ZENN

ADVOCATUUR 3.0

mr. Koen Konings

COMPLIANCE: PRIVACY & DATALEKKEN

1. INLEIDING PRIVACYRECHT

U heeft een workshop bijgewoond van ZENN Advocatuur over compliance aan de privacyregels. De relatief nieuwe wettelijke meldplicht van datalekken kwam hierbij ook aan de orde. Eén van de specialismen van ZENN is 'compliance'. Deze term betekent het laten voldoen van bedrijven en organisaties aan de wettelijke eisen omtrent privacy en informatiebeveiliging. Met name de informationele privacy, daar waar persoonsgegevens worden verwerkt, speelt vaak een belangrijke maar beperkende rol bij bedrijfsprocessen zoals deze op wereldwijde schaal voorkomen bij de meeste ondernemingen.

Privacy is ieders grondrecht om hun privéleven van derden af te schermen. In de moderne informatiemaatschappij zijn vooral de (digitale) persoonsgegevens onderwerp van discussie. Steeds moet het individuele privacyrecht worden afgewogen tegen (commerciële) belangen van dienstverleners, websitebeheerders en andere verwerkers van persoonsgegevens. Het uitgangspunt is dat iedereen een zekere mate van controle moet houden over zijn eigen persoonsgegevens. Medische persoonsgegevens worden daarbij als extra gevoelig beschouwd, zodat marktpartijen in de eHealth-sector grotere aansprakelijkheidsrisico's lopen.

Sinds de Tweede Wereldoorlog is de discussie over grondrechten in Europa goed op gang gekomen, waarbij ook het privacyrecht tot ontwikkeling is gekomen. Diverse Europese richtlijnen hebben het privacyrecht op de maatschappelijke en technische ontwikkelingen aangepast. Het Nederlandse uitvloeisel van Europese privacyrichtlijnen is de Wet bescherming persoonsgegevens (Wbp) met als toezichthouder de Autoriteit Persoonsgegevens (AP, voorheen het College bescherming persoonsgegevens of CBP). Ook zijn er privacyregels terug te vinden in onze Telecommunicatiewet (Tw), waaronder regels over spam en cookies.

Omdat vrijwel iedere onderneming persoonsgegevens verwerkt, is het privacyrecht zeer belangrijk. Het lastige is dat de regels vaak complex zijn, terwijl voor het niet correct verwerken van persoonsgegevens hoge boetes kunnen worden opgelegd. Bij het aanbieden van diensten, al dan niet in de cloud of via derden, moeten de verplichtingen en verantwoordelijkheden voor een correcte verwerking van persoonsgegevens contractueel en technisch goed worden vastgelegd. Denkt u hierbij niet alleen aan een bewerkersovereenkomst, maar ook bijvoorbeeld aan sluitende afspraken om de informatiebeveiliging te laten voldoen aan ISO-norm 27001:2013 of aan NEN 7510 voor medische gegevens. Vaak zal al in het functioneel ontwerp van een proces of software de wijze van verwerking van persoonsgegevens in lijn met de regels moeten worden gemaakt ('privacy by design'). Hoe er met persoonsgegevens moet worden omgegaan is zeer afhankelijk van de sector en van welke gegevens worden verwerkt.

Sinds 2016 is de strengere wettelijke plicht voor het melden van datalekken een feit. Hiermee liep Nederland vooruit op de aanstaande Algemene Verordening Gegevensbescherming (AVG, ook wel General Data Protection Regulation of GDRP). Deze nieuwe set regels, die de huidige Wet bescherming persoonsgegevens (Wbp) gaat vervangen, zorgt voor een nadere aanscherping van de regels waar marktpartijen zich op moeten voorbereiden. De deadline voor een correcte implementatie is 25 mei 2018, wanneer de AVG gaat gelden.

2. KERNBEGRIPPEN

In het privacyrecht zijn drie kernbegrippen van groot belang. Deze betreffen de begrippen "verantwoordelijke", "bewerker" en "betrokkene", en zijn afkomstig uit de Wet bescherming persoonsgegevens.

Het begrip *betrokkene* valt het gemakkelijkst te begrijpen; de betrokkene is degene wiens of wier gegevens het betreft. Het zijn dus de persoonsgegevens van de betrokkene die verwerkt worden.

De *verantwoordelijke* is volgens de wet degene die het doel en de middelen van de verwerking vaststelt. Vrijwel iedereen die rechtstreeks van de betrokkene afkomstige gegevens verwerkt, valt onder deze definitie. Een webshophouder bijvoorbeeld, die van de koper persoonsgegevens heeft ontvangen om vast te stellen waar het gekochte goed naar toe gestuurd moet worden, is verantwoordelijke.

Een *bewerker* is iemand die ten behoeve van of namens de verantwoordelijke gegevens verwerkt. Dit kan iemand zijn aan wie de verantwoordelijke de verwerking van persoonsgegevens heeft uitbesteed, maar dat hoeft niet noodzakelijkerwijs het geval te zijn. In bovengenoemd voorbeeld van de webshophouder, zou de provider die de webshop host voldoen aan de definitie van bewerker. In beginsel blijft de verantwoordelijke echter verantwoordelijk – de term zegt het al – voor het rechtmatig verwerken van de betreffende persoonsgegevens. Onder omstandigheden heeft de bewerker ook een eigen, zelfstandige verplichting om zorgvuldig met verkregen persoonsgegevens om te gaan.

3. MELDPLICHT DATALEKKEN

Wet Meldplicht Datalekken

Sinds 1 januari 2016 is de meldplicht datalekken uitgebreid in de vorm van artikel 34c Wbp. Dit houdt in dat organisaties die persoonsgegevens verwerken een melding moeten doen bij de AP zodra zich een

ernstig datalek voordoet. Bovendien zullen organisaties een melding moeten doen aan de betrokkenen indien het datalek waarschijnlijk ongunstige gevolgen zal hebben voor hen.

Wanneer is nu sprake van een datalek dat gemeld moet worden? Er is sprake van een datalek op het moment van een inbreuk op de beveiliging waardoor persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking. Het begrip datalek is dus ruimer dan alleen het vrijkomen (lekken) van persoonsgegevens, maar omvat ook vernietiging en andere vormen van onrechtmatige verwerking van persoonsgegevens. Voorbeelden van datalekken zijn een zoekgeraakte laptop met persoonsgegevens, een gestolen smartphone, een hack in een online systeem waarbij een databestand is buitgemaakt of een malwarebesmetting.

Het melden van een datalek aan de AP is verplicht wanneer dit *"leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens"* (artikel 34c lid 1 Wbp). De meldplicht geldt dus niet wanneer de gevolgen daarvan gering zijn of wanneer er slechts sprake was van de ontdekking van een kwetsbaarheid in het systeem. Het is echter verstandig om voor de zekerheid bij twijfel het datalek te melden. Een dergelijke melding kan later eventueel nog worden ingetrokken.

In sommige gevallen moet het datalek ook worden gemeld aan de betrokkene(n), dus aan degene op wie de persoonsgegevens betrekking hebben. Zij moeten op de hoogte worden gebracht als een datalek *"waarschijnlijk ongunstige gevolgen zal hebben"* voor hun persoonlijke levenssfeer (artikel 34c lid 2 Wbp).

Via een webformulier (of fax) zal de melding aan de AP moeten worden gedaan. Of en hoe er aan betrokkenen moet worden gemeld wordt ook door de richtsnoeren behandeld. Uiteraard zijn er vaak ook extra handelingen nodig, zoals een reset van wachtwoorden. Na een gedane melding zal de AP de omvang van de melding in kaart brengen. Eventueel geeft zij uw organisatie de instructie om de betrokkene(n) te informeren. Een melding kan ook aanleiding geven tot een nader onderzoek naar de algemene naleving van de privacywetgeving. Schending daarvan kan evenals het verzwijgen van een datalek tot boetes leiden of tot reputatieschade door publicatie van rapporten van de AP.

Het niet melden van een datalek kan u duur komen te staan. De AP kan boetes opleggen tot maximaal € 820.000,- en vanaf 25 mei 2018 maximaal 2% van de totale wereldwijde jaaromzet. Het is daarom belangrijk om datalekken te melden zo gauw deze zich voordoen. Aan de andere kant zal de AP dergelijke hoge boetes vooral opleggen aan grove inbreuken op de privacy en niet direct aan beperkte datalekken waarop kordaat is gereageerd. Het begint echter met een onderzoek.

Richtsnoeren en bewerkersovereenkomst

De AP heeft richtlijnen opgesteld die bedoeld zijn om organisaties te helpen bij het bepalen of sprake is van een datalek en of zij dat moeten melden aan de AP en aan de betrokkene(n). De richtsnoeren behandelen op eenvoudige wijze aan de hand van stroomschema's en voorbeelden vragen als: Wanneer is de Wet bescherming persoonsgegevens (Wbp) van toepassing op de verwerking? Wat moet uw organisatie regelen als zij persoonsgegevens laat verwerken door een bewerker? Wat is een datalek? Aan wie moet ik een datalek melden? Enzovoort.

Een van de belangrijkste tips uit de beleidsregels zijn de aandachtspunten van zaken die *verantwoordelijken* (diegenen die over de persoonsgegevens gaan) een aantal zaken met *bewerkers* (diegenen die voor verantwoordelijken de gegevens verwerken, zoals IT-leveranciers) dienen te regelen:

- Gaat de bewerker u daadwerkelijk informeren over alle relevante incidenten?
- Gaat de bewerker eventueel zelf meldingen doen aan de AP?
- Ontvangt u per incident alle informatie die u nodig heeft?
- Hoe gaat de bewerker u informeren over de incidenten?
- Wordt u tijdig geïnformeerd over de incidenten?
- Wordt u op de hoogte gehouden van eventuele nieuwe ontwikkelingen rond het incident, en van de maatregelen die de bewerker treft om aan zijn kant de gevolgen van het incident te beperken en herhaling te voorkomen?
- Kunt u vaststellen dat u daadwerkelijk op de hoogte wordt gesteld van alle relevante incidenten, en dat de verstrekte informatie klopt?

Dit kan met een zogenaamde bewerkersovereenkomst, die voor elke verantwoordelijke bovendien ook wettelijk verplicht is om te sluiten met haar bewerkers op grond van artikel 14 Wbp. Ook dit artikel is uitgebreid naar aanleiding van de strengere meldplicht.

Het opstellen van dergelijke bewerkersovereenkomsten is een specialisme van ZENN. Een dergelijke overeenkomst is maatwerk en kan ofwel meer in het voordeel van de verantwoordelijke (afnemer van IT) worden geschreven, of juist meer in het voordeel van de bewerker (leverancier van IT). Bovendien zal nu ook rekening gehouden moeten worden met de komende regels van de AVG, die nieuwe eisen stelt aan een dergelijke overeenkomst.

Wat gaat u doen?

Het kan verstandig zijn om uw organisatie eens goed onder de loep te nemen en te beoordelen of uw organisatie aan de privacyregelgeving voldoet (*compliance*), bijvoorbeeld door het uitvoeren van een

zogeheten *Privacy Impact Assessment (PIA)* of het laten beoordelen van de *bewerkersovereenkomst*. Ook dient de komende AVG in de gaten te worden gehouden, aangezien deze regels introduceert die nog iets strenger zullen zijn dan die van het huidige regime.

U kunt zelf grofweg de volgende stappen ondernemen om uw organisatie gereed te maken:

Stap 1:

Begin met het belangrijkste proces of systeem dat persoonsgegevens verwerkt.

Stap 2:

Bepaal de belangrijkste mogelijke oorzaken van datalekken (bijv. hacking, verliezen van laptops of smartphones, lek bij leverancier of bewerker, gebrekkige autorisaties of het testen met klantgegevens).

Stap 3:

Neem stappen om die risico's te verkleinen.

Stap 4:

Coördineer oftewel maak datalekteam en een draaiboek met bevoegdheden en wie wat doet.

Stap 5:

Oefen! Doe een conceptmelding, maak een conceptbericht aan betrokkene en bepaal wie nog meer geïnformeerd dient te worden.

Stap 6:

Formuleer een herstelaanpak, gericht op enerzijds de betrokkenen (nazorg, bijv. wachtwoordreset) en anderzijds gericht op de eigen organisatie (beveiliging, continuïteit dienst, reputatieherstel, aansprakelijkheid).

Stap 7:

Bepaal de registratie: incidentenlogging, afhandeling en eventuele financiële zaken, zoals wellicht een speciale verzekering voor schade door datalekken.

Stap 8:

Nadat de kernprocessen en –risico's zijn geregeld, breid de aanpak uit met andere processen en andere scenario's/risico's.

Stap 9:

Test de aanpak, zowel de protocollen op papier als in de praktijk.

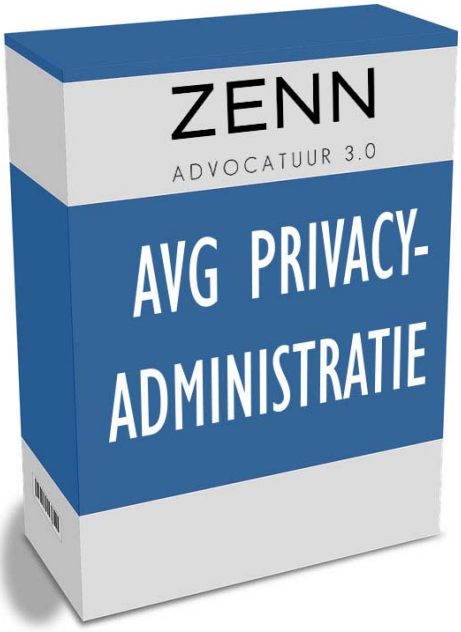
Uiteraard is ZENN u graag van dienst bij vraagstukken rondom de thema's compliance, privacy, datalekken, bescherming van persoonsgegevens en informatiebeveiliging.

4. VOORBEREIDING OP DE AVG

Hoewel er voor de betrokkenen, van wie persoonsgegevens worden verwerkt, hier en daar wat extra waarborgen en rechten zijn geformuleerd, zijn de meeste wijzigingen voelbaar aan de kant van diegenen die persoonsgegevens verwerken. Voor deze verwerkers van persoonsgegevens verandert behoorlijk veel, hoewel de uitgangspunten van het huidige privacykader (in de Wbp) worden voortgezet.

In de basis wordt door de AVG een grotere mate van *accountability* vereist en zijn de regels meer gericht op de risico's van gegevensverwerkingen. Op ieder moment moet de verantwoordelijke over de gegevensverwerking kunnen *aantonen* dat passende maatregelen zijn genomen, dat van tevoren goed is nagedacht over hoe de verwerkingen plaatsvinden en dat er regelmatig controles (audits) worden uitgevoerd. Dit moet allemaal zijn weerslag krijgen in een nieuw op te tuigen *privacy-administratie*.

Niets doen is geen optie, want de boetes zijn niet mals. Organisaties moeten worden voorbereid op de werking van de AVG. De boetes die geriskeerd worden zijn enorm. Een goede voorbereiding begint bij het lezen van de blogs van ZENN over de AVG, waarin per onderwerp wordt stilgestaan bij wat dit betekent voor uw organisatie. Uiteraard dient ZENN u graag van advies over dit onderwerp, bijvoorbeeld voor het inrichten van de vereiste *privacy-administratie* of het toetsen van uw diensten aan *privacy compliance*.



OVER ZENN

Een informatiemaatschappij vereist een advocatenkantoor gericht op informatierecht. Dat is ZENN. Een veranderende economie en nieuwe wijzen van zaken doen vereisen bovendien een nieuwe vorm van advocatuur. Dat is Advocatuur 3.0. ZENN biedt specialistische kennis en grote mate van betrokkenheid tegen reële uurtarieven of vaste prijzen. Hierbij wordt de balans tussen uw belang en de kosten steeds bewaakt. Het staat ook symbool voor de ambitie van de advocaat om een werkwijze te hanteren die transparanter, moderner en proactiever is dan de huidige standaard van één van de oudste beroepsgroepen. Duurzaamheid, vooral van de relatie met de klanten, is steeds het uitgangspunt. Zie zenn.law voor meer informatie.

Disclaimer

Hoewel de inhoud van deze handreiking met de grootste zorgvuldigheid is samengesteld, aanvaardt ZENN Advocatuur geen aansprakelijkheid voor schade die voortvloeit uit het gebruik hiervan en eventuele onvolledigheden in dit overzicht. De geboden informatie kan niet worden beschouwd als vervanging van een specifiek op uw praktijk toegesneden juridisch advies, maar is slechts een vrijblijvende bron van algemene juridische informatie.

Copyright

© 2017 ZENN Advocatuur. Alle rechten worden voorbehouden. Niets uit of van dit artikel mag zonder de uitdrukkelijke toestemming van de auteurs worden openbaar gemaakt of verveelvoudigd.

Contact

ZENN Advocatuur

050-2110066

konings@zenn.law

https://zenn.law

@ZENNlaw

LinkedIn