

Besluit inzake de verklaring omtrent de rechtmatigheid van de verwerking Waarschuwingsregister Particuliere Beveiliging van de Vereniging van Particuliere Beveiligingsorganisaties; z2010-00013.

1 Aanleiding voorafgaand onderzoek

Op 22 december 2009 heeft de Vereniging van Particuliere Beveiligingsorganisaties (hierna: VPB) – ingevolge artikel 27 van de Wet bescherming persoonsgegevens (Wbp) – melding gedaan bij het College bescherming persoonsgegevens (CBP) van een voorgenomen verwerking van persoonsgegevens. Deze melding is bij het CBP bekend onder meldingsnummer m1423079 onder de naam ‘Waarschuwingsregister Particuliere Beveiliging’.

Uit de verstrekte informatie blijkt dat de VPB voornemens is strafrechtelijke gegevens te verwerken, in de zin van artikel 22 Wbp. Het begrip ‘strafrechtelijke gegevens’ heeft betrekking op zowel de veroordeling als op min of meer gegronde verdenkingen van strafrechtelijk gedrag.

Naar aanleiding van de melding heeft het CBP een voorafgaand onderzoek, zoals bedoeld in artikel 31 Wbp, ingesteld. Ingevolge artikel 31, eerste lid, onder c, Wbp is een voorafgaand onderzoek vereist indien de verantwoordelijke, anders dan krachtens een vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus (Wpbr), voornemens is strafrechtelijke gegevens of gegevens over onrechtmatig of hinderlijk gedrag te verwerken ten behoeve van derden. De door de VPB voorgenomen verwerking valt buiten de werkzaamheden waarvoor een dergelijke vergunning wordt verleend.

In het voorbereidende deel van het voorafgaand onderzoek vormt het CBP zich een algemeen beeld van de rechtmatigheid van de door de VPB beschreven en voorgenomen gegevensverwerking tegen de achtergrond van de algemene waarborgen uit Wbp. In een nader onderzoek worden met name de risicovolle aspecten van de voorgenomen verwerking beoordeeld. Het voorafgaand onderzoek leidt tot een verklaring omtrent de rechtmatigheid, als bedoeld in artikel 32 Wbp.

2 Procedureverloop

Op 1 februari 2010 heeft het CBP aan de VPB medegedeeld dat naar aanleiding van het voorbereidend onderzoek een nader onderzoek is ingesteld als bedoeld in artikel 32, vierde lid, Wbp. In dit kader zijn schriftelijke en telefonische inlichtingen bij de VPB ingewonnen die op 29 juni 2010 leidden tot een aangepast ‘Protocol Waarschuwingsregister Particuliere Beveiliging met Toelichting’ (verder: protocol).

Op 19 oktober 2010 is het ontwerpbesluit van het CBP – met daarin het voornemen de verwerking rechtmatig te verklaren – gepubliceerd in de Staatscourant 2010, nr. 16215. Gedurende de zes weken dat de onderliggende stukken van het ontwerpbesluit bij het CBP ter inzage lagen, zijn geen zienswijzen ontvangen. Op grond daarvan zet het CBP het ontwerpbesluit om in een definitief besluit.

3 Feitelijke weergave van het protocol

De VPB heeft ten aanzien van de voorgenomen verwerking in het protocol het volgende naar voren gebracht.

Aanleiding, belang en doel van het protocol

De particuliere beveiligingsbranche wordt regelmatig geconfronteerd met ontslag of vertrek van beveiligingsmedewerkers om integriteitsredenen. Voorbeelden zijn mishandeling, diefstal, fraude of rijden onder invloed in een dienstauto.

Volgens de VPB komt het veelvuldig voor dat een medewerker, die ontslagen wordt door een beveiligingsbedrijf en tegen wie aangifte is gedaan wegens handelingen in strijd met de gedragsregels, bij een ander beveiligingsbedrijf in dienst kan treden zonder dat de bevoegde instanties (politie en justitie) of het andere beveiligingsbedrijf kennis krijgen van het eerdere ontslag.

De VPB geeft aan dat de bestaande waarborgen om de integriteit en betrouwbaarheid van beveiligingspersoneel te waarborgen, i.e. de *screening* van nieuwe beveiligingsmedewerkers door (1) de politie en (2) de beveiligingsbedrijven zelf, niet toereikend zijn.

Ten aanzien van de *screening* door de politie geeft de VPB de volgende tekortkomingen aan. Allereerst verschilt de organisatie van de *screening* per politiekorps. Hierdoor komt het volgens de VPB voor dat beveiligers in de ene regio wel door de *screening* komen en in de andere niet. Daarnaast leidt aangifte tegen voorgenoemde gedragingen niet altijd tot een vermelding in de registers die door de politie bij een *screening* worden geraadpleegd. Ook komt relevante informatie niet automatisch uit het door de politie gehanteerde systeem (Verona) naar voren en is er geen landelijk dekkend systeem waarin risicovolle groepen (zoals beveiligers) worden bijgehouden en bewaakt. Daarnaast leidt aangifte zelden tot vervolging door justitie (bijvoorbeeld het delict is niet ernstig genoeg om tot vervolging over te gaan maar is wel reden voor ontslag van de medewerker). Wanneer wel tot vervolging wordt overgegaan is er geen systeem dat signaleert dat sprake is van een veroordeling van een beveiligingsmedewerker. De mogelijkheid bestaat – zo stelt de VPB – dat beveiligers, die formeel niet in aanmerking komen voor een legitimatiebewijs wegens een veroordeling, dit toch krijgen of behouden en in de branche werkzaam kunnen blijven ondanks ontslagen te zijn geweest. De komst van een centraal geautomatiseerd systeem bij de politie (Verona), heeft volgens de VPB wel enige verbetering gebracht in de *screening*, maar heeft de behoefte aan de introductie van een waarschuwingsregister niet ondervangen.

Voorts schiet ook de *screening* van personeel door beveiligingsbedrijven zelf te kort. De VPB geeft aan dat diepgaande *pre-employmentsscreening* onmogelijk kan worden uitgevoerd bij het aannemen van nieuwe medewerkers door het hoge personeelsverloop in de beveiligingssector.

Als aanvullende maatregel op de *screening* door politie en beveiligingsbedrijven, is de VPB voornemens een Waarschuwingsregister op te zetten. Het doel van het Waarschuwingsregister is voorkomen dat een beveiligingsmedewerker die ten gevolge van fraude en/of criminaliteit wordt ontslagen of om die reden zelf ontslag neemt, bij een ander beveiligingsbedrijf in dienst treedt zonder dat dit beveiligingsbedrijf kennis krijgt van het eerdere ontslag.

De VPB verwacht met het Waarschuwingsregister zowel de materiële als immateriële schade als gevolg van fraude en/of criminaliteit van beveiligingsmedewerkers te kunnen beperken.

Inhoud van het protocol Waarschuwingregister Particuliere Beveiliging

Beveiligingsbedrijven die zijn aangesloten bij het onderhavige protocol (hierna: deelnemers) hebben een incidentenregister waarin gedragingen van beveiligingsmedewerkers, die hebben geleid of kunnen leiden tot benadeling van beveiligingsbedrijven, worden vastgelegd. Deze registers worden beheerd door de veiligheidsafdeling of een daartoe geautoriseerde medewerker van de deelnemer. Uit het incidentenregister worden verwijzingsgegevens (NAW-gegevens, geslacht en geboortedatum) van betrokkenen via het Waarschuwingregister beschikbaar gesteld aan de andere deelnemers ten behoeve van de *screening* van sollicitanten.

Het Waarschuwingregister wordt geraadpleegd via een externe applicatie. Uit het protocol blijkt dat dit enkel gebeurt door personen belast met het personeelsbeleid van een deelnemer en bij gebleken geschiktheid van een sollicitant. Teneinde misbruik te voorkomen wordt iedere bevraging vastgelegd. Wanneer sprake is van een 'match' moet contact worden opgenomen met de eigen veiligheidsafdeling of een geautoriseerde medewerker. Deze neemt contact op met de primaire bron om na te gaan of het om dezelfde persoon gaat en of het geconstateerde delict aanname in de weg staat.

Op grond van de verkregen informatie adviseert de veiligheidsafdeling dan wel de geautoriseerde medewerker van het raadplegende beveiligingsbedrijf de afdeling personeelszaken of Human Resources over het al dan niet aangaan van een arbeidsrelatie. De afdeling personeelszaken of Human Resources neemt op basis hiervan een beslissing.

Het protocol beschrijft de volgende criteria voor opname van een ex-medewerker in het Waarschuwingregister. Ten eerste moet sprake zijn van fraude en/of criminaliteit in de vorm van geweldsdelicten, vermogensdelicten of ernstige verkeersmisdrijven. Voorts moet aangifte zijn gedaan bij de politie en moet de gedraging hebben geleid tot ontslag of beëindiging van de arbeidsrelatie. Daarnaast moeten er voldoende bewijsstukken zijn en worden bewaard in het onderliggende dossier. Tenslotte moet de fraude en/of criminaliteit niet gering in omvang zijn en in principe aanleiding zijn voor een veroordeling door justitie of, indien gering van aard, meerdere malen (twee keer of meer) gepleegd.

Feitelijke opname van een ex-medewerker in het Waarschuwingregister geschiedt pas na uitvoering van een proportionaliteitstoets door de veiligheidsafdeling of de geautoriseerde medewerker van een deelnemer. Bij de uitvoering van deze proportionaliteitstoets wordt volgens het protocol rekening gehouden met verschillende factoren, waaronder functie van de betrokkene, aard en omvang van de gedraging en of sprake is van verzachtende of verzwarende omstandigheden.

Wanneer zijn gegevens in het incidentenregister respectievelijk het Waarschuwingregister worden opgenomen, wordt de ex-medewerker hiervan op de hoogte gesteld. Nieuwe medewerkers worden voorafgaand aan het sluiten van een overeenkomst geïnformeerd dat toetsing aan het Waarschuwingregister deel uitmaakt van de sollicitatieprocedure. Het zittend personeel wordt op twee manieren geïnformeerd over het Waarschuwingregister: (1) indirect doordat instemming wordt gevraagd van de ondernemingsraad of personeelsvertegenwoordiging en (2) direct door het actief informeren van het personeel door bijvoorbeeld memo's en mededelingen.

Opname in het Waarschuwingregister geschiedt voor een periode van maximaal vier jaar, tenzij in die periode zich een nieuwe aanleiding voordoet voor opname. Na deze periode worden de gegevens verwijderd en vernietigd.

In het protocol wordt aan een betrokkene de mogelijkheid geboden zijn gegevens in te zien, te corrigeren en bij 'bijzondere persoonlijke omstandigheden' verzet aan te tekenen tegen de verwerking van zijn persoonsgegevens. Een betrokkene ontvangt binnen vier weken een schriftelijke reactie op zijn verzoek tot inzage, correctie of aangetekende verzet. Daarbij wordt de betrokkene gewezen op de mogelijkheid bij het CBP een verzoek om bemiddeling in te dienen of de zaak aan rechter voor te leggen.

Het bestuur van de VPB kan zich laten bijstaan door een auditcommissie die tot taak heeft het (doen) uitvoeren van controlewerkzaamheden ten aanzien van het gebruik van het Waarschuwingregister en de verplichtingen die voortvloeien uit het protocol, de Wbp of andere wet- en regelgeving.

Nieuwe deelnemers conformeren zich –zo blijkt uit het protocol- aan de beschreven aanpak, tekenen een toetredingsverklaring en melden hun incidentenregister bij het CBP.

4 Beoordeling van het protocol

Het CBP neemt als uitgangspunt voor zijn beoordeling van de rechtmatigheid van het 'Protocol Waarschuwingregister Particuliere Beveiliging' (versie van 29 juni 2010) de daaraan ten grondslag liggende melding en de informatie die schriftelijk door de VPB aan het CBP is verstrekt. Het CBP heeft geen onderzoek gedaan naar het gebruik van het Waarschuwingregister en de onderliggende incidentenregisters van de individuele deelnemers in de praktijk.

De verwerking van strafrechtelijke gegevens is verboden ingevolge artikel 16 Wbp, tenzij een van de bepalingen in artikel 22 of 23 Wbp van toepassing is. In de praktijk blijkt behoefte te bestaan om op brede schaal strafrechtelijke gegevens uit te wisselen, aldus de Memorie van Toelichting van de Wbp. Het gaat dan met name om uitwisseling tussen bedrijven in een bepaalde branche.

Artikel 22, vierde lid, onder c, Wbp geeft daarom een bijzondere regeling ter bescherming van de belangen van derden die het slachtoffer zouden kunnen worden van criminaliteit. Dit artikel stelt dat het verwerkingsverbod om strafrechtelijke gegevens ten behoeve van derden te verwerken vervalt als de verantwoordelijke voldoende passende en specifieke waarborgen treft en daarnaast de procedure van een voorafgaand onderzoek is gevolgd, zoals bedoeld in artikel 31 Wbp. De getroffen waarborgen worden hierna besproken en beoordeeld.

Artikel 7 Wbp vereist dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld mogen worden. De VPB beoogt volgens de beschrijving in het protocol met het Waarschuwingregister te voorkomen dat zonder meer een contractuele relatie wordt aangegaan met een persoon die ten gevolge van fraude en/of criminaliteit door een van de deelnemers is ontslagen of met wie om die reden de arbeidsrelatie is beëindigd en tegen wie aangifte bij de politie is gedaan. De beschreven

doeleinden voor het Waarschuwingregister zijn daarmee voldoende duidelijk en gerechtvaardigd en voldoen aan de in artikel 7 Wbp gestelde eisen.

Een verwerking van persoonsgegevens dient te berusten op een grondslag zoals bedoeld in artikel 8 Wbp. Voor het Waarschuwingregister kan een dergelijke grondslag enkel worden gevonden in artikel 8, aanhef onder f, Wbp. Dit artikel vereist dat een verwerking noodzakelijk is voor de behartiging van een gerechtvaardigd belang van de verantwoordelijke dat prevaleert boven het recht van een betrokkene op bescherming van zijn persoonlijke levenssfeer. Daarbij dient de verantwoordelijke rekening te houden met de beginselen van proportionaliteit en subsidiariteit.

Het protocol van de VPB geeft voldoende blijk van een zorgvuldige belangenafweging tussen het gerechtvaardigde belang van de VPB en de deelnemers en de belangen van betrokkenen bij bescherming van hun rechten en vrijheden, in het bijzonder de bescherming van de persoonlijke levenssfeer. Bij die afweging is blijkens de toelichting bij het protocol rekening gehouden met de beginselen van proportionaliteit en subsidiariteit. Ook is voorgeschreven dat de deelnemer in elk individueel geval nogmaals een proportionaliteitstoets toepast. Daarmee voorziet het protocol in een wettelijke grondslag voor de verwerking.

Voorts mogen op grond van artikel 9 Wbp persoonsgegevens niet verder worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor de gegevens zijn verkregen. Het protocol voldoet aan dit artikel nu is vastgelegd dat het gebruik van het Waarschuwingregister bedoeld is voor *screening* van nieuwe medewerkers, doch uitsluitend voor zover deze personen beveiligingswerkzaamheden in de zin van de Wpbr zullen gaan verrichten.

Ingevolgde artikel 10 Wbp mogen persoonsgegevens ‘niet langer worden bewaard dan noodzakelijk is voor het bereiken van de doelstelling van de verwerking’. In het protocol is bepaald dat gegevens uit het Waarschuwingregister worden verwijderd indien vastlegging van persoonsgegevens niet langer gewenst is. Verwijdering moet voorts plaatsvinden binnen een periode van maximaal vier jaar. Daarnaast vindt verwijdering plaats op verzoek van de betrokkene, indien de gegevens feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend, dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Gelet op de doeleinden waarvoor de gegevens worden verzameld, is de bewaartermijn voor de gegevens in het Waarschuwingregister in overeenstemming met artikel 10 van de Wbp.

De verwerking van persoonsgegevens is alleen toegestaan voor zover die gegevens toereikend, ter zake dienend en niet bovenmatig zijn. Bovendien moeten deze gegevens juist en nauwkeurig zijn (artikel 11 Wbp). Het protocol voorziet in een afgebakend aantal noodzakelijk geachte persoonsgegevens voor de registratie van de ontslagen medewerker in het Waarschuwingregister, namelijk NAW-gegevens, geslacht en geboortedatum. De kwaliteit van de persoonsgegevens wordt volgens het protocol geborgd door instructies voor omgang met de gegevens aan de veiligheidsafdeling of de geautoriseerde medewerker. Wanneer invoer van gegevens niet kan plaatsvinden conform de regels van het protocol, wordt van invoer afgezien. Daarmee voldoet het protocol aan de eisen van artikel 11 Wbp.

Ten aanzien van de beveiliging van gegevens bevat het protocol passende technische en organisatorische maatregelen (artikel 13 Wbp). Het protocol regelt de fysieke en digitale toegang tot de persoonsgegevens en beperkt de toegang tot de daartoe geautoriseerde functionarissen of medewerkers van de deelnemers. Het protocol besteedt ook aandacht aan de vertrouwelijkheid van gegevens (artikel 12 Wbp); het geautoriseerde personeel valt onder een geheimhoudingsplicht.

Een verantwoordelijke dient zorg te dragen voor de naleving van de materiële vereisten – zoals artikelen 6-12 Wbp – die de Wbp aan een verwerking stelt (artikel 15 Wbp). Het protocol sluit aan bij deze wettelijke verplichting door een periodieke controle van de deelnemers op de naleving van de bepalingen in het protocol. Ter bewaking van het rechtmatige gebruik van het Waarschuwingsregister wordt door de VPB een auditcommissie opgericht die als taak heeft het (doen) uitvoeren van controlewerkzaamheden ten aanzien van het gebruik van het Waarschuwingsregister door de verantwoordelijke of de deelnemer en de verplichtingen die dienaangaande voortvloeien uit het protocol. Verder blijkt uit het protocol dat iedere deelnemer zich conformeert aan het protocol middels een toetredingsverklaring. Het protocol voorziet hiermee in de zorg voor naleving van de materiële vereisten van de Wbp.

Het CBP stelt vast dat het protocol voorziet in de naleving van de wettelijke informatieplicht uit artikel 33 en 34 van de Wbp. Voorafgaand aan het afsluiten van een arbeidsovereenkomst wordt de betrokkene geïnformeerd dat toetsing aan het Waarschuwingsregister deel uitmaakt van de sollicitatieprocedure. Op deze wijze worden alle nieuwe medewerkers van het bestaan van het register op de hoogte gesteld. Ook het zittend personeel wordt, zowel indirect via de ondernemingsraad of personeelvertegenwoordiging als direct via memo's en berichten, geïnformeerd. Verder beschrijft het protocol de individuele informatieverstrekking: wanneer opname in het Waarschuwingsregister plaatsvindt, zal de ontslagen medewerker hierover worden geïnformeerd.

De rechten van betrokken in de Wbp voorzien in belangrijke corrigerende waarborgen tegen ongerechtvaardigde inbreuken op de persoonlijke levenssfeer van de betrokkenen. In het protocol wordt – in overeenstemming met de Wbp – aan betrokkene de mogelijkheid geboden te verzoeken om inzage of correctie van de verzamelde gegevens (artikel 35 en 36 Wbp). Binnen de wettelijk vastgestelde termijn van vier weken wordt een volledig schriftelijk overzicht in begrijpelijke vorm verstrekt van de aard en omvang van de verzamelde gegevens van betrokkene en het gebruik dat ervan gemaakt wordt. Daarnaast kan een betrokkene verzoeken zijn gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn, of in strijd met een wettelijk voorschrift worden verwerkt. Bij 'bijzondere persoonlijke omstandigheden' kan een betrokkene verzet aantekenen tegen de verwerking van zijn persoonsgegevens (artikel 40 Wbp).

De artikelen 46 en 47 Wbp geven een betrokkene – bij verschil van mening over zijn rechten met een verantwoordelijke – de mogelijkheid zijn zaak voor te leggen aan de rechter of bij het CBP een verzoek om bemiddeling in te dienen. In het protocol wordt hierin voorzien, waardoor de beschreven verwerking ook op dit punt in overeenstemming is met de Wbp.

5 Conclusie

Op grond van het voorgaande stelt het CBP vast dat de door de melder beschreven voorgenomen verwerking 'Protocol Waarschuwingsregister Particuliere Beveiliging met Toelichting' voldoende waarborgen bevat, zodat het CBP besluit de voorgenomen verwerking rechtmatig te achten.

De rechtmatigheidsverklaring kent een geldigheidsduur van ten hoogste zes jaar. Deze verklaring laat onverlet dat de VPB gedurende de voorgenoemde periode dient na te gaan of de verwerking nog noodzakelijk is voor het doel en dat klachten of andere informatie (bijvoorbeeld veranderingen in de geschetste screeningsproblematiek) over de verwerking er alsnog toe kunnen leiden dat het CBP nadere inlichtingen inwint of een onderzoek start.

6 Afsluiting en rechtsmiddel

Op het voorafgaand onderzoek is de 'uniforme openbare voorbereidingsprocedure' van afdeling 3.4 van de Algemene wet bestuursrecht (Awb) van toepassing. Dit houdt onder meer in dat de zakelijke inhoud van het besluit in de Staatscourant wordt gepubliceerd en gedurende zes weken ter inzage zal worden gelegd bij het CBP ingevolge artikel 3:11 Awb.

Belanghebbenden kunnen binnen zes weken na publicatie van dit besluit om de beschreven verwerking rechtmatig te verklaren beroep instellen tegen dit besluit bij de sector bestuursrecht van de rechtbank. Het indienen van een beroepschrift schort de werking van dit besluit niet op. Indien onverwijld spoed – gelet op de betrokken belangen – dat vereist kan de voorzieningenrechter van de rechtbank worden verzocht een voorlopige voorziening te treffen.

Den Haag, 14 december 2010

Namens het College bescherming persoonsgegevens,
Voor het College,

Mw. mr. dr. J. Beuving
Lid van het College