten het administratiesysteem. Bijvoorbeeld persoons-gegevens in e-mails die zich bevinden in de persoonlijke mailbox van medewerkers. Het opschonen hiervan is veelal handwerk en moeilijk in kaart te brengen.
Een andere uitdaging is het beheer van ongestructureerde data op bijvoorbeeld netwerkschijven en SharePoint omgevingen.

Algemeen beeld en wat gaat goed

Verwerkingsregister
Alle deelnemende verzekeraars hebben een verwerkingsregister vastgelegd. Driekwart (78%) van de verzekeraars heeft hierbij alle benodigde informatie opgenomen.

Deskundige en onafhankelijke FG
Alle deelnemende verzekeraars hebben een deskundige FG aangesteld die onafhankelijk in de organisatie zijn taken kan uitvoeren. Alle verzekeraars betrekken de FG actief in kwesties over de bescherming en het verwerken van persoonsgegevens.

Verwerken van gezondheids- en strafrechtelijke gegevens
Alle deelnemende verzekeraars verwerken gezondheids- en strafrechtelijke gegevens volgens de criteria en voorwaarden van de GVPV.

Verzekeraars hebben daarbij ook een duidelijke scheiding aangebracht in de organisatie over wie toegang heeft tot deze gegevens en wie deze mag verwerken.

Cookiestatement
Alle deelnemende verzekeraars hebben wanneer dit nodig is een duidelijke cookie pop-up op de website staan. Wel viel op dat bij een aantal verzekeraars de snelkoppelingen in deze cookie pop-up naar bijvoorbeeld “meer informatie” niet werkten.

II. Mensen en middelen

Wat kan beter?

Het actueel houden van het verwerkingsregister
Twee derde van de deelnemende verzekeraars heeft een actueel verwerkingsregister waarbij het periodiek waarborgt dat de gegevens in het verwerkingsregister nog actueel en compleet zijn. Bij een derde van de verzekeraars was het verwerkingsregister niet of onvoldoende bijgehouden sinds de invoering van de AVG.

Voldoende tijd en middelen voor de FG
Het valt op dat bij kleine en middelgrote verzekeraars de FG veelal zijn taken uitvoert als een rol naast zijn functie als compliance officer.

Bij een derde van de verzekeraars is hierdoor soms een gebrek aan tijd om de functie van FG uit te voeren zoals de FG die zelf ambieert. Zaken zoals bewustwording, monitoring en het actualiseren van procedures en het verwerkingsregister zijn aangelegenheden waar FG's dan meer tijd aan willen besteden. Bij alle verzekeraars kan de FG wel de meest belangrijke taken van zijn functie goed uitvoeren.

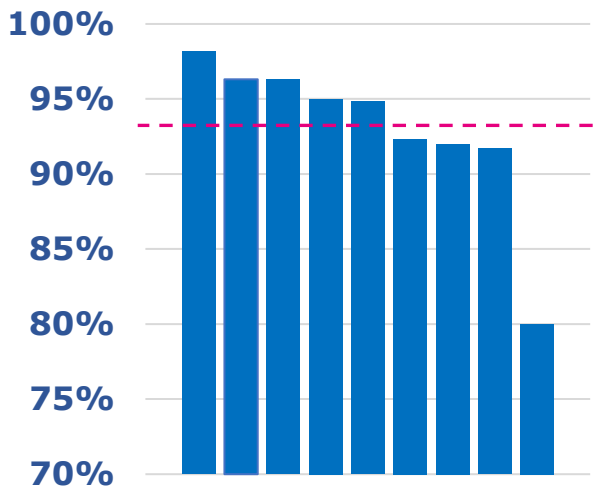
Trainingen over privacy
Een derde van de verzekeraars geeft (nieuwe) medewerkers een basistraining privacy en herhaalt deze vervolgens periodiek, bijvoorbeeld eens in de drie jaar.

Ruim de helft (57%) van de verzekeraars geeft medewerkers met een grotere rol binnen het privacybeleid, bijvoorbeeld een privacy- contactpersoon of ambassadeur, geen aanvullende of uitgebreidere training bovenop de basistraining.

De FG is bij iedere verzekeraar voldoende opgeleid en houdt zijn kennis actueel, bijvoorbeeld door opleidingen en (netwerk)bijeenkomsten te volgen.

Beleid voor het bewaren en verwijderen van e-mails en opgenomen telefoongesprekken
Een derde van de deelnemende verzekeraars heeft een volledig uitgewerkt beleid voor het bewaren van e-mails en opgenomen telefoongesprekken. Ook waarborgt een derde van de verzekeraars periodiek de verwijdering van e-mails en opgenomen telefoongesprekken met daarin persoonsgegevens.

III. Communicatie naar de klant



Benchmarkscore
In het onderdeel Communicatie naar de klant scoren verzekeraars gemiddeld 93%.

Marktbeeld
Een deel van de verzekeraars was zich niet bewust van specifieke vereisten uit de GVPV. Bijvoorbeeld het verwijzen naar de gedragscode in het privacystatement en het actief uitdragen dat een verzekeraar ook persoonsgegevens verwerkt voor de waarborging van de veiligheid en integriteit van de dienstverlening en de sector.

Verder zijn er grote verschillen tussen de diverse privacystatements. De een is kort, bondig en zakelijk terwijl de ander weer uitgebreid, informatief en zeer klantgericht is geschreven.

Algemeen beeld en wat gaat goed

Privacystatement
Alle deelnemende verzekeraars hebben een privacystatement dat goed vindbaar op de website staat. In alle gevallen geeft de verzekeraar duidelijk de rechten van de betrokkene weer. Hoe de klant vervolgens gebruik kan maken van zijn rechten staat bij 78% van de verzekeraars goed en duidelijk beschreven.

De doelen waarom een verzekeraar persoonsgegevens verzamelt en de wettelijke grondslag hiervoor is bij 78% van de verzekeraars duidelijk verwoord. Bij 22% was dit niet volledig duidelijk.

Inzage en correctieverzoeken
Alle deelnemende verzekeraars hebben duidelijke procedures en werkinstructies over hoe verzekeraars opvolging geven wanneer een betrokkene gebruik maakt van zijn rechten. In alle gevallen is er binnen de gestelde reactietermijn gereageerd.

Informeren over het verwerken van persoonsgegevens bij de aanvraag van een verzekering
Alle deelnemende verzekeraars informeren de klant bij het aanvragen van een verzekering duidelijk over het verwerken van persoonsgegevens en verwijzen daarbij naar het privacystatement.

III. Communicatie naar de klant — Wat kan beter

Informatie over het opnemen of registreren van telefoongesprekken en chatsessies
De helft van de verzekeraars heeft in het privacystatement niet of onvoldoende beschreven of het telefoongesprekken en chatsessies opneemt of registreert en waar ze dit vervolgens voor gebruiken.

Voor verzekeraars die geen gebruik maken van het opnemen van telefoongesprekken of het registreren van chatsessies adviseren wij om dit ook expliciet te vermelden in het privacystatement.

Informatie over geautomatiseerde verwerkingen
73% van de deelnemende verzekeraars voert (gedeeltelijk) geautomatiseerde verwerkingen uit. Bij een derde van deze verzekeraars is er geen of onvoldoende informatie in het privacystatement over het (gedeeltelijk) uitvoeren van geautomatiseerde verwerkingen en het recht van de betrokkene om hier bezwaar tegen te maken.

Informeren over het bestaan en de verwerking van persoonsgegevens in een gebeurtenissenadministratie
Een derde van de verzekeraars informeert klanten in het privacystatement of in het fraudebeleid niet of onvoldoende over het verwerken van persoonsgegevens in een gebeurtenissenadministratie.

7. Goede praktijkvoorbeelden

Tijdens onze onderzoeken naar de kerncode GVPV en de Module Kwaliteitsverbetering kwamen we bij verzekeraars allerlei goede praktijkvoorbeelden tegen. We vermelden hier de meest opvallende.

Informatief en duidelijk filmpje op de website over hoe de verzekeraar omgaat met privacy

Twee verzekeraars hebben op de website bij de informatie over privacy een informatief en duidelijk filmpje geplaatst om uitleg te geven over hoe de organisatie omgaat met privacy. Dit is een mooie manier om klanten laagdrempelig te informeren.

Openbaar verwerkingsregister

Enkele verzekeraars hebben (een deel van) het verwerkingsregister openbaar gemaakt en gedeeld op de website. Een best practice hierbij zijn we bij een van de deelnemers aan de Module Kwaliteitsverbetering tegengekomen: de verzekeraar linkt vanuit het privacystatement naar het verwerkingsregister. Het verwerkingsregister is voor zowel intern als extern gebruik gelijk en geeft op een overzichtelijke manier informatie.

Intern onderzoek en audits op privacy

Een aantal verzekeraars heeft voorafgaand aan het onderzoek van Stv een eigen intern onderzoek uitgevoerd op de naleving van de GVPV. Dit geeft verzekeraars meer inzicht over de mate waarin ze voldoen aan de GVPV en geeft verzekeraars vooraf de mogelijkheid om eventuele tekortkomingen te verhelpen.

Interne terugkoppeling over privacy

Een groot deel van de verzekeraars deelt op het intranet informatie over privacy en geeft daarbij toegang tot bijvoorbeeld werkinstructies. We hebben ook een beperkt aantal verzekeraars gezien die het intranet hebben verrijkt met dashboards en rapportages over bijvoorbeeld het aantal datalekken met analyse en toelichting, alle relevante contactpersonen, een overzicht van relevante wet- en regelgeving, inzicht in het verwerkingsregister en een overzicht van verwerkers.

Een actueel verwerkingsoverzicht met behulp van software

Een software tool voor het verwerkingsregister geeft de mogelijkheid om een periodieke uitvraag van de business in te regelen. Dit om te verifiëren of verwerkingen nog actueel zijn. Ook helpt een software tool om risico’s bloot te leggen, de informatieflow en verbanden inzichtelijk te maken en zet het desgewenst de DPIA-uitvoering in gang.

Privacystatement in samenwerking met een tekstbureau

Een van de verzekeraars heeft een tekstbureau betrokken bij het (her)schrijven en visualiseren van het privacystatement. Zo maken ze gebruik van icoontjes om klanten een keuze te laten maken tussen de verschillende informatie. Daarnaast is veel informatie gevisualiseerd.

Duidelijke DPIA keuzehulp
Een aantal verzekeraars gebruikt een DPIA pre-scan of quickscan bij ieder nieuw proces of verwerking om te bepalen of een DPIA nodig is.

Rollen en verantwoordelijkheid privacy(processen)
Enkele verzekeraars hebben uitgebreid de rol van verschillende functies/afdelingen op procesniveau in kaart gebracht. Bijvoorbeeld met behulp van stroomschema's of een RACI.

Een privacybeleid en -statement
Een aantal verzekeraars hebben ervoor gekozen om het (interne) privacybeleid ook aan te houden als privacystatement op de website.

DPIA's op bestaande verwerkingen
Een aantal verzekeraars heeft ook een DPIA op bestaande processen met een hoog risico uitgevoerd. Eén verzekeraar heeft zelfs op ieder bestaand en nieuw proces een DPIA uitgevoerd. Een goed uitgevoerde DPIA is een waardevol middel om mogelijke risico's in kaart te brengen. Vandaar dat het aan te raden valt om deze niet alleen uit te voeren voor processen met een hoog risico die zijn gestart na invoering van de AVG, maar om ook kritisch te kijken naar processen met een hoog risico voor invoering van de AVG.

Periodieke rapportages over het verwijderen van persoonsgegevens
Een aantal verzekeraars heeft vanuit periodieke IT-rapportages of terugkoppeling in een risk control framework goed zicht op de werking van het (automatisch) verwijderen van persoonsgegevens.