Mr. F.B.M. Olijslager

Branchewaarschuwingssystemen

Het aanleggen van een waarschuwingssysteem (in de volksmond "zwarte lijsten") door bedrijven is volgens de Autoriteit Persoonsgegevens pas te rechtvaardigen wanneer de schade een dusdanige omvang heeft bereikt dat een beperking op het recht van de persoonlijke levenssfeer van personen die zijn opgenomen in het systeem noodzakelijk is. Steeds meer brancheorganisaties beschikken over een signaleringssysteem om hun leden te waarschuwen voor potentiële fraudeurs en malafide werknemers. Een branchewaarschuwingslijst mag echter niet zomaar worden aangelegd. Zo moeten personen die op een lijst staan daarvan op de hoogte worden gebracht.

'Een vos verliest wel zijn haren, maar niet zijn streken.' Dit spreekwoord is de basis voor de wens van veel bedrijven om zich te wapenen tegen een groep van personen dat zonder schroom misbruik maakt van het vertrouwen dat anderen in hen stelt. Met een waarschuwingslijst kan worden voorkomen dat iemand de belangen, integriteit of veiligheid van (cliënten of medewerkers van) een bedrijf of instelling (opnieuw) schaadt. De Autoriteit Persoonsgegevens - de privacytoezichthouder in Nederland - is van mening dat bedrijven en bedrijfstakken een gerechtvaardigd belang kunnen hebben bij de aanleg en het gebruik van signaleringssystemen om potentiële oplichters en andere fraudeurs tijdig te herkennen. Zo'n signaleringssysteem van malafide klanten of ex-werknemers wordt ook wel waarschuwingslijst of – wat meer populair - zwarte lijst genoemd. De Autoriteit Persoonsgegevens vindt dat het een gevoelig instrument is, dat alleen mag worden ingericht en gebruikt indien de hoogste mate van zorgvuldigheid wordt betracht. Het aanleggen van een waarschuwingssysteem is volgens de Autoriteit Persoonsgegevens pas te rechtvaardigen wanneer de schade een zodanige omvang heeft bereikt dat een beperking op het recht van de persoonlijke levenssfeer van personen die zijn opgenomen in het systeem noodzakelijk is. Het gerechtvaardigd belang van een waarschuwingslijst is mede afhankelijk van de gevolgen van de plaatsing op de lijst voor de betrokkene. Bij de beoordeling daarvan is de vraag relevant in welke mate betrokkenen, door plaatsing op de waarschuwingslijst, worden afgesneden van bepaalde voorzieningen, zoals de toegang tot een deel van de arbeidsmarkt. Personen die op de waarschuwingslijst worden vermeld moeten daarvan (in beginsel) op de hoogte worden gebracht. Op deze manier kan de geregistreerde zijn rechten uitoefenen zoals correctie, verwijdering of afscherming van gegevens.

Strafrechtelijke persoonsgegevens

Bij de totstandkoming van de Wet Bescherming Persoonsgegevens (de voorloper van de Algemene Verordening Gegevensbescherming – afgekort: AVG) was de regering van mening de verwerking van "strafrechtelijke persoonsgegevens" niet alleen kon worden voorbehouden aan overheidsorganen, zoals de politie en het Openbaar Ministerie. Ook private (rechts)personen hebben op dat punt een gerechtvaardigde informatiebehoefte, zeker nu verstrekking van gegevens uit de politie- of justitieregisters aan derden voor buiten strafrecht gelegen doelen zo goed als uitgesloten is.

De AVG verbiedt het verwerken van "strafrechtelijke gegevens" door bedrijven en instellingen, tenzij de nationale wetgever een voorziening heeft getroffen dat dit wel mogelijk maakt. In Nederland is het verwerken van strafrechtelijke gegevens (lees: het

uitwisselen van informatie tussen bedrijven of instellingen) door middel van een branchewaarschuwingssysteem geoorloofd als de Autoriteit Persoonsgegevens hiervoor aan de deelnemers aan het waarschuwingssysteem een vergunning heeft verleend. De bepalingen hierover zijn opgenomen in de Uitvoeringswet AVG (zie art. 33 lid 4 onder c van de UAVG).
Het begrip «strafrechtelijke persoonsgegevens» heeft betrekking zowel op veroordelingen als op min of meer gegronde verdenkingen dat iemand een strafbaar feit heeft begaan. Een veroordeling is een vaststelling door de strafrechter dat iemand een strafbaar feit heeft gepleegd (een schuldigverklaring). Bij "min of meer gegronde" verdenkingen gaat het om concrete aanwijzingen dat iemand een strafbaar feit heeft gepleegd.

Als maatstaf voor het mogen verwerken van strafrechtelijke gegevens in een waarschuwingssysteem heeft de Hoge Raad bepaald dat de vastgestelde gedraging(en) een zwaardere verdenking moeten opleveren dan een "redelijk vermoeden van schuld, in die zin dat de te verwerken strafrechtelijke gegevens in voldoende mate moeten vaststaan. Verder heeft de Hoge Raad heeft als voorwaarde voor het uitwisselen van "strafrechtelijke gegevens" door bedrijven en instellingen bepaald dat sprake moet zijn van "zodanige concrete feiten en omstandigheden dat zij een als strafbaar feit te kwalificeren bewezenverklaring – in de zin van artikel 350 WvSv – moet kunnen dragen". Een veroordeling door de strafrechter is echter niet vereist om iemand te kunnen plaatsen op een waarschuwingslijst. Voor het begrip strafrechtelijk persoonsgegeven maakt het niet uit of een bedrijf of instelling wel of niet aangifte heeft gedaan bij een opsporingsambtenaar. Een werknemer die bijvoorbeeld op staande voet ontslagen is wegens het onrechtmatig toe-eigenen van geld heeft een strafbaar feit gepleegd en dat is bepalend. Het gaat er om dat "door de feiten heen kijkend" een strafbaar feit geconstrueerd kan worden en dat in voldoende mate vaststaat dat betrokkene zich aan dat strafbare feit heeft schuldig gemaakt.

Wettelijke basis
De basis voor waarschuwingssystemen ligt in art. 31 van de Uitvoeringswet AVG. Voor de verwerking van strafrechtelijke gegevens wordt onderscheid gemaakt tussen verwerking "ten eigen behoeve" en verwerking "voor derden". In het belang van de onderneming of (overheids)instelling mogen "ten eigen behoeve" strafrechtelijke gegevens van personeelsleden worden verwerkt, alsmede van derden wanneer deze personen ten nadele van de onderneming onrechtmatige handelingen hebben gepleegd. Een goed strafrechtelijk geheugen is voor ondernemingen of (overheids)instelling van belang voor in de toekomst te nemen beslissingen over het al dan niet aangaan of het al dan niet onder voorwaarden aangaan van een zakelijke relatie met personen die eerder het vertrouwen van het bedrijf of instelling geschonden hebben. Voor het binnen de eigen onderneming of instelling vastleggen en verder gebruiken van strafrechtelijke gegevens gelden naast de algemene bepalingen in de AVG over het verwerken van gegevens geen specifieke eisen. De Autoriteit Persoonsgegevens hoeft voorafgaand aan de verwerking "ten eigen behoeve" geen toestemming te geven.

Concernbreed
Dat geldt eveneens voor de verwerking van strafrechtelijke gegevens binnen een concern, groep of economische eenheid als bedoeld in de artikel 2:24b van het Burgerlijk Wetboek. Gegevens die afkomstig zijn van het ene bedrijfsonderdeel zijn doorgaans ook relevant voor een ander bedrijfsonderdeel voor de beoordeling van de vraag of een contract met de betrokkene zal worden aangegaan. Het komt in de praktijk maar al te vaak voor dat

medewerkers of uitzendkrachten ontslagen worden bij de ene werkmaatschappij wegens misdrijven of ander laakbaar gedrag en vervolgens bij de andere groepsmaatschappij probleemloos aangenomen worden. De Uitvoeringswet AVG (art. 31 lid 1 onder c) staat toe dat binnen concernverband strafrechtelijke gegevens worden vastgelegd door een onderdeel van een concern met het oog op haar dienstverlening aan de werkmaatschappijen van dat concern. Voor een concernbrede waarschuwingslijst is geen voorafgaande vergunning van de Autoriteit Persoonsgegevens vereist. Indien de waarschuwingslijst wordt uitgebreid naar andere onderdelen van het concern, behoeft dat echter wel nadere motivatie. Het systeem van de waarschuwingslijst krijgt door de concernbrede basis immers een zodanige omvang dat de gevolgen voor de betrokkenen aanzienlijk verstrekkender zijn. Vanwege de grotere gevolgen voor de geregistreerden, dient het belang bij een dergelijke lijst ook zwaarwegend te zijn. De waarborgen van de geregistreerden moeten in overeenstemming zijn met de grotere gevolgen door plaatsing op een concernbrede lijst. Een waarborg kan zijn dat strafrechtelijke gegevens uitsluitend worden vastgelegd door een centrale veiligheidsafdeling. In de praktijk gebeurt dat doordat de veiligheidsafdeling een onderzoeksadministratie aanlegt en vervolgens een technische voorziening treft (intern verwijzingsregister) opdat gegevens ook daadwerkelijk beschikbaar zijn voor de werkmaatschappijen van het concern. Zo kunnen gegevens van wegens onregelmatigheden ontslagen personeel in een intern waarschuwingssysteem worden vastgelegd. Als concernregel is dan voor recruiters voorgeschreven dat zij het intern verwijzingsregister moeten raadplegen voordat een nieuwe medewerker of uitzendkracht aanstellen.

Branchewaarschuwingssysteem

Zodra strafrechtelijke gegevens buiten het eigen bedrijf of buiten concernverband worden verspreid, moet de Autoriteit Persoonsgegevens hiervoor per deelnemer een vergunning afgeven. Bij plaatsing op een branchebrede waarschuwingslijst dient de ernst van de misstand (de gedraging is vanuit branche-optiek onacceptabel) groter te zijn dan bij plaatsing op een bedrijfs- of concernbrede waarschuwingslijst. Dat betekent dat de criteria voor plaatsing op de lijst (opnamecriteria) zwaarder zijn. Op dit moment zijn verschillende branches die waarschuwingssystemen gebruiken die de goedkeuring van de Autoriteit Persoonsgegevens hebben. Genoemd worden de financiële sector en de detailhandel. Aan deze waarschuwingssystemen ligt een protocol van de brancheverenigingen) ten grondslag. In het protocol wordt gemotiveerd waarom dit zware middel gerechtvaardigd is in relatie tot het privacybelang van degenen wiens persoonsgegevens worden geregistreerd. Verder worden in het protocol bepalingen opgenomen over de vereisten om te kunnen deelnemen, de rechten en plichten van de deelnemers aan het systeem, de opnamecriteria, het toetsingsproces en de toegang tot de basisgegevens, geheimhouding, de bewaarduur van gegevens, de rechten van de geregistreerde en een geschillenregeling.

Incidentenregister

Hoe ziet zo'n branchewaarschuwingssysteem er uit. Bij wijze van voorbeeld wordt de situatie geschetst bij banken die dit systeem zowel bij cliëntacceptatie als bij indienstneming van personeel gebruiken. Iedere aan het waarschuwingssysteem deelnemende bank heeft een incidentenregister. Het incidentenregister is de naam van de onderzoeksadministratie Onder verantwoordelijkheid van de deelnemer treedt de veiligheidsafdeling op als beheerder van het incidentenregister. Van het incident worden verschillende gegevens vastgelegd, zoals:

- de kenmerken van de bedreiging, zoals modus operandus;

- de onderzoeksmethoden- en middelen die gebruikt zijn en de afwegingen die tot dat gebruik hebben geleid (proportionaliteit en subsidiariteit);
- de personen die bij het incident betrokken zijn. Daarbij kan gedacht worden aan lieden die misbruik hebben gemaakt van het stelsel van de dienstverlening (externe fraudeurs), maar ook aan personeelsleden die gedragscodes overtreden;
- de op het incident betrekking hebbende gegevensdragers, zoals foto's, camerabeelden en geluidsopnamen
- de maatregelen die naar aanleiding van het incident zijn genomen (zoals beëindiging van de arbeidsovereenkomst of het verhalen van de schade)

Hit-no hit

Het systeem werkt op basis van 'hit-no hit'. De toetser ziet niet waarom iemand in het systeem is opgenomen. In geval van een 'hit' dient de bevrager ten allen tijde de eigen veiligheidsafdeling te raadplegen. Door een ingebouwde signaleringsfunctie is het de veiligheidsafdeling al bekend dat iemand getoetst heeft met een hit als gevolg. Dit is gedaan om te voorkomen dat het systeem wordt bevraagd en dat een product wordt geweigerd, zonder dat bij een hit naar de achterliggende gegevens wordt gevraagd. Dan verwordt het systeem tot een zwarte lijst, hetgeen nadrukkelijk niet de bedoeling is. Als de veiligheidsafdeling wordt benaderd, verschaft zij de achterliggende gegevens als zij zelf verantwoordelijk was voor opname van de geregistreerde in het systeem en voor zover de gegevens relevant zijn voor de toetser. Wanneer de eigen veiligheidsafdeling niet verantwoordelijk was voor de signalering maar een veiligheidsafdeling van een andere deelnemer, raadpleegt de veiligheidsafdeling van de toetser de veiligheidsafdeling van de (primaire) bron. Dat is dus een andere deelnemer aan het waarschuwingssysteem. Vervolgens vindt er door de veiligheidsafdeling van de toetsende instantie een afweging plaats of wel of geen contract met de sollicitant dient te worden aangegaan.

Stappen

Welke stappen dient een brancheverenigingte nemen als zij geïnteresseerd is om het voorbeeld van de banken, detailhandel of de horeca te volgen? Allereerst dient te worden bepaald of er behoefte is aan een dergelijk signaleringsysteem binnen de branche. In de praktijk ontstaat deze behoefte veelal 'bottom-up'. Tijdens de reguliere werkoverleggen tussen vertegenwoordigers van een branche is het van gedachten uitwisselen over opzettelijke benadelingen door eigen personeel of door derden een regelmatig terugkerend onderwerp. Vaak is praktijk dat gegevens van fraudeurs informeel al tussen de bedrijfsbeveiligingsdiensten worden uitgewisseld, al dan niet via elektronisch berichtenverkeer.

Als deze manier van informele berichtenuitwisseling door de omvang van de fraude niet meer beheersbaar is, komt de tweede stap in beeld. Dat is overleg met de brancheverenigingom vast te stellen of een branchewaarschuwingssysteem oplossing kan bieden voor de als dringend ervaren behoefte van gegevensuitwisseling.

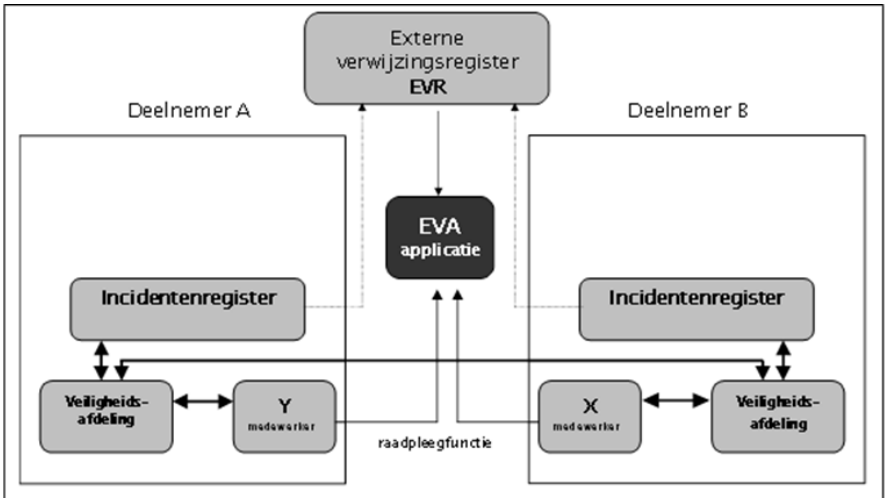
De derde stap bestaat uit het contracteren van een terzake deskundige privacyjurist die de wens van de branche verwoord in een concept-protocol. Deze stap bespaart tijdwinst en teleurstellingen. De Autoriteit Persoonsgegevens gaat alleen akkoord met een waarschuwingssysteem indien een goed protocol aan de basis ligt. De privacyjurist is in staat om te beoordelen wie als 'verwerkingsverantwoordelijke' voor het systeem moet

worden aangemerkt en welke waarborgen geboden zijn opdat de belangen van de branche en de geregistreerde met elkaar in evenwicht zijn.

De vierde stap bestaat uit het aanvragen van een eerste oriënterend gesprek met de Autoriteit Persoonsgegevens. In dit gesprek dient duidelijk te worden gemaakt wat het gerechtvaardigd belang is van een branchewaarschuwingssysteem en dient te worden gepolst of een dergelijk systeem van gegevensuitwisseling kans van slagen heeft. Vaak leidt zo'n overleg tot vervolgafspraken en meerdere hernieuwde overleggen met de Autoriteit Persoonsgegevens.

Als vijfde stap moet worden nagedacht over de wijze van berichtenuitwisseling. De techniek is een uiterst bepalende factor bij het uiteindelijke succes van een waarschuwingssysteem. Er zijn op dit moment een paar aanbieders die ervaring hebben met branchewaarschuwingssystemen en die in staat zijn om een op maat gemaakt product te leveren.
De zesde stap bestaat uit het doorlopen van de formaliteiten. De Autoriteit Persoonsgegevens heeft aangegeven dat zij in het kader van de vergunningaanvraag wenst te beschikken over de uitgevoerde Data Privacy Impact Assessment (hierna afgekort tot: DPIA).
Een DPIA (artikel 35 AVG) is een proces dat bedoeld is om de verwerking van persoonsgegevens te beschrijven die waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, de noodzaak en evenredigheid ervan te beoordelen en de daaraan verbonden risico's voor de rechten en vrijheden van natuurlijke personen in te schatten en maatregelen te nemen om de risico's te beheersen. Onder "de rechten en vrijheden van natuurlijke personen" wordt onder andere verstaan het recht op gegevensbescherming en bescherming van de persoonlijke levenssfeer.

Al naar gelang wie als 'verwerkingsverantwoordelijke' in de zin van de AVG wordt aangemerkt zullen de deelnemers aan het waarschuwingssysteem op een bepaald moment een vergunning moeten aanvragen bij de Autoriteit Persoonsgegevens. Als het vooroverleg vruchtbaar is geweest kan binnen redelijke tijd een vergunning door de Autoriteit Persoonsgegevens worden afgegeven en kan de branche daadwerkelijk aan de slag. Zolang deze vergunning uitblijft mogen geen strafrechtelijke persoonsgegevens worden uitgewisseld. Een branche dient zeker rekening te houden met een doorlooptijd van twee jaar vanaf het moment dat de eerste stap wordt gezet tot en met de vergunning van de Autoriteit Persoonsgegevens.



Het PIFI
PIFI is de afkorting voor Protocol Incidentenwaarschuwingssysteem financiële instellingen. Het PIFI bestaat uit een stelsel van afspraken over de uitwisseling van persoonsgegevens binnen de financiële sector, tussen expliciet in het PIFI aangewezen partijen. Het PIFI is geschreven tegen de achtergrond dat financiële instellingen samen wensen te werken op het gebied van het beheersen van fraude, veiligheid en integriteit.

Er zijn verschillende partijen betrokken bij het PIFI. Dat zijn de vijf brancheverenigingen van de financiële sector (de Nederlandse Vereniging van Banken het Verbond van Verzekeraars, de Vereniging van financieringsondernemingen in Nederland, Zorgverzekeraars Nederland en de Stichting Fraudebestrijding Hypotheken. Zij onderhouden het PIFI, coördineren de toelating van deelnemers aan de gegevensuitwisseling en monitoren de naleving van het PIFI voor zover zij de financiële instelling hebben toegelaten tot het PIFI .

Daarnaast kent het PIFI deelnemers. Dat zijn financiële instellingen, zoals een bank en/of (zorg)verzekeraar en/of hypothecaire instelling en/of financieringsonderneming.
De deelnemers zijn zelf verantwoordelijk voor de persoonsgegevens die zij verwerken en voor beslissingen over het uitwisselen van persoonsgegevens.
Het PIFI beschrijft twee soorten van gegevensuitwisseling:

1. Het uitwisselen van persoonsgegevens voor het onderzoeken en coördineren van incidenten (art. 4.2.1 t/m/ 4.2.7 PIFI).

Er worden al dan niet strafrechtelijke persoonsgegevens uitgewisseld met veiligheidszaken van (de organisatie van) een deelnemer of een derde-organisatie als bedoeld in het PIFI of met het fraudeloket van de brancheverenigingen, met als doel:
- het verzamelen van bewijs voor betrokkenheid van sector gerelateerde fraude en criminaliteit en/of
- het nagaan of sprake is van vergelijkbare incidenten door het fraudeloket, zodat zij de betrokken verzekeraars met elkaar in contact kan brengen.

2. Waarschuwingsfunctie door registratie van plegers van incidenten

Er worden persoonsgegevens vastgelegd van iemand die zich eerder schuldig heeft

gemaakt aan sector gerelateerde fraude en criminaliteit en de op deze persoon betrekking hebbende gegevens worden na een hit in het externe verwijzingsregister uitgewisseld met (de organisatie van) een deelnemer of een derde-organisatie als bedoeld in het PIFI of het fraudeloket. Daarmee wordt de toetser de gelegenheid geboden om na te gaan of deze persoon een risico vormt voor dienstverlening of indienstneming**.**

In het PIFI is een aantal waarborgen voor betrokkene(n) opgenomen. Zo worden betrokkenen via bijvoorbeeld via privacystatements en aanvraag- en sollicitatieformulieren geïnformeerd over het feit dat er onderzoek kan worden ingesteld indien inbreuk gemaakt wordt op veiligheid en integriteit.
Om de uniformiteit met betrekking tot de uitleg en de toepassing van het PIFI te waarborgen is per brancheverenigingen of voor meerdere brancheverenigingen samen een begeleidingscommissie ingesteld. Indien daarvoor aanleiding is adviseert de begeleidingscommissie de deelnemers aan het EVR over de toepassing van de onder artikel 5.2.1 PIFI genoemde vastleggingscriteria (art. 6.2 PIFI)**.**

Voor meer informatie en protocollen:

www.autoriteitpersoonsgegevens.nl: onderdeel thema's, themadossier 'zwarte lijsten'
www.nvb.nl : zoeken op 'incidentenwaarschuwingssysteem'
www.stichtingcis.nl : specifiek voor verzekeraars
www.stichtingfad.nl : Detailhandel