

R e g i s t r a t i e k a m e r

's-Gravenhage, 19 maart 2001

Ons kenmerk z2000-0080

Onderwerp Biometrisch toegangscontrolesysteem VIS 2000

Inleiding

Uw cliënte B b.v. brengt voor horeca- en sportgelegenheden het toegangscontrolesysteem VIS 2000 op de markt. Hierbij wordt gebruik gemaakt van biometrische gegevens van bezoekers. Deze en andere gegevens van ongewenste bezoekers worden op een elektronische zwarte lijst geplaatst.

Dit systeem gaf de Registratiekamer aanleiding tot het instellen van een onderzoek, waaraan door uw cliënte medewerking is verleend (zie voor een beschrijving van de gang van zaken bijlage 1). De Registratiekamer heeft u per brief haar aanbevelingen doen toekomen. Vervolgens heeft uw cliënt op deze aanbevelingen gereageerd. Uw cliënt deelde mede de aanbevelingen over te zullen nemen en gaf aan goed te kunnen leven met de conclusies.

In deze brief behandelt de Registratiekamer achtereenvolgens:

- de met biometrie samenhangende begrippen in het VIS 2000 (1)
- de werking van het VIS 2000 (2)
- de toetsing van dit systeem aan de wetgeving ter bescherming van persoonsgegevens, in het bijzonder van het gebruik van biometrische gegevens voor toegangscontrole, marketingdoeleinden en de zwarte lijst (3);
- conclusies en aanbevelingen (4), met daarin verwerkt de reactie van B en de reactie daarop van de Registratiekamer.

Uw brief

Bijlagen

Contactpersoon

Doorkiesnummer

Prins Clauslaan 20

Postbus 93374

2509 AJ 's-Gravenhage

Tel. 070-3811300

Fax 070-3811301

Datum 19 maart 2001

Ons kenmerk z2000-0080

Blad 2

1. Begrippen

Alvorens de voorgelegde feiten uiteen te zetten vermeld ik voor de goede orde wat de Registratiekamer bedoelt, wanneer zij in deze brief de begrippen ‘template’, ‘scan’, ‘identificatie’ en ‘verificatie/authenticatie’ gebruikt.

Met een *template* wordt de binaire representatie van lichaamskenmerken bedoeld. In de voorliggende zaak zijn het gezicht en de vinger de lichaamskenmerken.

Onder een *scan* wordt het aftasten van een object verstaan, met als doel het opsporen van markante punten.

Bij *identificatie* wordt in aanwezigheid van de betrokken persoon vastgesteld wie iemand werkelijk is.

Bij *verificatie* of *authenticatie* wordt niet onderzocht wie iemand werkelijk is, maar wordt vastgesteld dat twee gegevens bij dezelfde persoon horen. Er vindt daarbij een vergelijking plaats met een ander gegeven. Op deze wijze wordt vastgesteld dat iemand is wie hij claimt te zijn. In de voorliggende zaak kan verificatie /authenticatie plaats vinden door de vergelijking van templates. De vergelijking leidt tot de uitkomst: wel of geen toegangsgerechtigde.

Gelet op de samenhang tussen beide vormen van onderzoek van de identiteit gaat de Registratiekamer er evenwel vanuit dat beide zijn te rubriceren onder de uitzondering van het verbod tot verwerking van rasgegevens als bedoeld in artikel 18 onder a van de Wet bescherming persoonsgegevens (zie nader onderdeel 3.3).

2. VIS 2000

Eerst volgt een beschrijving van de werking van VIS 2000 voor zover in dit kader relevant. Daarna worden de vanuit de privacywetgeving relevante doelstellingen van het systeem beschreven.

Datum 19 maart 2001

Ons kenmerk z2000-0080

Blad 3

2.1 Werking VIS 2000

Ieder die voor de eerste maal een horeca- of sportgelegenheid bezoekt, welke is aangesloten bij VIS 2000, is verplicht om plaats te nemen voor een 'biomaat'. Vervolgens wordt van zijn of haar gezicht door een camera een digitale opname gemaakt. Deze digitale opname wordt in een template vertaald. De bio-engine van VIS 2000 is in staat om van de template van het gezicht een bruikbare gezichtsopname te reconstrueren. Ook wordt een scan gemaakt van de wijsvinger van de bezoeker die vervolgens direct wordt vertaald in een template. De biomaat bevat verder een monitor, een kaartlezer en een printer. De apparatuur is gekoppeld aan een personal computer met behulp waarvan de gegevens in de database van de exploitant worden vastgelegd. De gegevens die hierin worden vastgelegd zijn in ieder geval de template van het gezicht en de template van de vinger. Deze gegevens worden in beginsel korte tijd bewaard, namelijk tot de gelegenheid gesloten is voor bezoekers en indien er geen wanordelijkheden zijn voorgevallen.

De bezoekers van de gelegenheden hebben de mogelijkheid om 'lid' te worden van de desbetreffende discotheek, club, etc. Sommige exploitanten stellen het lidmaatschap zelfs verplicht voor het bezoek van hun gelegenheid. Als een bezoeker besluit om lid te worden, wordt hem of haar gevraagd om een aantal aanvullende gegevens. Dit zijn in de regel de naam-, adres- en woonplaats- (NAW-)gegevens. Maar dit kunnen ook aanvullende gegevens zijn, zoals leeftijd, interesses, voorkeuren, etc. Of het aspirant-lid verplicht is om deze gegevens te geven, bepaalt de exploitant van de desbetreffende gelegenheid.

Alle gegevens van het lid - dit zijn de bij het eerste bezoek vervaardigde template van het gezicht en de template van de vinger, de door hem c.q. haarzelf gegeven gegevens en het lidmaatschapsnummer - worden vastgelegd in de database van de exploitant. Deze gegevens blijven opgeslagen in dit bestand.

Bij een nieuw bezoek is herkenning van de bezoeker, die lid is geworden, mogelijk doordat deze een lidmaatschapspas krijgt in de vorm van een smartcard. Hierop staan naast het lidmaatschaps- of kaartnummer zijn of haar biometrische gegevens. Bij ieder

Datum 19 maart 2001

Ons kenmerk z2000-0080

Blad 4

volgend bezoek moet het lid zijn smartcard in de kaartlezer van de biomaat steken, waarna authenticatie plaatsvindt.

Een belangrijk onderdeel van VIS 2000 is de centrale zwarte lijst waarin gegevens zijn vastgelegd van personen die zich schuldig hebben gemaakt aan nader omschreven misdragingen. Deze kunnen hebben plaatsgevonden in elk van de gelegenheden die deelnemen aan VIS 2000. De gegevens die in deze database worden vastgelegd zijn de templates van gezicht en vinger van de betrokkene, diens kaartnummer en een codering die de aard van de misdraging aangeeft.

Met het kaartnummer kan de exploitant die de kaart heeft uitgegeven de identiteit van de kaarthouder herleiden, mits deze de daarvoor benodigde personalia heeft opgegeven.

2.2 Doelstellingen VIS 2000

Met het vastleggen van gegevens van iedere bezoeker van een horeca- of sportgelegenheid beoogt de exploitant daarvan – in eerste instantie - de orde te handhaven en daarmee de veiligheid van alle aanwezigen (bezoekers en medewerkers) te vergroten. Hiertoe is het noodzakelijk dat een eventuele onruststoker kan worden herkend, dan wel dat zijn identiteit achteraf kan worden achterhaald, bijvoorbeeld als hij de gelegenheid in het tumult na de misdraging ongemerkt heeft kunnen verlaten. Met VIS 2000 is deze identiteitscontrole mogelijk, doordat de exploitant in ieder geval voor de duur van de openingstijd van zijn gelegenheid beschikt over een bestand met templates van de gezichten van alle bezoekers, die door de bio-engine van VIS 2000 kunnen worden vertaald in een bruikbare gezichtsopname.

In de praktijk zal het ook kunnen voorkomen dat de exploitant gebruik maakt van een systeem van videocamera's om op deze wijze te kunnen vaststellen wie de onrust heeft veroorzaakt. Door de videobeelden te vergelijken met de door de bio-engine vertaalde templates van de gezichten van de bezoekers kan de onruststoker worden herkend. Zijn gegevens, in ieder geval de templates van vinger en gezicht, kunnen zonodig in de centrale zwarte lijst worden opgenomen. Indien de onruststoker in het bezit is van een lidmaatschapskaart, kunnen diens NAW-gegevens ook snel worden achterhaald.

Het systeem VIS 2000 verifieert ook of de bezoeker die reeds in het bezit is van een smartcard de rechtmatige eigenaar hiervan is door een vergelijking van de op de

Datum 19 maart 2001

Ons kenmerk z2000-0080

Blad 5

smartcard vastgelegde templates van gezicht en vinger van de bezoeker met de door de biomaat digitaal opgenomen en gescande gegevens.

Vervolgens wordt geverifieerd of de bezoeker op de (centrale) zwarte lijst staat op basis waarvan de toegang kan worden geweigerd. Deze verificatie vindt plaats door templates van de vingers en de gezichten die zijn vastgelegd in de zwarte lijst te vergelijken met de door de biomaat gegenereerde templates van gezicht en vinger. Het vastleggen van de templates van de vingers en de gezichten in een centraal bestand vindt plaats om toegang te kunnen weigeren aan ongewenste bezoekers.

Naast de beoogde doelstellingen in het kader van orde en veiligheid is het mogelijk dat de in VIS 2000 vastgelegde gegevens ook voor commerciële doeleinden (zoals marketing) worden gebruikt. Verder bestaat ook de mogelijkheid om managementinformatie op basis van de vastgelegde gegevens te produceren. Het opsporen van strafbare feiten is niet een op zichzelf staande doelstelling van VIS 2000. Aan het ondersteunen van politie en justitie bij het opsporen van strafbare feiten kan met behulp van VIS 2000 echter wel nadere invulling worden gegeven.

2.3 Samenvatting van de voorgelegde feiten

Een horeca- en/of sportgelegenheid die gebruikt maakt van VIS 2000 verwerkt gegevens over personen. Deze gegevens worden in ieder geval opgeslagen op een smartcard, die als toegangs- en eventueel ook als lidmaatschapspas dient, en – in elk geval tijdelijk - in een database van de ondernemer. Opslag in de centrale zwarte lijst volgt bij geconstateerd wangedrag. Van de personen met betrekking tot wie gegevens worden vastgelegd worden in ieder geval de template van de digitale opname van het gezicht, een template van de scan van de vinger, videobeelden en (voor zover het leden betreft) de NAW- gegevens vastgelegd. Deze gegevens worden vastgelegd met het oog op de verwezenlijking van de volgende doelen: toegangscontrole, - eventueel - marketing en management aangelegenheden. B zal zorgdragen voor gescheiden opslag van de gegevens voor de fysieke toegang (waaronder de biodata) en opslag in een aparte database van de gegevens welke voor marketingdoeleinden gebruikt zullen worden. Het ondersteunen van politie en justitie activiteiten is een potentieel gebruiksdoel van de opgeslagen gegevens.

Datum 19 maart 2001

Ons kenmerk z2000-0080

Blad 6

3. Toetsing van VIS 2000

De Registratiekamer merkt op dat het gaat om verwerking van biometrische persoonsgegevens ten behoeve van toegangscontrole. De Registratiekamer stelt dat dit een ingrijpend middel is. Er dient bezien te worden of dit middel in een juiste verhouding staat tot het doel met het oog waarop het wordt ingezet.

De Registratiekamer toetst de werking van VIS 2000 aan de Wet bescherming persoonsgegevens (WBP, Stb. 2000, 302) die in de loop van dit jaar in werking zal treden.

Een bijzonder element van VIS 2000 is het gebruik van biometrische gegevens van bezoekers van horeca- en sportgelegenheden voor verschillende doeleinden: toegangscontrole, eventueel plaatsing op de zwarte lijst, marketing en managementinformatie. Hierop concentreert de Registratiekamer dan ook haar reactie.

In VIS 2000 komen ook andere vormen van het gebruik van persoonsgegevens voor waarover de Registratiekamer zich al eerder heeft uitgelaten. Zij gaat er vanuit dat uw cliënt, bij deze aspecten met haar zienswijze in deze rekening houdt. Met name betreft dit het gebruik van videocamera's, foto's, zwarte lijsten en klantgegevens.

Achtereenvolgens zijn in dit verband relevant de documenten:

- 'In beeld gebracht; Privacyregels voor het gebruik van videocamera's voor toezicht en beveiliging', Registratiekamer, januari 1997;
- 'Over het gebruik van foto's; de brief van de Registratiekamer aan Horeca Nederland', d.d. 18 augustus 2000, nr. z2000-0684.04;
- 'Zwarte lijsten; belangen en effecten van waarschuwingssystemen', A.F. Rommelse, Registratiekamer, mei 1995;
- 'Koning Klant; Het gebruik van klantgegevens voor marketingdoeleinden', M.J.T. Artz, Registratiekamer, juli 1999;
- 'At face value; On biometrical identification and privacy', R. Hes e.a., Registratiekamer, september 1999.
- 'Beveiliging van persoonsgegevens', J.J. Borking en G.W. van Blarckom, Registratiekamer, maart 2001

Datum 19 maart 2001

Ons kenmerk z2000-0080

Blad 7

3.1 Biometrische gegevens: bijzondere persoonsgegevens?

Van VIS 2000 vormt de opslag van biometrische gegevens een belangrijk element. Biometrische gegevens bevatten informatie over unieke lichaamskenmerken van personen. De Registratiekamer heeft zich in haar studie 'At face value' uitgelaten over biometrische identificatie en privacy. Van belang is dat biometrische gegevens in dit verband en in elk geval gedurende de thans relevante fasen van het gebruik beschouwd moeten worden als persoonsgegevens in de zin van artikel 1 van de WBP.

De vraag is vervolgens of de in VIS 2000 gebruikte gegevens tevens zijn aan te merken als bijzondere gegevens als bedoeld in artikel 16 van de WBP. In casu wordt een scan van de vinger en een digitale opname van het gezicht gemaakt, die beide in een template worden vertaald; de gezichtopname en de vingerscan. De opname en de scan leveren bijzondere gegevens op (zie 'At face value', pagina 37). Een dergelijk gegeven kan met name worden aangemerkt als een persoonsgegeven betreffende iemands ras. De templates die hiervan worden vastgelegd zijn echter niet automatisch aan te merken als een bijzonder gegeven. Dit hangt af van de vraag of uit de template een volledig signaal is af te leiden.

Uit de stukken van B BV is gebleken dat het gebruikte algoritme kan 'terugrekenen' en zo de oorspronkelijke scan kan reconstrueren.

Tevens is vastgesteld dat de template van het gezicht wordt vastgelegd in het bestand van de exploitant van de gelegenheid. De template van het gezicht van leden blijft opgeslagen gedurende de gehele periode van lidmaatschap. Uit het oorspronkelijke gezicht zijn in principe steeds rasgegevens af te leiden. De gezichtstemplate is daarom als een bijzonder gegeven aan te merken.

Voor de vingerscan geldt in het algemeen dat deze gegevens betreffende iemands ras kan bevatten. Hiervoor geldt derhalve hetzelfde als bovengesteld met betrekking tot de gezichtstemplate. In casu is er evenwel geen sprake van het vastleggen van deze scan in een bestand; slechts de template van de scan wordt vastgelegd. Deze template is, voor zover bij de Registratiekamer bekend, niet te herleiden tot het oorspronkelijke lichaamskenmerk en vormt derhalve geen bijzonder gegeven.

Datum 19 maart 2001

Ons kenmerk z2000-0080

Blad 8

3.2 Rechtsgrond verwerking van bijzondere persoonsgegevens

Ter beoordeling staat vervolgens de rechtmatigheid van de verwerking van biometrische gegevens die zijn aan te merken als bijzondere gegevens. In het algemeen zal voor het verwerken van persoonsgegevens een grondslag nodig zijn als omschreven in artikel 8 WBP. Voor de bijzondere persoonsgegevens waarvan in dit kader ook sprake is, moet worden gezien of er een ontheffing bestaat van het in de Wet bescherming persoonsgegevens neergelegde verbod om bijzondere gegevens te verwerken (artikel 16 WBP). Deze ontheffingen zijn limitatief genoemd in hoofdstuk w, paragraaf 2, van de WBP. In casu is met name artikel 18 WBP van belang waarin de gevallen waarin persoonsgegevens betreffende iemands ras verwerkt mogen worden, zijn aangegeven.

3.3 Identificatie

Artikel 18, onder a, WBP geeft een ontheffing van het verbod om dergelijke persoonsgegevens te verwerken, indien die verwerking geschiedt met het oog op de identificatie van de betrokkene en slechts voor zover dit voor dit doel onvermijdelijk is. De vraag is dus of hiervan bij de toepassing van VIS 2000, met name bij de toegangscontrole en de plaatsing op de zwarte lijst van bezoekers sprake is.

De toegangscontrole dient ertoe, in combinatie met andere maatregelen, de identiteit van eventuele onruststokers vast te stellen en deze met behulp van de aan te leggen zwarte lijst later de toegang te kunnen weigeren. Nader te onderscheiden - in het licht van onderdeel 1 - gaat het achtereenvolgens om identificatie en - bij vergelijking met de zwarte lijst - om verificatie. Voor de exploitant van de horeca- of sportgelegenheid vormen deze maatregelen onderdeel van de handhaving van de orde en veiligheid in zijn gelegenheid.

Bij het vaststellen van de identiteit dan wel het verifiëren van de gegevens van eventuele onruststokers zal doorgaans het gebruik van de template van het gezicht, al of niet in aanvulling op geregistreerde videobeelden van de betrokkene, onvermijdelijk zijn. Indien is vastgesteld om wie het gaat, worden de templates van de vinger en van het gezicht van de bezoeker vastgelegd in een centrale zwarte lijst. Gelet op deze sleutelrol van het gebruik van deze gegevens in dit proces acht de Registratiekamer het voldoende aannemelijk dat voor de exploitant van een horeca- of sportgelegenheid het

Datum 19 maart 2001

Ons kenmerk z2000-0080

Blad 9

gebruik van de gezichtstemplate onvermijdelijk is. Voor zover het gaat om het vaststellen van de identiteit van bezoekers die tijdens hun bezoek onrust veroorzaken en het weren van deze onruststokers door hen betreffende gegevens op de centrale zwarte lijst te plaatsen en deze gegevens bij een volgend bezoek te vergelijken, is bij VIS 2000 dus aan het vereiste van artikel 18, onder a, WBP voldaan. Aangezien tevoren niet is te bepalen wie onrust zal kunnen gaan stoken is vastlegging van de onderhavige biometrische kenmerken van alle bezoekers gedurende 24 uren (tenzij er een duidelijk aanwijsbare reden bestaat om dit langer te doen) onvermijdelijk te achten en is ook in dit opzicht aan artikel 18, onder a, WBP voldaan.

3.4 Gerechtvaardigd belang

Daarnaast dient, zoals reeds is opgemerkt, het gebruik van biometrische gegevens te voldoen aan de vereisten van het gebruik van persoonsgegevens in het algemeen. Voor alle persoonsgegevens die in het kader van VIS 2000 worden verwerkt gelden de algemene vereisten van de WBP. Hoofdregel is dat gegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze dienen te worden verwerkt (artikel 6 WBP). Daarnaast moeten de gegevens worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (artikel 7 WBP), moet de verwerking een rechtmatige grondslag hebben (artikel 8 WBP) en mag de verwerking van de gegevens niet onverenigbaar zijn met het doel waarvoor de persoonsgegevens worden verzameld (artikel 9 WBP). Verder moet de voor de gegevensverwerking verantwoordelijke de betrokkenen op de hoogte stellen van de beoogde verwerkingen (artikel 33 dan wel 34 WBP).

Aan de vereiste doelspecificatie is voldaan door de omschrijving van de met het VIS 2000-systeem beoogde doeleinden. Als grondslag voor het gebruik van persoonsgegevens in dit kader komen zowel de behartiging van het gerechtvaardigd belang van de betrokken exploitant (artikel 8 onder f WBP) als de ondubbelzinnige toestemming van de bezoekers (artikel 8 onder a WBP) in aanmerking. In het algemeen kan het als een gerechtvaardigd belang van de exploitant worden beschouwd om gegevens over bezoekers te verzamelen met het oog op de handhaving van de orde en veiligheid in de horeca- of sportgelegenheid. Aan de belangen van de bezoeker wordt recht gedaan door het geven van een adequate voorlichting, het in acht nemen van een

Datum 19 maart 2001
Ons kenmerk z2000-0080
Blad 10

beperkte bewaartermijn en in het algemeen een zorgvuldig en selectief gebruik van de over hem verzamelde gegevens.

Vervolgens acht de Registratiekamer het gebruik van de (bijzondere) persoonsgegevens voor de verificatie van de bezoeker als lid dan wel als geplaatste op de zwarte lijst niet onverenigbaar met het doel waarvoor deze gegevens oorspronkelijk zijn verzameld, namelijk het kunnen verifiëren of er voor de biomaat een (voormalige) onruststoker staat. In onderling verband beschouwd is de Registratiekamer van oordeel dat de deelnemer aan VIS 2000 de elementen van artikel 9 WBP, uitgaande van de aan haar verstrekte informatie, in voldoende mate in deze verdere verwerkingen heeft verdisconteerd. De Registratiekamer benadrukt de - wettelijke - noodzaak van een adequate informatieverstrekking aan betrokkenen (artikel 33 WBP).

3.5 Uitdrukkelijke toestemming

Ontheffing van het verbod om bijzondere persoonsgegevens te verwerken is ook mogelijk ingevolge artikel 23, eerste lid, onder a, WBP. Volgens dit artikel geldt het verbod niet als de verwerking geschiedt met uitdrukkelijke toestemming van de betrokkene.

Voor iedere verdere verwerking van de bijzondere gegevens - anders dan ten behoeve van in de onderdelen 3.3 en 3.4 genoemde doeleinden - zal de bezoeker uitdrukkelijk toestemming moeten verlenen. Deze toestemming moet expliciet zijn en de verantwoordelijke moet kunnen aantonen dat de toestemming inderdaad is verleend. Een stilzwijgende of impliciete toestemming is onvoldoende: de betrokkene dient in woord, schrift of gedrag uitdrukking te hebben gegeven aan zijn wil toestemming te verlenen aan de hem betreffende gegevensverwerking. Een eenmaal gegeven toestemming tot het verzamelen van gegevens kan overigens te allen tijde worden ingetrokken. Als een toestemming is ingetrokken, dan kan deze niet langer dienen als grondslag voor de verwerking. Een dergelijke intrekking heeft echter geen consequenties voor gegevensverwerkingen die vóór het moment van de intrekking hebben plaatsgevonden. Voor deze kwestie is voorts van bijzonder belang het vereiste dat de toestemming in vrijheid is gegeven.

Datum 19 maart 2001

Ons kenmerk z2000-0080

Blad 11

De uitdrukkelijke toestemming voor het gebruik van biometrische gegevens zou dus gelet op de hiervoor omschreven doeleinden van VIS 2000 met name betrekking hebben op het gebruik van deze gegevens voor marketingdoeleinden. Op het eerste gezicht lijkt de WBP zich hiertegen niet te verzetten. Het knelpunt is evenwel gelegen in het element vrijwilligheid. Bezoekers hebben bij VIS 2000 zich de toegangscontrole en de plaatsing op een eventuele zwarte lijst met behulp van biometrische gegevens te laten welgevallen.

Voor een dwingende koppeling tussen dit gebruik en de aanwending van de hiervoor verzamelde gegevens voor marketingdoeleinden is geen rechtvaardiging te vinden. De toestemming kan door deze koppeling immers niet meer als in vrijheid gegeven worden beschouwd. Waar geen keuzemogelijkheid is, is vrijwilligheid een illusie. Vandaar dat de Registratiekamer u de mogelijkheid aanbeveelt om de dwingende koppeling tussen persoonsgegevens van leden ten behoeve van marketing en (biometrische) persoonsgegevens ten behoeve van toegangscontrole, orde en veiligheid op te heffen door de betreffende domeinen te compartimenteren.

Indien betrokkene voor marketing in aanmerking wenst te komen kan dit op grond van door hem te verstrekken algemene, NAW-gegevens geschieden. Ten aanzien van andere, aanvullende gegevens (zie onderdeel 1: leeftijd, interesses, voorkeuren) moet hem ook de vrijheid worden gelaten deze informatie te verstrekken. Voor het gebruik van hem betreffende biometrische gegevens is zijn uitdrukkelijke toestemming nodig.

Voor VIS 2000 betekent dit dat de bezoekers door de ondernemer over de werking van het systeem goed moeten worden voorgelicht. Het moet de betrokkene duidelijk worden gemaakt dat hij kan kiezen voor de onvermijdelijke, maar tijdelijke vastlegging van (bijzondere) persoonsgegevens dan wel voor vastlegging hiervan voor langere tijd uit hoofde van zijn lidmaatschap. De toestemming kan vervolgens verleend worden door op elektronische wijze zich akkoord te verklaren met het gebruik van biometrische en daarmee - ten dele - ook het gebruik van de (bijzondere) persoonsgegevens, mits dit er expliciet bij wordt vermeld.

Voor buiten de handhaving van de orde en veiligheid gelegen doelen dient de bezoeker in vrijheid te kunnen opteren. Kiezen voor het gebruik van met name diens NAW-gegevens voor marketingdoeleinden mag niet automatisch meebrengen

dat ook de biometrische gegevens hiervoor mogen worden aangewend. Pas bij keuzevrijheid wordt voldaan aan de ingevolge artikel 23, eerste lid onder a, WBP vereiste van toestemming.

3.6 Geen onnodige verwerkingen persoonsgegevens

Een relevante bepaling voor de onderhavige zaak is bovendien artikel 13 WBP, waarin de verplichting tot het treffen van de noodzakelijke technische en organisatorische maatregelen is opgenomen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen dienen er mede op gericht te zijn om onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. Mede gelet op artikel 13 WBP zij verwezen naar de mogelijkheid om gebruik te maken van privacybevorderende technologie. In casu betekent dit onder andere dat daar waar volstaan kan worden met verificatie in plaats van identificatie, voor verificatie gekozen dient te worden. Ook komt aanwending van bijzondere persoonsgegevens voor managementdoeleinden niet alleen met het hiervoor geldende bijzondere regime in strijd, maar ook met het algemeen geldende artikel 13 WBP.

3.7 Beveiligen verwerking persoonsgegevens

De beveiliging van persoonsgegevens kent drie kwaliteitsaspecten, te weten exclusiviteit, integriteit en continuïteit. De bescherming van de personen over wie persoonsgegevens worden verwerkt, vereist dat met name de exclusiviteit voldoende gewaarborgd wordt.

Het vereiste niveau van bescherming wordt bepaald aan de hand van een analyse op basis van de aard en omvang van de te beschermen persoonsgegevens, de soort verwerkingen en het te lopen risico als gevolg van verlies of onrechtmatige verwerking van de persoonsgegevens. Uit deze analyse volgt een risicoklasse. Op basis van het gestelde in de WBP worden vier risicoklassen onderkend. Nadat de risicoklasse is vastgesteld, bepaalt de verantwoordelijke de technische en organisatorische maatregelen die genomen moeten worden om het wettelijk vereiste, passende beveiligingsniveau te bereiken. Deze technische en organisatorische maatregelen behoren daarbij altijd een samenhangend stelsel te vormen, afgeleid uit een (informatie-) beveiligingsbeleid, (informatie-) beveiligingsplan en terug te vinden in een stelsel van algemene maatregelen en procedures.

Datum 19 maart 2001
Ons kenmerk z2000-0080
Blad 13

De verwerking van bijzondere gegevens vereist een verhoogd beschermingsniveau, daar er extra negatieve gevolgen bestaan voor de betrokkene, verantwoordelijke of bewerker bij onbehoorlijke of onzorgvuldige verwerking van deze persoonsgegevens.

Naar aanleiding hiervan beveelt de Registratiekamer u aan om de reconstructie van templates tot de oorspronkelijke gegevens onmogelijk te maken. Dit geldt zowel voor de in een bestand opgeslagen gegevens als voor de gegevens die op de chipcard worden opgeslagen. In onderhavige casus kan op dit vereiste slechts een uitzondering worden gemaakt gedurende de eerdergenoemde 24 uren (of zoveel langer als noodzakelijk is) met het oog op orde en veiligheid. Voorts beveelt de Registratiekamer u op grond van het bepaalde in artikel 13 WBP aan dat de templates en de kaartnummers versleuteld opgeslagen worden.

3.8 Bewaren en verstrekken van bijzondere gegevens

Artikel 10 WBP vereist dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk is voor de realisatie van de doeleinden waarvoor ze zijn verzameld of vervolgens worden verwerkt. In casu worden bijzondere gegevens van iedere bezoeker door de exploitant van een horeca- of sportgelegenheid vastgelegd om deze in geval van een misdraging te kunnen opnemen in een centrale zwarte lijst die wordt gebruikt ter identificatie van bezoekers van aan VIS 2000 deelnemende gelegenheden. Dit impliceert dat deze gegevens niet langer bewaard mogen blijven dan noodzakelijk. In het geval er geen misdraging heeft plaatsgevonden ontvalt de noodzaak en dient verwijdering van de bijzondere gegevens plaats te vinden. Langer bewaren hiervan kan rechtmatig zijn als de bezoeker hiermee uitdrukkelijk heeft ingestemd. Dit betekent dat het voor de bezoeker expliciet duidelijk moet zijn hoe lang de gegevens worden bewaard en voor welk doel. Ook eventuele overige relevante informatie, aangaande het bewaren van de gegevens, moet hem of haar worden verstrekt. De procedure voor verwijdering vraagt bijzondere aandacht. Het 'deleten' van gegevens is niet toereikend om dit te realiseren, aangezien herstel in de oorspronkelijke staat dan nog mogelijk is.

De Registratiekamer stelt dat na 24 uren de noodzaak voor het bewaren van de bijzondere gegevens ontvalt, indien er geen misdragingen hebben plaatsgevonden en de Registratiekamer stelt dat de bijzondere gegevens na deze periode verwijderd dienen te worden, tenzij betrokkene toestemming heeft gegeven voor het bewaren van de

bijzondere gegevens of tenzij er een duidelijk aanwijsbare reden is om de gegevens langer te bewaren.

3.9 Zwarte lijst

Voor het opnemen van gegevens in een zwarte lijst is het noodzakelijk dat er voldoende waarborgen zijn getroffen voor de bescherming van de persoonlijke levenssfeer van de betrokkene. De Registratiekamer verwijst hierbij naar haar uitgave 'Zwarte lijsten, belangen en effecten van waarschuwingssystemen'. Meer concreet betekent dit voor de zwarte lijst behorende bij VIS 2000, dat aan de volgende criteria dient te worden voldaan.

1. *Doelbinding*. Leg vast wat het exacte doel is van de lijst. Stel ook nauwkeurig vast op grond waarvan iemand op de zwarte lijst wordt geplaatst. Er dienen duidelijke normen en criteria te zijn, die vaststellen op grond van welke gedragingen betrokkenen in de zwarte lijst kunnen worden opgenomen.
2. *Belangenafweging*. Als het doel ook op een minder ingrijpende manier kan worden bereikt, dan moet voor die andere manier worden gekozen.
3. *Verstreking van gegevens*. Vergewis u er van dat er niet meer gegevens dan noodzakelijk worden verstrekt en leg van tevoren vast aan wie de gegevens verstrekt mogen worden.
4. *Transparantie*. Hoe en op welke wijze wordt 'de onruststoker' in kennis gesteld van het feit dat hij op een zwarte lijst zal worden geplaatst? In welke gevallen wordt de betrokken persoon van de lijst verwijderd?
5. *Zorgvuldigheid*. Hoe verifieert u of de gegevens op uw lijst juist zijn? Op welke wijze kan de (vermeende) onruststoker bezwaar maken tegen opname?
6. *Rechten van de geregistreerde*. Heeft u voldoende technische en organisatorische maatregelen getroffen voor de wijze waarop de geregistreerde zijn inzage- en correctierecht kan uitoefenen?

De Registratiekamer beveelt u aan voor het gebruik van de centrale database als zwarte lijst de bovengestelde criteria uit te werken.

4. Conclusies en aanbevelingen

De Registratiekamer stelt dat verwerking van biometrische persoonsgegevens ten behoeve van toegangscontrole een ingrijpend middel is. Het is van belang om te bezien of dit middel in deze zaak niet bovenmatig is.

De Registratiekamer heeft de werking van VIS 2000 getoetst aan de Wet bescherming persoonsgegevens (WBP) die in de loop van dit jaar in werking zal treden. Op grond hiervan komt de Registratiekamer tot de volgende conclusies en aanbevelingen, waarvan B inmiddels in kennis is gesteld. In het algemeen neemt B de aanbevelingen over.

Cursief is de reactie van B overgenomen.

In de eerste plaats dienen de biometrische gegevens die in VIS 2000 verwerkt worden in elk geval gedurende de thans relevante fasen van het gebruik beschouwd te worden als persoonsgegevens.

B neemt deze vaststelling voor kennisgeving aan.

In de tweede plaats worden in VIS 2000 bijzondere persoonsgegevens verwerkt, te weten rasgegevens. Vastgesteld is namelijk dat de template van het gezicht (een digitale foto) te reconstrueren is tot de kenmerken van het oorspronkelijke gezicht. Uit het oorspronkelijke gezicht kan informatie over het ras worden afgeleid.

Overigens valt de vingertemplate waar VIS 2000 gebruik van maakt, voor zover bij de Registratiekamer bekend, niet te herleiden tot oorspronkelijke lichaamskenmerken. Bij die toepassing worden dus geen bijzondere gegevens verwerkt.

B neemt deze vaststelling voor kennisgeving aan.

In de derde plaats kan het verwerken van rasgegevens ten behoeve van de gezichtstemplate volgens de Registratiekamer ten dele gerechtvaardigd worden op grond van artikel 18, onder a, WBP. Voor de vaststelling van de identiteit van de bezoeker die tijdens zijn bezoek onrust veroorzaakt acht de Registratiekamer het namelijk onvermijdelijk dat gebruik wordt gemaakt van de betreffende gezichtstemplates. Gedurende de periode die redelijkerwijs onvermijdelijk is om te bepalen wie onrust heeft veroorzaakt is vastlegging van de te reconstrueren

Datum 19 maart 2001

Ons kenmerk z2000-0080

Blad 16

gezichtstemplates te rechtvaardigen. De Registratiekamer stelt deze periode op 24 uren, mede gelet op artikel 13 WBP, tenzij er een duidelijk aanwijsbare reden bestaat voor een langere bewaartermijn. Deze stellingname wordt nog eens ondersteund door de beveiligingsbepalingen in artikel 13 WBP. De Registratiekamer beveelt u daarom aan uw systeem wat dat betreft aan te passen door reconstructie van templates tot de oorspronkelijke gegevens onmogelijk te maken met uitzondering van de gezichtstemplate voor, in beginsel, de periode van 24 uren.

B geeft aan de aanbeveling te zullen opvolgen. De gezichtstemplate zal in de database bewaard blijven tot maximaal 24 uur na sluiting van de betreffende gelegenheid, uitgezonderd de situatie waarin de betrokkene waartoe de template behoort aan de blacklist dient te worden toegevoegd.

In de vierde plaats biedt VIS 2000 de mogelijkheid om de (bijzondere) gegevens die verwerkt worden ten behoeve van toegangscontrole en het handhaven van orde en veiligheid tevens te gebruiken voor marketingdoeleinden. Weliswaar biedt artikel 23, eerste lid, onder a, WBP de mogelijkheid om op grond van uitdrukkelijke toestemming van de betrokkene bijzondere gegevens te verwerken. Wil er echter sprake zijn van uitdrukkelijke toestemming van de betrokkene, dan moet deze toestemming expliciet zijn en aan moet de verantwoordelijke tevens kunnen aantonen dat de toestemming inderdaad is verleend. In het bijzonder is van belang het vereiste dat de toestemming in vrijheid moet zijn gegeven. Bezoekers hebben bij VIS 2000 zich echter de toegangscontrole en de plaatsing op een eventuele zwarte lijst met behulp van biometrische gegevens te laten welgevalen. Voor een dwingende koppeling tussen dit gebruik en de aanwending van de hiervoor verzamelde gegevens voor marketingdoeleinden is geen rechtvaardiging te vinden. De toestemming kan door deze koppeling immers niet meer als in vrijheid gegeven worden beschouwd. Waar geen keuzemogelijkheid is, is vrijwilligheid een illusie. Vandaar dat de Registratiekamer u de mogelijkheid aanbeveelt om de dwingende koppeling tussen persoonsgegevens van leden ten behoeve van marketing en (biometrische) persoonsgegevens ten behoeve van toegangscontrole, orde en veiligheid op te heffen door de betreffende domeinen te compartimenteren.

B geeft aan zorg te zullen dragen voor gescheiden opslag van de gegevens voor de fysieke toegang en opslag in een aparte database van gegevens welke voor

Datum 19 maart 2001
Ons kenmerk z2000-0080
Blad 17

marketingdoeleinden zullen worden gebruikt. Tevens zullen de marketinggegevens niet 'persoonsgebonden' worden opgeslagen, maar geaggregeerd.

In de vijfde plaats beveelt de Registratiekamer u aan om de ondernemers aan wie u VIS 2000 verkoopt er op te wijzen dat zij hun cliënten goed moeten voorlichten over de werking van het systeem. Het moet de betrokkene duidelijk worden gemaakt dat hij kan kiezen voor de onvermijdelijke, maar tijdelijke vastlegging van (bijzondere) persoonsgegevens dan wel voor vastlegging hiervan voor langere tijd uit hoofde van zijn lidmaatschap. De toestemming kan vervolgens verleend worden door op elektronische wijze zich akkoord te verklaren met het gebruik van biometrische en daarmee - ten dele - ook het gebruik van de (bijzondere) persoonsgegevens, mits dit er expliciet bij wordt vermeld.

B geeft aan dat ze haar gedragscode VIS 2000 zal aanscherpen om deze aanbeveling nader uit te werken.

De Registratiekamer onderstreept het belang van een adequate voorlichting aan de betrokkenen en gaat er vanuit dat dit aspect wordt meegenomen.

In de zesde plaats beveelt de Registratiekamer u aan om voor managementdoeleinden geen (bijzondere) persoonsgegevens te gebruiken. Voor managementdoeleinden kan en moet dan ook worden volstaan met geaggregeerde informatie.

B geeft aan deze aanbeveling integraal te zullen overnemen.

In de zevende plaats beveelt de Registratiekamer u op grond van het hiervoor genoemde artikel 13 WBP aan om uw systeem zodanig in te richten dat gekozen wordt voor verificatie waar volstaan kan worden met verificatie in plaats van identificatie.

B geeft aan dat identificatie wordt toegepast bij de toetsing op de blacklists, daar deze procedure volgens B zonder identificatie niet mogelijk is. B geeft aan dat verder alle procedures werken op basis van verificatie alleen.

De Registratiekamer neemt hiervan kennis.

In de achtste plaats beveelt de Registratiekamer u op grond van artikel 13 WBP eveneens aan om de templates en de kaartnummers versleuteld op te slaan, zowel op de chipcard als in de bestanden.

Datum 19 maart 2001

Ons kenmerk z2000-0080

Blad 18

B geeft aan dat het kaartnummer en de templates op de chipcard versleuteld zullen worden opgeslagen. De versleuteling van databasegegevens wordt nader onderzocht. De Registratiekamer gaat er vanuit dat er een toereikend niveau van bescherming van persoonsgegevens zal zijn. In deze verwijst de Registratiekamer naar haar binnenkort te verschijnen A&V studie nummer 23 'Beveiliging van persoonsgegevens', geschreven door G.W. van Blarkom en J.J. Borking.

In de negende plaats beveelt de Registratiekamer u aan de criteria uit haar rapport 'Zwarte lijsten, belangen en effecten van waarschuwingssystemen' uit te werken voor het gebruik van de centrale database.

B geeft aan dat ze hieraan gevolg zal geven.

De Registratiekamer gaat er vanuit dat u bevordert dat de voorgaande aanbevelingen, waarmee u aangaf zeer goed te kunnen leven, ook worden toegepast op alle bestaande VIS 2000 systemen. Waar nodig kan hierbij een korte overgangstermijn in acht worden genomen. De Registratiekamer vertrouwt er op dat u zorg zult dragen voor voorlichting in deze aan uw afnemers en dat u uw afnemers er op wijst dat ze zorg dienen te dragen voor een goede voorlichting aan hun cliënten.

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,

mr. U. van de Pol
plv. voorzitter

Datum 19 maart 2001

Ons kenmerk z2000-0080

Blad 19

Bijlage 1 Gang van zaken

Bij brief van 12 juli 2000 heeft de Registratiekamer, gelet op het maatschappelijk belang van de persoonlijke levenssfeer bij het vastleggen van biometrische gegevens, laten weten dat zij het systeem VIS 2000 van B aan een nader onderzoek wil onderwerpen.

Naar aanleiding van deze brief vond er op 31 augustus 2000 een onderhoud plaats tussen dhr. Velders (Interstat), mw. mr. M.D. Ubbink (Cohen De Jong van Lier Huiskes), dhr. mr. M.J.T. Artz en dhr. mr.dr. U. van de Pol (Registratiekamer).

Op 13 september 2000 ontvingen wij uw fax welke volgde op het genoemde onderhoud tussen B BV (B), Cohen De Jong van Lier Huiskes en de Registratiekamer. In dit overleg heeft de Registratiekamer een nadere toelichting gekregen op de introductie van een toegangscontrolesysteem (VIS 2000) waarbij gebruik gemaakt wordt van biometrische gegevens van bezoekers van met name horeca- en/of sportgelegenheden. Tijdens het overleg heeft u een concept-gedragscode alsmede een concept van een informatiebrochure voor het publiek overgelegd. De conceptgedragscode heeft u naar aanleiding van het onderhoud in aangepaste vorm als conceptreglement aan de Registratiekamer toegezonden met het bovenbedoelde faxbericht.

Daarbij verzoekt u de Registratiekamer om haar op- en of aanmerkingen ten aanzien van voornoemde stukken te geven. De Registratiekamer heeft in haar brief van 31 januari 2001 voldaan aan uw verzoek en geeft in de betreffende brief nader commentaar en aanbevelingen waarbij de Wet bescherming persoonsgegevens (Stb. 2000, 302; WBP) als richtsnoer is gebruikt. Deze wet zal naar verwachting medio 2001 in werking treden.

Datum 19 maart 2001

Ons kenmerk z2000-0080

Blad 20

De Registratiekamer stelt vast dat de conceptgedragscode en de concept-informatiebrochure voornamelijk uitleg geven over de procedure van het vastleggen van biometrische gegevens door exploitanten van horeca- en sportgelegenheden die deelnemen aan VIS 2000 en het plaatsen van dergelijke gegevens op een centrale zwarte lijst die wordt gebruikt om ongewenste bezoekers te kunnen weren.

Naar aanleiding van intern beraad binnen de Registratiekamer hebben wij u per brief van 12 december 2000 om aanvullende informatie verzocht. B heeft daarop schrijven gereageerd met haar brief van 28 december 2000 (uw referentie: 20006225/rv/da).

Vervolgens heeft de Registratiekamer u per brief van 31 januari 2001 haar aanbevelingen doen toekomen, en u in de gelegenheid gesteld daar op te reageren.

Naar aanleiding van de aanbevelingen in de brief van de Registratiekamer van 31 januari 2001 heeft uw cliënt een brief geschreven, gedateerd 21 februari 2001, waarin een reactie is geformuleerd op genoemde aanbevelingen. In de genoemde brief geeft uw cliënt aan zeer goed te kunnen leven met de bevindingen en conclusies van de Registratiekamer.

Datum 19 maart 2001

Ons kenmerk z2000-0080

Blad 21

Bijlage 2

- Uitgave van de Registratiekamer, 'Zwarte lijsten'
- Uitgave van de Registratiekamer, 'At face value'
- Uitgave van de Registratiekamer, 'In beeld gebracht'
- Uitgave van de Registratiekamer, 'Koning Klant'
- Uitgave van de Registratiekamer, 'Beveiliging van persoonsgegevens'
- Brief Registratiekamer aan Horeca Nederland