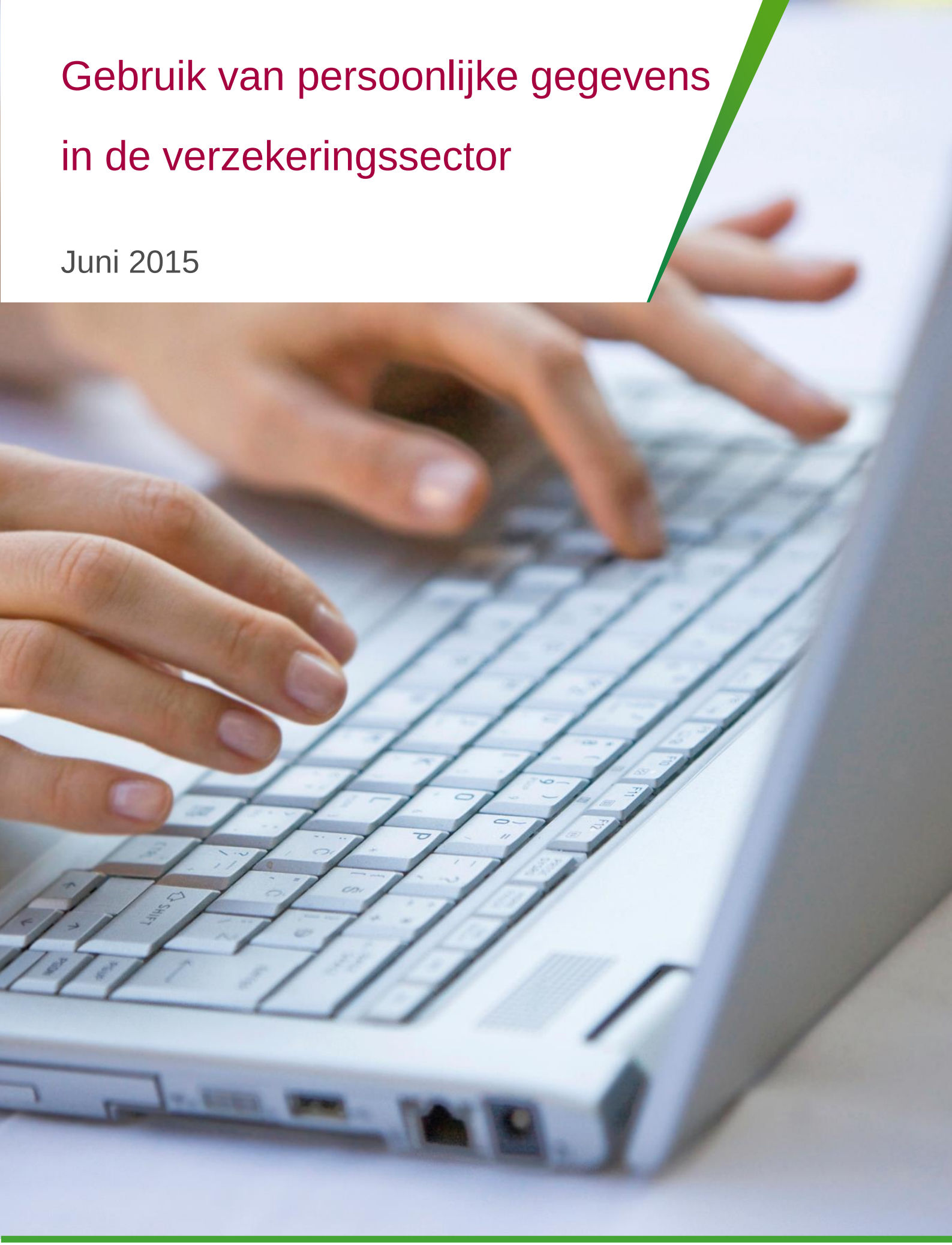
Gebruik van persoonlijke gegevens in de verzekeringssector

Juni 2015



VERBOND VAN VERZEKERAARS

Inhoud

1. Management summary

"Privacy is niet alleen een kwestie van wetgeving, maar ook van vertrouwen en integriteit."

Verzekeraars staan voor enorme uitdagingen. De technologische vooruitgang biedt kansen, maar er zijn ook bedreigingen. Hamvraag is hoe de juiste balans kan worden gevonden. Een balans tussen zorgvuldig omgaan met persoonlijke gegevens aan de ene kant en kansen pakken aan de andere kant. In die zoektocht is een dialoog tussen de verzekeringssector en de samenleving noodzakelijk. Het Verbond heeft tien uitganspunten/aanbevelingen opgesteld die de basis vormen om de dialoog te starten.

1.1 Het gebruik van persoonlijke gegevens in een digitaal tijdperk

We hoeven er niet veel woorden aan te wijden. De mogelijkheden tot verzamelen, opslaan en koppelen van persoonlijke gegevens nemen in rap tempo toe. Door ontwikkelingen als Big Data en cloud computing, maar zeker ook door de enorme vlucht van social media. De wetgever moet handvatten bieden, maar kan de ontwikkelingen amper bijhouden. Gevolg is onzekerheid en mede daardoor is er een brede maatschappelijke discussie ontstaan over de balans tussen het gebruik van persoonlijke gegevens én de bedreigingen voor de privacy.

In dit visiedocument hebben we geen kant-en-klare antwoorden, maar we willen wel graag de bewustwording vergroten, een richting aangeven voor toekomstig beleid en de dialoog tussen de sector en de samenleving over mogelijkheden en onmogelijkheden op gang brengen.

1.2 Uitgangspunten voor dialoog

Zoals gezegd hebben we daarvoor tien uitgangspunten opgesteld, die in hoofdstuk zeven nader aan bod komen. Kort samengevat:

1. De sector heeft persoonlijke gegevens nodig om zijn kerntaak te kunnen uitvoeren.
2. Vanzelfsprekend gaan verzekeraars integer met de gegevens van de klant om.
3. Verzekeraars moeten hun klanten goed uitleggen wat er wel en niet wordt gedaan met hun gegevens en waarom.
4. Verzekeraars moeten zich niet alleen bewust zijn van de wettelijke kaders, maar ook van sociale en culturele opvattingen bij het gebruik van persoonlijke gegevens.
5. Door de exponentiele groei van (Big) data zullen verzekeraars met een specifieke visie moeten komen op het gebruik daarvan.
6. De overheid heeft als wetgever de taak om kaders te bieden waarbinnen gegevens mogen worden gebruikt. Flexibiliteit en duidelijkheid zijn echter van belang.
7. De overheid moet daarnaast het gelijke speelveld tussen marktpartijen bewaken.
8. Verzekeraars hebben, net als andere partijen, behoefte aan vroegtijdig advies en overleg met de toezichthouder/overheid om een goede vertaalslag van wet naar praktijk te kunnen maken.
9. Klanten moeten zich bewuster worden van privacy en de kansen inzien van nieuwe toepassingen.
10. Verzekeraars, overheid, toezichthouders en klanten moeten gezamenlijk waken over het behoud van het solidariteitsprincipe door informatiegelijkheid.

1.3 Bewustwording rondom gebruik van persoonlijke gegevens

Intussen zitten wij niet stil. Integendeel. Belangrijk is om de bewustwording aan te wakkeren en het gesprek met de samenleving aan te gaan. Wij zullen onze uitgangspunten bij stakeholders en consumenten onder de aandacht (blijven) brengen om de dialoog te starten. Mogen we daarnaast op u rekenen als het gaat om een standpuntbepaling op het gebruik van persoonlijke gegevens in de verzekeringssector?

2. Inleiding

De wensen in het gebruik van persoonlijke gegevens nemen enorm toe. Toepassingen als Big Data, social media en cloud computing vergroten de mogelijkheden in het verzamelen, opslaan, koppelen en analyseren van (persoonlijke) gegevens. De wetgeving die handvatten moet bieden, is daar nog niet voldoende op toegespitst, terwijl de ontwikkelingen in rap tempo doorgaan. Dit heeft een brede maatschappelijke discussie losgemaakt over
de mogelijkheden en kansen versus de grenzen en bedreigingen. Die discussie is nog lang niet uitgekristalliseerd en vanzelfsprekend denken ook verzekeraars hierover na.

Hoe kunnen verzekeraars zorgvuldig omgaan met persoonlijke gegevens en toch de kansen pakken die nieuwe technologieën bieden? Dat is de hamvraag die moet worden beantwoord. Een pasklare oplossing is op dit moment nog niet voorhanden, maar dit document geeft wel een schets van de huidige ontwikkelingen, met aanknopingspunten voor het toekomstig beleid van het Verbond van Verzekeraars op het gebruik van persoonlijke gegevens. Maar ook om de bewustwording bij verzekeraars te vergroten wat betreft het gebruik van persoonlijke gegevens via nieuwe technologieën. Dit visiedocument biedt uitgangspunten om de dialoog binnen de verzekeringssector en tussen de verzekeringssector en de samenleving over de (on)mogelijkheden in het gebruik van persoonlijke gegevens op te starten en richting te geven.

Het document start met een beknopte uitleg over nut en noodzaak van het gebruik van persoonsgegevens door verzekeraars. Vervolgens wordt ingezoomd op de wettelijke context en de waarborgen die de verzekeringssector zelf stelt voor een zorgvuldig gebruik van persoonsgegevens. Daarna volgt een algemene analyse van de meest invloedrijke tendensen in het gebruik van persoonsgegevens. Vervolgens wordt ingegaan op de mogelijkheden, grenzen en dilemma´s waar verzekeraars voor staan. Wat zijn eventuele kansen en bedreigingen bij het ontwikkelingen van nieuwe toepassingen? We sluiten het document af met conclusies en uitgangspunten voor de verdere dialoog.

3. Gebruik van persoonsgegevens is noodzakelijk

Het gebruik van persoonlijke gegevens is onontbeerlijk voor de bedrijfsvoering en de kerntaken van verzekeraars. Zonder die gegevens kunnen zij geen adequate risico-inschatting maken en komt hun kerntaak (zekerheid bieden) in het gedrang. Het verwerken van persoonsgegevens is dus noodzakelijk voor de uitvoering van de verzekeringsovereenkomst en het kunnen maken van een risico-inschatting. Deze twee elementen vormen samen de kern van het verzekeringswezen. Daarnaast zijn persoonsgegevens noodzakelijk voor het waarborgen van de integriteit en veiligheid binnen het verzekeringsbedrijf. De wetgever heeft dit ook erkend door in de Wet bescherming persoonsgegevens (Wbp) specifieke bepalingen op te nemen die hierop toezien.

“Het verwerken van persoonsgegevens is noodzakelijk voor het kunnen maken van een risico-inschatting.”

Het verzekeringsprincipe is gebaseerd op solidariteit. Dat betekent dat iedereen meebetaalt om het verzekeringsvangnet te bieden. Om dit vangnet te kunnen blijven bieden, maakt een verzekeraar een inschatting van het te verzekeren risico dat een activiteit, persoon of object met zich meebrengt. Op basis van dat risico bepaalt hij of de verzekering wordt afgesloten, de hoogte van de dekking en de hoogte van de premie.

Bij het berekenen van de risico's gebruiken verzekeraars uiteenlopende gegevens. Uiteraard is dat afhankelijk van het te verzekeren risico, maar vaak zijn dit persoonsgegevens als leeftijd of gegevens over de gezondheid. Soms zijn ook andersoortige gegevens nodig, zoals informatie over een verzekerd object. Denk maar aan een woning of een auto. En verzekeraars hebben persoonlijke gegevens nodig in het kader van criminaliteitsbestrijding. Het kan daarbij gaan om fraude met claims, maar ook om het voorkomen van witwassen, terrorisme financiering, cybercrime of andere vormen van financiële criminaliteit die de integriteit van de sector kunnen bedreigen.

Ten slotte mogen verzekeraars onder bepaalde voorwaarden ook persoonsgegevens gebruiken voor marketingdoeleinden en voor het uitvoeren van statistisch onderzoek. In de telecommunicatiewet is aanvullende regelgeving opgesteld onder welke condities klanten commercieel mogen worden benaderd. De verzekeringsovereenkomst bevat de afspraken met de klant rondom de risico-inschatting, claimafhandeling, uitvoering van statistisch onderzoek en een eventuele rechtstreekse benadering van klanten voor marketingactiviteiten.

4. Waarborgen ter bescherming van persoonsgegevens

Tegelijkertijd schrijft de wetgever in diezelfde Wbp de waarborgen voor die verzekeraars moeten hanteren om klanten te beschermen. Verzekeraars hechten veel waarde aan een correct gebruik van persoonsgegevens en geven hier, onder meer via een breed scala aan zelfregulering, invulling aan.

"De verzekeringssector heeft de nodige branchegerichte regelgeving opgesteld om privacywaarborgen te bieden."

De Wbp bepaalt de kaders waarbinnen persoonsgegevens mogen worden verwerkt. Wettelijk gezien zijn persoonsgegevens: "iedere informatie betreffende identificeerbare of geïdentificeerde natuurlijke personen". Hieronder vallen gegevens als naam, adres, woonplaats en geboortedatum, maar ook een kentekenplaat of gezondheidsgegevens. Uitgangspunt van de Wbp is een minimale inbreuk op de privacy door een minimaal gebruik van die persoonlijke gegevens. Dat betekent dat alleen die persoonsgegevens worden gebruikt die noodzakelijk zijn voor een vooraf bepaald en duidelijk omschreven doel. Ook moet er een dringende reden zijn om persoonsgegevens te verwerken. Bij verzekeraars is dat bijna altijd het kunnen uitvoeren van de verzekeringsovereenkomst. Tot slot moet er sprake zijn van een adequate beveiliging van de persoonsgegevens.

De verzekeringssector heeft in aanvulling op de wetgeving de nodige branchegerichte regelgeving opgesteld om privacywaarborgen te bieden. De Gedragscode Verwerking Persoonsgegevens Financiële Instellingen[1] biedt een praktijkgerichte interpretatie van de open Wbp-normen. Deze zelfregulering biedt kaders voor verzekeraars, maar is er ook op gericht de privacybelangen en rechten van de consument duidelijk te maken en te beschermen. Verzekeraars hebben in hun

[1] https://www.verzekeraars.nl/overhetverbond/zelfregulering/Paginas/Gedragscodes/Gedragscode-Verwerking-Persoonsgegevens.aspx

polisvoorwaarden en privacy statements opgenomen wat ze met de gegevens doen.

Naast deze overkoepelende Gedragscode, die zich richt op het gebruik van alle persoonsgegevens, is er ook zelfregulering opgesteld die zich volledig toespitst op bijzonder privacygevoelige gegevens, waaronder gezondheidsgegevens.
Verzekeraars hebben in het Protocol Verzekeringskeuringen[2] een nadere uitwerking gegeven aan de grenzen en vereisten die in de Wet op de Medische Keuringen (WMK) al zijn vastgelegd. De verzekeraar zorgt ervoor dat de medische gegevens alleen worden verwerkt door een medisch adviseur, en zodanig worden bewaard in de organisatie dat geheimhouding van de inhoud is verzekerd. Daarnaast zijn er extra waarborgen vastgelegd rondom medische informatie in de HIV gedragscode en het Moratorium erfelijkheidsonderzoek. Zo mag medewerking aan erfelijkheidsonderzoek nooit een voorwaarde zijn voor het afsluiten van een verzekering.

Voor het gebruik van persoonlijke gegevens in het kader van fraudepreventie en de waarborging van integriteit en veiligheid is ook zelfregulering opgesteld. Als mensen misbruik maken van de producten en diensten van verzekeraars, wordt dat vastgelegd in een incidentenregister. Het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen ziet toe op de (wettelijke) eisen waaraan verzekeraars moeten voldoen bij het vastleggen van een incident[3] en het delen van de daarin opgenomen informatie met andere verzekeraars.

5. Trends in het gebruik van persoonsgegevens

Er is een aantal belangrijke trends die het daadwerkelijke gebruik, maar ook het denken over gegevensgebruik beïnvloeden: opkomende technologie, nieuwe verdienmodellen, veranderende sociale normen/waarden en het politieke speelveld. Begrip van deze tendensen is van groot belang om de valkuilen/successen te kunnen begrijpen. Overigens zijn deze trends niet specifiek voor de verzekeringssector, maar spelen ze zich af binnen meerdere sectoren in het bedrijfsleven en de overheid.

5.1 Technologische trend: Big Data, cloud computing, sensor technologie

Digitalisering en globalisering zorgen ervoor dat gegevens gemakkelijker zijn te verzamelen, te verspreiden, te koppelen en op te slaan, zelfs over landsgrenzen heen. Data zijn altijd en overal toegankelijk via met elkaar communicerende devices. Big Data stelt bedrijven bovendien in staat om op enorme schaal gegevens te verzamelen en gedetailleerde profielen op te stellen over de voorkeuren van een groep klanten. Dit betekent dat persoonlijke gegevens steeds wijder verspreid en makkelijker toegankelijk worden. Mensen delen informatie sneller en makkelijk wat het inzicht in hun gedrag vergroot. Data uit bronnen die op zichzelf geen tot personen te herleiden gegevens bevatten, kunnen door een slimme combinatie van die data wel weer leiden tot inzichten over een specifieke persoon.

“Persoonlijke gegevens worden steeds wijder verspreid en makkelijker toegankelijk.”

5.2 Economische trend: nieuw verdienmodel

Persoonsgegevens hebben een steeds grotere economische waarde. De handel in gegevens neemt toe, er komen steeds meer commerciële aanbieders die grote datasets met klantgegevens aan-, ver- en doorverkopen. Het combineren van gegevens uit diverse bronnen van data, zoals sociale media kan leiden tot nieuwe inzichten die bijvoorbeeld gebruikt kunnen worden om fraude met verzekeringen tegen te gaan.[4]

Daarnaast ontstaan er nieuwe verdienmodellen.[5] Diensten worden betaald door persoonlijke gegevens af te geven. De gegevens zijn als het ware wisselgeld voor meer service, gemak of een korting. Door het

[2] https://www.verzekeraars.nl/overhetverbond/zelfregulering/Paginas/Protocollen/Protocol-Verzekeringskeuringen.aspx
[3] https://www.verzekeraars.nl/overhetverbond/zelfregulering/Paginas/Protocollen/Protocol-Incidentenwaarschuwingssysteem-Financi%c3%able-Instellingen.aspx

[4] Casus van Aegon die via onderzoek op Facebook er achter kwam dat een verzekerde een arbeidsongeschiktheidsuitkering kreeg terwijl hij gezond was. De rechtbank heeft de verzekeraar daarbij in het gelijk gesteld.
[5] Boston Consulting Group voorspelt dat in 2020 big data in Europa 1 biljard euro zal vertegenwoordigen.

verzamelen van persoonlijke gegevens is ook gerichte(re) advertising mogelijk, omdat je makkelijker kunt aansluiten bij de voorkeuren van de klant. De inkomsten uit targeted advertising en profiling stijgen dan ook enorm. Via tracking cookies is het voor bedrijven gemakkelijk om surfgedrag te volgen, waardoor het reclameaanbod kan worden afgestemd op het koopgedrag.

De keerzijde hiervan is dat consumenten steeds minder vrijheid hebben in het niet verstrekken van persoonlijke gegevens. Het ontbreken van een level playing field kan zorgen voor wantrouwen. Dit betekent dat de voorwaarden en het voordeel voor de consument vooraf kraakhelder moeten zijn. Geen verrassingen achteraf.

5.3 Sociale trend: wat is acceptabel?

Culturele en sociale waarden bepalen wat gevoelige persoonlijke informatie is en wat niet. De opvattingen over privacy en wat gevoelige gegevens zijn verschillen per land, per persoon en veranderen ook nog eens door de tijd en over generaties heen. Een Amerikaan zal zonder schroom vertellen wat hij verdient, terwijl een Nederlander dat het liefst voor zich houdt.

Persoonlijke gegevens worden gezien als gegevens die van ‘mij’ zijn. Autonomie is een belangrijk element. Niet iedereen, denk aan gezin, vrienden, collega’s of werkgever, krijgt dezelfde persoonlijke gegevens ter beschikking.[6] Tegelijkertijd heb ‘ik’ geen exclusief zeggenschap over het gebruik van die gegevens. Dat zorgt soms voor frictie, met name als er verrassingen achteraf volgen. Daarnaast wordt de samenleving steeds individualistischer. Consumenten willen een product dat bij hen past. Ook uiten ze hun mening over de geboden service en het functioneren van een product via sociale media, zoals Facebook, waardoor negatieve reacties snel een groot publiek kunnen bereiken en gehoor vinden.

Dit betekent dat de grens tussen wat wel en niet acceptabel is, dun kan zijn. Het niet meenemen van sociale en culturele normen kan het in de markt zetten van nieuwe diensten of producten frustreren, met imagoschade tot gevolg. Het elektronisch patiënten dossier, de Equens-pilot en de ING-pilot zijn enkele voorbeelden die dit illustreren.[7]

5.4 Politieke en wettelijke trend: noodzaak striktere regels en transparantie

Consumenten zullen hun gegevens eerder toevertrouwen aan een bedrijf dat goede privacywaarborgen biedt. Ook de overheid en toezichthouder zullen minder snel ingrijpen met regelgeving en boetes als een bedrijf transparant is over het gebruik van persoonlijke gegevens en goede waarborgen heeft ingesteld. Intransparantie en negatieve media-aandacht zorgen voor wantrouwen bij burgers en bij het parlement. Niet alleen ten opzichte van bedrijven, maar ook in zekere mate richting de overheid.[8] Er ontstaat een verkrampte reactie om onzekerheden zoveel mogelijk te ondervangen. Meer en striktere regels en scherper toezicht moeten dan uitkomst bieden. Dit is terug te zien in de roep om een betere bescherming van persoonlijke gegevens en heldere kaders op nationaal en Europees niveau.[9] Het gevaar bestaat echter dat deze regels hun doel voorbij schieten.[10]

[6] http://netherlands.emc.com/campaign/privacy-index/netherlands.htm

[7] Maart 2014 maakte ING bekend een pilot te starten met betalingsgegevens. In 2013 had betalingsverwerker Equens al plannen om de transactiegegevens van pinbetalingen in Nederland te verkopen aan winkeliers. Uiteindelijk werd deze onder druk van politiek, consumentenorganisaties en toezichthouders gestaakt. Het EPD is op basis van privacy bezwaren nooit van de grond gekomen en heeft de maatschappij uiteindelijk een verlies van 300 miljoen euro opgeleverd.

[8] Zie EMC privacy index, http://netherlands.emc.com/campaign/privacy-index/index.htm Nederlanders verwachten privacy van overheid

[9] Zie www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2012)0011_/com_com(2012)0011_nl.pdf voor de tekst van de Verordening.

[10] De cookiewetgeving is daar een voorbeeld van. De informatieplicht en het vragen van toestemming leidde tot een explosie van pop-ups met een averechts effect op het

"Bedrijven moeten steeds meer investeren om aan te tonen dat ze aan de wettelijke verplichtingen voldoen."

Die striktere regelgeving komt er op korte termijn aan, in de vorm van de Europese Algemene verordening gegevensbescherming. De uitgangspunten van de huidige Richtlijn zijn aangescherpt en zo veel mogelijk afgestemd op de technologische ontwikkelingen in gegevensverzameling, opslag, analyse en toepassingsmogelijkheden. Het geven van toestemming door de consument en de belangenafweging in gegevensgebruik, wegen nog zwaarder in de toekomstige wetgeving. Dit met als doel de consument meer controle en grip te bieden. Nieuw zijn het '"recht om vergeten te worden'", de meldplicht datalekken en verplichting tot het aanstellen van een Data Protection Officer.[11] De toezichthouder krijgt meer mogelijkheden om op te treden tegen misbruik en de boetes gaan spectaculair omhoog. Een boete kan oplopen tot honderd miljoen of vijf procent van de jaaromzet.

Het signaal is duidelijk. Bedrijven moeten steeds meer investeren om aan te tonen dat zij aan deze wettelijke verplichtingen voldoen. Dat vergt een privacy check voorafgaand aan de ontwikkeling van nieuwe diensten en producten, privacymaatregelen op maat (privacy by design en privacy by default) én transparantie door heldere communicatie over het gebruik van persoonlijke gegevens.

6. Mogelijkheden, grenzen en dilemma's?

De mogelijkheden die nieuwe technologische toepassingen bieden, zijn nog niet uitgekristalliseerd. Nog lang niet zelfs. Nieuwe toepassingen in gegevensgebruik kunnen kansen bieden om de service te verbeteren. Een verzekeraar kan immers nieuwe diensten ontwikkelen die beter zijn afgestemd op de behoeften en wensen van de klant. Dit zou kunnen leiden tot nieuwe bronnen van inkomsten en een optimalisering van de infrastructuur. Verzekeraars bevinden zich, op enkele starts-ups na, nog in de beginfase. Ze verkennen momenteel de opties en lopen daarbij tegen een aantal grenzen en dilemma's aan.

6.1 Mogelijkheden: dashcams en wearable devices

De sector experimenteert bijvoorbeeld met het inzetten van dashcams en andere apparatuur die rijgedrag kan monitoren. Het inzetten van dashcams is nog lang geen breed ingezet middel en de verdere toepassingsmogelijkheden zijn nauwelijks uitgerold. Zo kunnen de gegevens die bij het monitoren van rijgedrag over de verkeerssituatie worden verzameld, worden ingezet bij het verbeteren van de verkeersveiligheid. Kortom, perspectief op nieuwe markten, nieuwe producten, meer maatwerk, betere service en nog betere risico-inschattingen waardoor de schadelast beheersbaar blijft.

Daarnaast is de opkomst van de wearable devices een feit. Deze devices verzamelen continue gegevens over iemands gedrag: zoals het aantal stappen dat hij vandaag heeft gezet, aantal uren slaap, de hoogte van de hartslag en zijn bloeddruk. Er zijn apps waarmee het eetpatroon in kaart wordt gebracht, en vervolgens wordt berekend hoeveel calorieën zijn ingenomen en welk effect dat heeft op gewicht en BMI. Een verzekeraar zou deze informatie goed kunnen gebruiken bij het in kaart brengen van gezondheidsrisico's.

beoogde doel. In plaats van bewustwording, zorgde het voor irritatie en gedachteloos wegklikgedrag bij gebruikers.

[11]Consumenten mogen van bedrijven (met name zoekmachines), eisen dat zij onjuiste of verouderde gegevens verwijderen. Bedrijven zijn verplicht lekken van persoonlijke gegevens, te melden aan de toezichthouder én de consument. Aanstellen van een Data Protectie Officer is verplicht bij 5000 records of meer van verschillende personen.

6.2 Wettelijke grenzen: profilering en doelbinding

Profilering en doelbinding zijn belangrijke kernpunten in de discussie over het gebruik van persoonlijke gegevens door nieuwe technologische toepassingen. Profilering is het verzamelen, analyseren en combineren van (persoons)gegevens, met als doel iemand in te delen in een bepaalde categorie. Profilering wil dus zeggen dat iemand aan de hand van een profiel wordt beoordeeld.[12] Profilering mag niet leiden tot discriminatie (onderscheid op basis van geslacht, geloof, ras et cetera). De Wet gelijke behandeling trekt daar een heel duidelijke grens.

Profilering brengt wel een aantal risico's met zich mee. Het inzetten van Big Data en profilering is vaak gebaseerd op een grote set gegevens waar vervolgens automatisch formules op los worden gelaten. Uit de gedragswetenschap blijkt dat menselijk gedrag complex is. Misschien zelfs te complex om te vatten in rekenkundige formules. Ook leveren rekenkundige modellen, die de basis vormen voor de profielen, altijd een gemiddelde op. En zelfs al past een individu in een bepaald profiel op basis van objectieve kenmerken, dan wil dat nog niet zeggen dat het profiel daadwerkelijk op dat ene individu van toepassing is.[13]

In de verzekeringspraktijk speelt profilering een cruciale rol in bij het maken van een risico-inschatting. De risico-inschatting is noodzakelijk om de vangnetfunctie van verzekeraars, gebaseerd op solidariteit, te kunnen blijven bieden. Doordat grote risico's een hogere premie betalen dan kleine risico's, blijft de solidariteit in stand. De kleine risico's zullen immers, gegeven de geringere prijs, bereid blijven de premie te betalen. En de hogere risico's zullen, gegeven hun hogere risico, ook bereid zijn wat meer te betalen. Als iedereen dezelfde premie zou betalen, ontstaat het gevaar dat de kleine risico's overwegen de verzekering op te zeggen (kosten-baten afweging), waardoor alleen grote risico's zich willen verzekeren en de premie op blijft lopen, totdat uiteindelijk niemand zich meer fatsoenlijk kan verzekeren.

De wetgeving gaat uit van een strikte doelbinding. In de huidige praktijk kunnen door het combineren van data uit diverse bronnen inzichten in gedrag ontstaan die van groot maatschappelijk nut zijn, maar niet mogen worden ingezet. Simpelweg omdat ze niet passen binnen het vooraf gestelde doel. Toestemming vragen is niet altijd werkbaar. In de nieuwe Europese verordening worden het doelbindingsprincipe, de toestemmingvereisten en de voorwaarden voor profilering flink aangescherpt. Hoe dat precies uitwerkt, zal moeten blijken na de definitieve vaststelling. De huidige en aankomende wetgeving is in ieder geval onvoldoende ingericht op veranderingen in het gegevensgebruik. Het bedrijfsleven heeft daardoor niet genoeg houvast. En de angst om de wet te overtreden, kan een rem zetten op nieuwe ontwikkelingen. Het zou dan ook wenselijk zijn als de overheid en het College Bescherming Persoonsgegevens (CBP) openstaan voor vragen uit de markt op dergelijke ontwikkelingen.

6.3 Dilemma's: solidariteit, nudging en eigenaarschap

6.3.1 Afname solidariteit versus toename individualisering

Het gebruik van Big Data en sensortechnologie maakt een betere risicoschatting en op maat premieberekening mogelijk. Onderzoek toont ook aan dat klanten bereid zijn persoonsgegevens door te geven aan een verzekeraar als dat leidt tot voordeel.[14] Een gezonde of 'veilige' leefstijl leidt tot een korting op de premie, dat lijkt eerlijk. Want waarom zou

[12]College Bescherming Persoonsgegevens, Profilering, https://cbpweb.nl/nl/onderwerpen/reclame-profiling/profilering

[13]College Bescherming Persoonsgegevens over profilering: www.mijnprivacy.nl/Vraag/profilering/Paginas/Profilering.aspx

[14]Rapport van PWC: http://www.pwc.nl/nl/verzekeraars/toekomst-van-verzekeraars.jhtml

iemand met een gezonde leefstijl (sportief, eet gezond, slaapt genoeg) meer moeten betalen dan iemand die ongezond leeft (onsportief, kettingrokend)? En waarom zou een bewuste automobilist meer moeten betalen voor zijn autoverzekering dan een roekeloos rijdende automobilist?

Premie- en risicodifferentiatie zijn nodig om het verzekeringssysteem in stand te houden. Maar als beide te ver doorschieten, vormen ze een bedreiging voor het verzekeringssysteem. Naarmate de premiedifferentiatie toeneemt, worden de verschillen in premie tussen de hoogste en laagste risico's steeds groter. Meer differentiatie in het risico kan er uiteindelijk toe leiden dat klanten met een hoog risicoprofiel de premie niet meer willen of kunnen betalen. Dit is zowel vanuit de klant als vanuit de verzekeraar bezien onwenselijk.

6.3.2 Nudging versus big brother

In het kader van preventie kan, op basis van Big Data, schade worden voorkomen. Informatie over een ongezonde leefstijl kan bijvoorbeeld op een positieve manier worden ingezet. De verzekeraar kan een signaal afgeven en enkele gezondheidstips meegeven om het leefpatroon te verbeteren. Een duwtje in de goede richting kan soms helpen. Kleine prikkels kunnen ertoe leiden dat klanten hun gedrag aanpassen, waardoor de totale schadelast (en daarmee de premie) voor alle klanten kan dalen. De vraag hierbij is wel of een verzekeraar vanuit zijn rol gezondheidstips moet geven en, in het verlengde daarvan, of verzekerden dat prettig of juist bemoeizuchtig vinden?

De vraag rijst of de klant wel wil dat sommige analyses mogelijk worden? Klanten kunnen door de steeds verder reikende mogelijkheden, het onbehaaglijke gevoel krijgen dat de verzekeraar wel erg veel te weten kan komen. Te snelle, grote en onduidelijke stappen in het gebruik van nieuwe technologie heeft dus het risico dat er een gevoel van wantrouwen ontstaat richting de verzekeraar.

6.3.3 Eigenaarschap versus toegang tot gegevens

Daarnaast is er het vraagstuk van eigenaarschap van gegevens en informatie(on)gelijkheid. De verzekerde zal over steeds meer en nauwkeuriger gegevens over onder meer zijn gezondheid gaan beschikken. Hij kan zoveel informatie over zichzelf afleiden dat hij ook een beter inzage kan krijgen in zijn eigen risico en een kennisvoorsprong kan opbouwen ten opzichte van zijn verzekeraar. Ook dit kan het solidariteitsprincipe ondermijnen, omdat alleen klanten die een hoog risico lopen (op basis van hun eigen kennisvoorsprong) zich melden bij een verzekeraar en klanten met een laag risico juist niet.

"Heeft degene met de beste toegang tot persoonlijke gegevens ook de meeste macht?"

Daarnaast komen er mogelijk nieuwe toetreders op de verzekeringsmarkt die strikt gereguleerd is. Hoe werkt dat uit als we het hebben over een level playing field, zowel voor de klant de verzekeraar? Heeft degene met de beste toegang ook de meeste macht?

Het is aan de sector zelf om dergelijke vraagstukken verder uit te diepen en een passende oplossing te vinden, waarbij de verzekeraars nieuwe producten en diensten kunnen aanbieden die de belangen van de klant en de verzekeraar verbinden. Eigenaarschap en regie, voorzienbaarheid en wenselijkheid spelen hierbij een grote rol.

7. Conclusies en uitgangspunten voor dialoog

Samengevat is het gebruik van persoonlijke gegevens onontbeerlijk voor de bedrijfsvoering en kerntaken van verzekeraars. Verzekeraars hechten veel belang aan een zorgvuldige omgang met persoonlijke gegevens en implementeren diverse vormen van zelfregulering om dit te waarborgen. Er zijn een aantal invloedrijke trends op het gebied van gegevensbescherming en gebruik waar verzekeraars rekening mee moeten houden:

- Persoonlijke gegevens worden door nieuwe technologische ontwikkelingen als sociale media, Big Data, sensor technologie en cloud computing, steeds wijder verspreid en toegankelijk;
- Persoonlijke gegevens krijgen in snel toenemende mate een stijgende economische waarde als grondstof voor het leveren van een dienst en als betaalmiddel voor het afnemen van een dienst;
- Sociale en culturele normen spelen een grote rol in de perceptie rondom acceptabel gebruik van persoonlijke gegevens. Deze normen zijn dynamisch en verschillen per individu en per regio;
- Een gebrek aan vertrouwen en negatieve media-aandacht zorgt voor verscherpt toezicht en striktere regelgeving rondom het gebruik van persoonlijke gegevens.

De positieve kant van meer mogelijkheden in het gebruik van gegevens is dat dit kansen biedt in het verbeteren van de dienstverlening en bijvoorbeeld het voorkomen en bestrijden van fraude. Het biedt mogelijkheden tot een meer individueel op maat gemaakt aanbod van producten en tot nieuwe verdienmodellen.

“Privacy is niet alleen een kwestie van wetgeving, maar ook van vertrouwen en integriteit.”

De keerzijde is dat klanten overzicht en grip kunnen verliezen op de verspreiding van hun gegevens en de effecten daarvan niet goed kunnen overzien. Consumenten hebben steeds minder vrijheid in het niet verstrekken van persoonlijke gegevens. Het ontbreken van regie en een level playing field werken wantrouwen bij de consument in de hand.

Privacy is niet alleen een kwestie van wetgeving, maar ook van vertrouwen en integriteit. Onvoldoende aandacht voor privacygevoeligheid en sociale/culturele normen zal nieuwe (verzekerings)diensten of producten frustreren, met aanzienlijke imagoschade tot gevolg. Het aantoonbaar maken van waarborgen en bieden van transparantie zijn dus noodzakelijk. Dit is een kans om het vertrouwen in nieuwe toepassingen voor gegevensgebruik te vergroten, of een enorm afbreukrisico als het wordt nagelaten.

Er is een spanningsveld tussen gegevensgebruik en gegevensbescherming. De dilemma’s op het gebied van solidariteit, nudging en eigenaarschap, zullen in de toekomst alleen maar ingewikkelder worden. Om deze dilemma’s het hoofd te kunnen bieden, moeten verzekeraars goed samenwerken met de overheid, toezichthouder en, niet in de laatste plaats, de klant.

Transparantie, goede privacywaarborgen en aansluiten bij de beleving van de klant zijn cruciaal om succesvolle verzekeringsinitiatieven te kunnen ontwikkelen.

Nieuw te ontwikkelen beleid moet gericht zijn op deze aspecten. Om aan te kunnen sluiten bij de wensen uit de samenleving is een dialoog noodzakelijk. Daarbij moeten de volgende uitgangspunten worden gehanteerd:

1. Verzekeraars hebben persoonlijke gegevens nodig om hun kerntaak te kunnen uitvoeren en dienen daarom de beschikking over deze gegevens te hebben.

2. Verzekeraars moeten integer met de gegevens van de klant omgaan en er geen misbruik van maken.

3. Verzekeraars moeten kraakhelder zijn richting klanten wat er met de door hen verstrekte gegevens wel en niet wordt gedaan. Klanten moeten kunnen begrijpen wat een verzekeraar met hun gegevens doet

4. Verzekeraars moeten zich bij het ontwikkelen van nieuwe toepassingen in gegevensgebruik niet alleen bewust zijn van de wettelijke kaders, maar zeker ook van de sociale en culturele opvattingen.

5. Verzekeraars dienen, door de exponentiele groei van (Big) data met een specifieke visie te komen op data en het gebruik daarvan. Hoe verhoudt profiling zich tot non-discriminatie? Wat zijn de randvoorwaarden, kansen en de mogelijkheden binnen wet- en regelgeving? Welke waarborgen en bedrijfsmatige maatregelen zijn noodzakelijk? Welke beleidsvrijheid biedt dat?

6. De overheid heeft als wetgever de taak om de kaders te bieden waarbinnen gegevens mogen worden gebruikt. De overheid moet wetgeving zo opstellen, dat deze duidelijkheid biedt, maar ook voldoende flexibel is om nieuwe ontwikkelingen en innovatie mogelijk te maken.

7. De overheid moet het gelijke speelveld tussen marktpartijen dusdanig bewaken, zodat de Nederlandse maatschappij als geheel de economische en sociale ‘vruchten’ van technologische mogelijkheden plukt.

8. Verzekeraars, en andere partijen, hebben behoefte aan vroegtijdig advies en overleg. Dit om een goede vertaalslag van de wettelijke uitgangspunten naar de praktijk te kunnen maken. Het College Bescherming Persoonsgegevens en de overheid zouden gesprekspartners moeten zijn voor vroegtijdig advies en overleg.

9. De klant moet privacybewuster worden. Dat bewustzijn moet groeien, net als het verantwoord omgaan met sociale media en andere digitale toepassingen.

10. Verzekeraars, overheid, toezichthouder en klanten dienen te waken voor behoud van de informatiegelijkheid om te voorkomen dat bij informatieongelijkheid de solidariteit in het verzekeringssysteem onder druk komt te staan. Branchevreemde partijen die verzekeringsproducten ontwikkelen, moeten aan dezelfde regulering als verzekeraars voldoen.