Normenkader
Module Kwaliteitsverbetering

Gedragscode Verwerking Persoonsgegevens Verzekeraars

Stichting toetsing verzekeraars

Inleiding

In de Module Kwaliteitsverbetering ligt de focus van ons onderzoek op de verbeterkansen voor de verzekeraar. In dit document beschrijven we wat we toetsen in de Module Kwaliteitsverbetering voor de Gedragscode Verwerking Persoonsgegevens Verzekeraars (GVPV).

Tijdens het onderzoek toetsen we uiteraard ook of de verzekeraar voldoet aan de GVPV, dat toetsen we immers bij alle leden van het Verbond. In de Module Kwaliteitsverbetering gaan we dieper in op het onderwerp, verderop lichten we toe welke onderwerpen we in deze module onderzoeken.

Naast het normenkader ontvangt de verzekeraar een toetsformulier met alle toetspunten van het onderzoek. Daarnaast ontvangt hij een uitvraag met de documenten die we vooraf willen ontvangen en een gespreksschema voor de onderzoeksdagen.

Na de onderzoeksdagen ontvangt u de rapportage met onze bevindingen en aanbevelingen. Daarbij geven we tevens aan of u voldoet aan de gedragscode. Nadat we alle verzekeraars hebben getoetst, maken we een totaalrapportage over alle deelnemende verzekeraars, met bevindingen, goede voorbeelden en een benchmark van de scores.

Score

In het toetsingskader staan alle toetspunten vermeld. Wij scoren uw organisatie op elk toetspunt tussen 0 en 10 punten. De som van de scores zien we als uitkomst van de toets en hanteren we als input voor de benchmark. Er is geen vereiste minimum score in de Module Kwaliteitsverbetering, de module is immers bedoeld om de verzekeraar te helpen zich verder te verbeteren.

Opzet normenkader

Bij dit normenkader hebben we de eisen geordend in de volgende drie onderdelen:

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

We lichten hieronder op hoofdlijnen toe wat we bij elk onderdeel toetsen.

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.

Het privacybeleid gaat in op alle relevante aspecten in de GVPV: privacystatement, rechten van de klant, doelen en grondslagen van de verwerking, functionaris voor gegevensbescherming, verwerkingenregister, gegevensbeschermingseffectbeoordeling, privacy door ontwerp en standaardinstellingen, juistheid van gegevens, beveiliging, datalek, bewaartermijnen, verwerkers en audit. Het privacybeleid beschrijft de relatie

tussen de Product Approval and Review Procedure (PARP) en de Procedure voor een Gegevensbeschermingseffectbeoordeling (hierna: DPIA).

Verder verwachten we van de verzekeraar, dat:
- het privacybeleid en het privacystatement van de verzekeraar verwijzen naar de GVPV;
- het privacybeleid een overzicht bevat van de rechten van de klant en de doelen waarom de verzekeraar persoonsgegevens verzamelt. Ook beschrijft het de positionering en de functie-eisen van de functionaris voor gegevensbescherming (hierna: FG), de criteria wanneer sprake is van een datalek en een opsomming van de verwerkers die de verzekeraar heeft aangesteld;
- de verzekeraar een procedure heeft voor het aanpassen en actueel houden van het privacystatement;
- de verzekeraar een procedure heeft voor het uitvoeren van een DPIA;
- de verzekeraar heeft vastgelegd wat de procedure is voor het tijdig melden van een datalek bij de AP en (op grond van de Wft) voor het informeren van de betrokken klanten;
- de verzekeraar de werking van het beleid evalueert en waar nodig aanpast;
- de verzekeraar periodiek audits uitvoert op het nakomen van de eisen van de GVPV.

Het privacybeleid en de procedures zijn gecommuniceerd naar en bekend bij alle betrokkenen.

De verzekeraar legt bij uitbesteding van taken aan gevolmachtigden of andere dienstverleners, naleving van de GVPV dwingend op in een onderlinge overeenkomst.

De verzekeraar kan voor een aantal belangrijke onderwerpen aantonen dat hij werkt volgens het vastgestelde beleid en procedures.

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.

In dit onderdeel richten we ons op de volgende specifieke aspecten:

Functionaris gegevensbescherming

- de verzekeraar heeft een Functionaris Gegevensbescherming (FG) aangesteld;
- de FG is gepresenteerd aan de organisatie, bekend bij relevante medewerkers en aangemeld bij de Autoriteit Persoonsgegevens (AP);
- de verzekeraar heeft een functieprofiel of rolbeschrijving voor de FG opgesteld. De FG rapporteert aan de hoogste leidinggevende, kan zijn rol onafhankelijk invullen en krijgt voldoende tijd en middelen om zijn taak naar behoren uit te voeren. Hij brengt advies uit over de DPIA's die de verzekeraar uitvoert;
- de verzekeraar betrekt de FG op alle niveaus actief in kwesties over de gegevensbescherming;
- de FG is deskundig op het gebied van wetgeving, gegevensbescherming en de organisatie. Hij geniet ontslagbescherming en heeft geen andere taken die conflicteren met de rol van FG;
- de verzekeraar kan aantonen dat de FG zijn kennis jaarlijks actueel houdt door opleidingen en dat hij bouwt aan een netwerk met externe deskundigen waar hij op kan terugvallen.

Verantwoordelijkheden en vastlegging

- de verzekeraar heeft een verantwoordelijke aangewezen voor het voldoen aan verzoeken door de klant rondom inzage, wijziging en verwijdering van persoonsgegevens. De verzekeraar houdt zich aantoonbaar aan de reactietermijnen die in de GVPV staan;
- de verzekeraar die 'toestemming' gebruikt als rechtsgrondslag om persoonsgegevens te verwerken kan aantonen hoe hij toestemming vraagt aan de klant en legt de toestemming vast;
- de verzekeraar heeft een verantwoordelijke aangesteld voor het beheren van het verwerkingenregister en houdt het verwerkingenregister actueel. Het verwerkingenregister bevat de bewaartermijnen en bevat een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen;
- de verzekeraar heeft de medewerkers die het verwerkingenregister bijhouden en de klantverzoeken verwerken, een uitgebreide training aangeboden over de privacywetgeving en de GVPV;
- de verzekeraar heeft alle overige medewerkers een basistraining aangeboden over dit onderwerp. Onderdeel van de trainingen zijn de richtlijnen voor de medewerkers over hoe zij om moeten gaan met privacygevoelige informatie;
- de verzekeraar kan aantonen dat hij DPIA's uitvoert en dat hij de uitgevoerde DPIA's documenteert;
- de verzekeraar heeft een verantwoordelijke aangesteld voor de registratie van de datalekken die plaatsvinden. Datalekken meldt hij binnen 72 uur bij de AP.

Verwerkers

- de verzekeraar heeft een modelovereenkomst opgesteld om de afspraken met zijn verwerkers vast te leggen;
- de verzekeraar heeft aantoonbaar afspraken gemaakt met partijen in de keten aan wie hij persoonsgegevens verstrekt (verwerkers) en met partijen in de keten van wie hij persoonsgegevens ontvangt, om te kunnen voldoen aan verzoeken van de klant om persoonsgegevens te wijzigen of te verwijderen;
- de verzekeraar kan aantonen dat hij de verwerkers monitort op de naleving van de gemaakte afspraken.

III Communicatie met 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.

In dit onderdeel richten we ons op de volgende specifieke aspecten:

Privacystatement

- de verzekeraar heeft een privacystatement op de website staan;
- in het privacystatement vermeldt hij zijn identiteit en contactgegevens;
- het privacystatement beschrijft het recht van de klant op inzage, wijziging en verwijdering van zijn persoonsgegevens en het recht op verzet tegen de verwerking van zijn persoonsgegevens;
- de verzekeraar vermeldt in het privacystatement welke categorieën persoonsgegevens hij verzamelt, via welke bronnen hij dit doet, de doelen waarom hij persoonsgegevens verzamelt en de rechtsgrondslagen die hij daarbij hanteert;
- de verzekeraar vermeldt of en met welk doel hij gezondheidsgegevens en strafrechtelijke gegevens verwerkt. Hij vermeldt expliciet dat voor gezondheidsgegevens een geheimhoudingsplicht geldt en dat hij gegevens deelt met andere instanties, zoals CIS;
- de verzekeraar vermeldt in het privacystatement de bewaartermijn van de gegevens van de klant;

- de verzekeraar geeft een toelichting op hoe hij eventuele geautomatiseerde besluitvorming heeft ingericht en vermeldt het recht van de klant om daar niet aan onderworpen te worden;
- het privacystatement beschrijft verder het recht van de klant op beperking van de verwerking van zijn gegevens en op overdracht van zijn gegevens;
- de verzekeraar publiceert in het privacystatement de contactgegevens van de FG;
- de verzekeraar vermeldt in het privacystatement de ontvangers of categorieën van ontvangers van de persoonsgegevens die hij verzamelt;
- het privacystatement bevat informatie over plaatsing van cookies, registratie van bezoek aan website, gebruik van apps en het opnemen/registreren van telefoongesprekken en chatsessies;
- het privacystatement bevat informatie over hoe de klant klachten over de gegevensverzameling kan uiten en hoe hij zijn rechten kan uitoefenen. De verzekeraar maakt het de klant die zijn rechten wil uitoefenen zo makkelijk mogelijk;
- het privacystatement is goed vindbaar op de website;
- in het privacystatement maakt de verzekeraar duidelijk onderscheid tussen hoofd- en bijzaken;
- het privacystatement is opgesteld in begrijpelijke taal;
- het privacystatement bevat een ingangsdatum en is goed leesbaar op een mobiele telefoon.

Informeren

- voorafgaand aan een verwerking voor een ander doel dan waarvoor hij de gegevens verzameld heeft, informeert de verzekeraar de betrokkene;
- de klant kan in de mijn-omgeving relevante persoonsgegevens (NAW, bankrekeningnummer) zelf wijzigen. Wijzigingen waar de klant om verzoekt, of die de klant in de mijn-omgeving aanpast, verwerkt de keurmerkhouder in alle producten die de klant bij hem heeft;
- de verzekeraar informeert de klant in de aanvraagmodule voor een verzekeringsproduct over hoe hij omgaat met de verzameling van persoonsgegevens.