

CBP Richtsnoeren

IDENTIFICATIE EN VERIFICATIE VAN PERSOONSGEGEVENS

Gebruik van 'kopietje paspoort' in de private sector

...ming persoonsgegevens

van 6 juli 2000, houdende
bescherming van persoonsgegevens
bescherming persoonsgegevens

...rix, bij de gratie Gods, Koningin der Nederlanden

...e deze zullen zien of horen lezen, salu
...j in overweging genomen hebben, da
...opees Parlement en de Raad van de
...herming van natuurlijke personen in
...effende het vrije verkeer van die ge
...op artikel 10, tweede en derde lid, v
...het, dat Wij, de Raad van State
...en goedgevonden en verstaan, gel

Hoofdstuk I
Algemene bepalingen

Art. 1

...deze wet en de daarop berustende
...persoonsgegevens: elk gegeven
...persoon:

...verwerking van persoonsgegevens
...ing tot persoonsgegevens, w
...bijwerken, wijzigen,
...overreiding

INHOUD

Inleiding 2

1 Mag u iemand vragen om legitimatie? Ja, mits... 4

2 Is daarnaast een 'kopietje paspoort' toegestaan?

Nee, tenzij... 6

1 Wettelijke verplichting 7

2 Uitvoeren van een overeenkomst of contract 8

3 Bezit schept verplichtingen 10

1 Meldingsplicht 11

2 Informatieplicht 11

3 De kwaliteit van gegevens 11

4 Beveiliging 11

5 Bewaartermijnen en vernietiging van gegevens 11

4 Waarom het 'kopietje paspoort' alleen onder strikte voorwaarden is toegestaan 12

1 De pasfoto en het BSN 13

2 Toezicht en handhaving door het CBP 13

BIJLAGE 15

CBP Richtsnoeren

IDENTIFICATIE EN VERIFICATIE VAN PERSOONSGEGEVENS

Gebruik van 'kopietje paspoort' in de private sector

INLEIDING

Veel bedrijven en organisaties in de private sector willen de identiteit van bijvoorbeeld een klant of relatie kunnen vaststellen. Enerzijds omdat deze vaststelling nodig is om een besteld product te leveren of een verlangde dienst te kunnen verlenen. Anderzijds om zich tot op zekere hoogte te beschermen tegen bedrijfseconomische schade als gevolg van fraude en andere vormen van criminaliteit.

In toenemende mate vragen bedrijven en organisaties daarom aan burgers zich te legitimeren (ook wel: identificeren) met een officieel identiteitsdocument, zoals een paspoort of rijbewijs.¹ In aanvulling daarop wordt regelmatig ook om een ander, aanvullend identificerend document gevraagd, zoals een recent bankafschrift voor het uitvoeren van een adrescontrole. Naar hun aard, bevatten dergelijke documenten diverse persoonsgegevens. Het verzamelen en verder gebruiken van deze gegevens ('verwerken') is aan regels gebonden. Deze staan in de Wet bescherming persoonsgegevens (Wbp). Het College bescherming persoonsgegevens (CBP) houdt toezicht op de naleving van de Wbp.

Alertheid is geboden bij het toenemend kopiëren, scannen en uitlezen² van identiteitsdocumenten. Dit verschijnsel staat ook wel bekend als 'kopietje paspoort'. Het onnodig en bovenmatig kopiëren of scannen van deze documenten is niet zonder risico. Door op grote schaal persoonsgegevens te verzamelen neemt het risico van identiteitsfraude toe. Verkeerd gebruik kan ook leiden tot een inbreuk op de persoonlijke levenssfeer die in bestuursrechtelijke of civiele zin verwijtbaar is.

Deze richtsnoeren geven aan welke regels de wet stelt aan het overnemen van persoonsgegevens of het kopiëren, scannen of uitlezen van identiteitsdocumenten. Deze richtsnoeren dienen tevens als uitgangspunt voor het CBP bij het toepassen van handhavende maatregelen.

1 In artikel 1 van de Wet op de uitgebreide identificatieplicht (WUID) zijn het paspoort, de nationale identiteitskaart, het rijbewijs en het vreemdelingendocument aangewezen als officiële identiteitsdocumenten.

2 In 2004 oordeelde de Raad van State dat het uitlezen van een simkaart vergelijkbaar is met het kopiëren van papieren, documenten en bescheiden (ABRvS 6 mei 2004, nr. 200401455, JV 2004/263). De Belgische Commissie voor de bescherming van de persoonlijke levenssfeer beschouwt het uitlezen van een identiteitsdocument als een verwerking van persoonsgegevens die alleen mag plaatsvinden wanneer dat noodzakelijk is (Aanbeveling 03/2011 van 25 mei 2011).

1 MAG U IEMAND VRAGEN OM LEGITIMATIE? JA, MITS...

In het algemeen hebben medewerkers van bedrijven en organisaties geen wettelijke bevoegdheid om een persoon te verplichten zich te legitimeren. Ze kunnen iemand dus hooguit vragen om legitimatie. Dat maakt een gerechtvaardigde behoefte aan legitimatie er niet minder om, maar stelt daaraan wel voorwaarden.

Het vragen om legitimatie heeft alleen zin wanneer de medewerker de echtheid en geldigheid van het identiteitsdocument controleert. Wanneer een medewerker zonder deugdelijke controle een vals of vervalst document als 'bewijs' accepteert, neemt het risico op identiteitsfraude en andere vormen van criminaliteit juist toe. Een deugdelijke controle kan alleen plaatsvinden aan de hand van een origineel document, niet een kopie; daarop zijn beschadigingen of vervalsingen vaak niet meer te zien.

De echtheid van een identiteitsdocument kan de medewerker nagaan aan de hand van voelbare en zichtbare echtheidskenmerken die met dat doel op het document zijn aangebracht,³ zoals een voelbaar reliëf en een door perforatie aangebrachte tweede afbeelding van de gezichtsopname.⁴ Daarnaast is het van belang te letten op beschadigingen en wijzigingen. Deze kunnen wijzen op een vervalsing.

De geldigheid van een document is af te leiden van de geldigheidsdatum op het document. Ook is van belang te weten dat niet elk officieel identiteitsdocument in elke situatie een geldige legitimatie oplevert. Voor het vaststellen van de nationaliteit van een persoon is het rijbewijs bijvoorbeeld geen geldig identiteitsdocument, omdat deze informatie op het document ontbreekt.

Het onderzoeken en onderscheiden van echte en valse of vervalste identiteitsdocumenten vereist enige instructie van medewerkers die verantwoordelijk zijn voor de controle van getoonde identiteitsdocumenten. Bij twijfel over de echtheid of geldigheid van een identiteitsdocument dienen zij aanvullende legitimatie te vragen en zo nodig aangifte te doen bij de politie.

³ Voor een eenvoudige eerste controle van identiteitsdocumenten op echtheid en geldigheid zie de bijlage.

⁴ Meer informatie over echtheidskenmerken treft u aan op de website www.paspoortinformatie.nl van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

2 IS DAARNAAST EEN 'KOPIETJE PASPOORT' TOEGESTAAN? NEE, TENZIJ...

1 Wettelijke verplichting 7

2 Uitvoeren van een overeenkomst of contract 8

Als het laten tonen van een identiteitsdocument volstaat, zoals bij een leeftijdscontrole, is het overnemen van gegevens van het identiteitsdocument of het kopiëren, scannen of uitlezen ervan niet toegestaan.

Voorbeeld 1

Leeftijdscontroles voor (sterke) drank

De Drank- en Horecawet verbiedt horeca- en slijterijbedrijven om (sterke) drank te verkopen aan jongeren onder een bepaalde leeftijd. De ongeoorloofde verkoop van (sterke) drank is strafbaar gesteld, evenals de ongeoorloofde toegang tot of verkoop van films of games aan minderjarigen. Voor de naleving van de leeftijdsverificatie is het gerechtvaardigd dat bij twijfel over de leeftijd om een identiteitsdocument wordt gevraagd.⁵ Voor een controle op leeftijd kan worden volstaan met het tonen van een geldig identiteitsdocument. Het is niet noodzakelijk om persoonsgegevens te noteren of daarvan een kopie te maken. Leeftijdscontrole kan achterwege blijven als een klant of bezoeker evident ouder of jonger is dan de vereiste minimumleeftijd.

Soms is tonen niet voldoende, maar moeten bepaalde gegevens worden overgenomen, zoals voor een register van nachtverblijven (hotels).⁶ Ook daarvoor is het maken van een kopie of scan niet toegestaan. Dat betekent dat alleen in uitzonderlijke gevallen het maken van een kopie of scan is toegestaan.

Voorbeeld 2

Registratie van hotelgasten

Hotels en andere 'nachtverblijven' zijn op grond van het Wetboek van Strafrecht verplicht enkele gegevens van hun gasten te registreren aan de hand van een geldig identiteitsdocument.⁷ De verplicht te registreren gegevens betreffen het type identiteitsdocument, de naam van de gast, diens beroep of betrekking, zijn woonplaats en de dag van aankomst en vertrek. Deze gegevens moeten op aanvraag aan de politie kunnen worden getoond. Een kopie is daarvoor niet noodzakelijk.

Bij de vraag of persoonsgegevens van een identiteitsdocument mogen worden overgenomen, gekopieerd of gescand, is het volgende van belang:

Is het overnemen, kopiëren of scannen toegestaan?

Voor het verzamelen en gebruiken van persoonsgegevens, dus ook voor het overnemen, kopiëren of scannen, moet een juridische basis ('grondslag') bestaan. Voor het bedrijfsleven is dat in de meeste gevallen:⁸

1. een wettelijke verplichting nakomen;
2. een overeenkomst (ook wel: contract) uitvoeren.

2.1 Wettelijke verplichting

Het bestaan van een wettelijke verplichting is relevant in bijvoorbeeld arbeidsrelaties en in de financiële dienstverlening.

5 Niet-naleving van de gestelde leeftijdsgrenzen van artikel 20, vierde lid, Drank- en Horecawet is strafbaar gesteld in artikel 1, onder 4°, Wet op de economische delicten. De Nederlandse Voedsel- en Warenautoriteit houdt toezicht op de naleving van de leeftijdsgrens voor de verkoop van alcohol en tabak. Niet-naleving van de leeftijdsgrenzen bij films en games is strafbaar ingevolge artikel 240a Wetboek van Strafrecht. Het Commissariaat voor de Media houdt toezicht op het Nederlands Instituut voor de Classificatie van Audiovisuele Media (NICAM) op grond van de Mediawet.

6 Artikel 438 Wetboek van Strafrecht. Zie ook het advies van het CBP van 3 december 2007 (te raadplegen via www.cbprecht.nl/downloads_adv/z2007-01131.pdf), waarin het CBP aangeeft dat 'in Algemeen Plaatselijke Verordeningen (APV) weliswaar nadere registratieverplichtingen kunnen zijn vastgelegd, maar dat daarin geen verplichting kan worden opgenomen tot het maken van een kopie of scan door houders van nachtverblijven.'

7 Artikel 438 Wetboek van Strafrecht; vgl. bovengenoemd advies van het CBP.

8 Het betreft twee van de zes Wbp-grondslagen, te weten die in artikel 8 onder c en b Wbp.

Voorbeeld 3**Arbeidsrelaties**

Een werkgever is op grond van de Wet op de Loonbelasting verplicht om bij indiensttreding van een nieuwe werknemer diens identiteit te controleren aan de hand van een geldig identiteitsdocument – met uitzondering van een rijbewijs – en dit op echtheid te controleren (verificatieplicht).⁹ De identiteit mag niet aan de hand van een kopie van een identiteitsdocument worden gecontroleerd!¹⁰ Na deze controle is de werkgever verplicht om een kopie van het gecontroleerde document – inclusief burgerservicenummer (BSN) en pasfoto – in zijn loonadministratie op te nemen en te bewaren (bewaarplicht). Dit ontslaat de individuele werknemer echter niet van zijn toonplicht als er een arbeidsinspectie op de werkvloer plaatsvindt. De werkgever dient ervoor te zorgen dat alle werknemers een geldig identiteitsdocument kunnen tonen (zorgplicht), bijvoorbeeld door opbergkluisjes aan werknemers ter beschikking te stellen.¹¹

Voorbeeld 4**Identiteitscontrole bij financiële dienstverlening**

Sinds 1 augustus 2008 zijn de Wet identificatie bij (financiële) dienstverlening (Wid) en de Wet melding ongebruikelijke transacties (Wet MOT) samengevoegd in de Wet ter voorkoming van witwassen en financiering van terrorisme (WWFT).¹² De WWFT gaat uit van een 'risicogeorïenteerde' benadering: een financiële instelling moet zelf inschatten in hoeverre een financiële transactie risico's met zich meebrengt. Hoe groter dat risico, hoe meer onderzoek naar de (identiteit van de) cliënt wordt vereist.¹³ De financiële instelling kan – als bewijs van de identificatieverplichting (reconstructieplicht) – daarbij ook een afschrift (lees: kopie) van het gecontroleerde identiteitsdocument vastleggen en gedurende vijf jaar bewaren.¹⁴

2.2 Uitvoeren van een overeenkomst of contract

Voor de uitvoering van een overeenkomst zal bij het opstellen van een contract vaak om adresgegevens worden gevraagd, bijvoorbeeld voor de aflevering van een bestelling. In een online situatie is bovendien een e-mailadres vereist.¹⁵ Een geboortedatum is voor een bestelling meestal niet nodig, tenzij een product bijvoorbeeld niet voor minderjarigen is bedoeld.

Voor de uitvoering van bijvoorbeeld een abonnement of lidmaatschap zijn vaak betalingsgegevens nodig. De grondslag voor het verwerken van persoonsgegevens beperkt zich in deze gevallen tot het overnemen van de meest relevante gegevens. Een 'kopietje paspoort' is in geen van deze gevallen nodig en mag niet worden gevraagd.

Voorbeeld 5**Lidmaatschap van een (sport)vereniging**

Een praktijksituatie: een nieuw lid van een sportschool wordt bij zijn inschrijving gevraagd om verschillende persoonsgegevens, zoals zijn NAW-gegevens en betalingsgegevens om het lidmaatschapsgeld automatisch te kunnen afschrijven. In aanvulling wil de baliemedewerker ook een geldig identiteitsdocument van het nieuwe lid scannen. Desgevraagd geeft de medewerker aan dat dit een voorwaarde is om lid te kunnen worden. Dit is echter geen toelaatbare voorwaarde, omdat met het scannen van een identiteitsdocument ook het BSN wordt verwerkt. Dat is zonder wettelijke grondslag verboden en overigens ook niet noodzakelijk om lid te worden.

Leveranciers of verkopers staat het in beginsel vrij om aan hun dienst of product voorwaarden te verbinden. Voordat een overeenkomst wordt aangegaan – zeker als het kostbare producten betreft, langer lopende abonnementen of een koop op afstand – zal een ondernemer (meer) zekerheid willen hebben over met wie hij zaken doet om (toekomstige) betalingen veilig te stellen. Daarvoor kan de ondernemer aanvullende informatie verlangen of voorwaarden stellen om bijvoorbeeld fraude te voorkomen of snel te laten opsporen. Dat betekent overigens niet dat het kopiëren of scannen van identiteitsdocumenten zomaar als voorwaarde gesteld kan worden.

9 Artikel 6a, onder c, Wet op de Loonbelasting. Artikel 15, eerste lid, Wet arbeid vreemdelingen (WAV) kent eenzelfde verifieer- en bewaarverplichting.

10 Vgl. www.belastingdienst.nl/zakelijk/loonheffingen/lb22_gegevens_administreren/lb22_gegevens_administreren-08.html.

11 Artikel 55, tweede en derde lid, Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI).

12 De samenvoeging van de Wid en de Wet MOT in de WWFT is een gevolg van de implementatie van Richtlijn 2005/60/EG, ook wel de 'derde Europese witwasrichtlijn' genoemd.

13 De naleving van de WWFT wordt onder meer gecontroleerd door het Bureau Financieel Toezicht (BFT); www.bureaufn.nl.

14 Artikel 33, eerste lid, onder a, sub 1°, WWFT. Vgl. Kamerstukken II 2007-2008, 31 238, nr. 3, p. 35.

15 Een webshop is wettelijk verplicht een online aankoop per e-mail te bevestigen (artikel 6:227c Burgerlijk Wetboek).

Voorbeeld 6***Kopiëren van identiteitsdocumenten door telecom- en internetbedrijven***

Om enige zekerheid te hebben over de betaling van abonnementsgelden, kan een telecoomaanbieder een kredietwaardigheidsonderzoek doen naar een potentiële nieuwe klant. Daarvoor heeft de ondernemer enkele persoonsgegevens nodig – zoals NAW-gegevens en de leeftijd van de klant in geval van een minderjarige – en kan hij de klant vragen om een geldig identiteitsdocument te tonen om diens identiteit deugdelijk vast te stellen. Zo nodig kan de ondernemer de aard van het identiteitsdocument en het documentnummer noteren. Het maken van een kopie of scan van zo'n document is echter niet toegestaan; het BSN mag niet door een telecoomaanbieder worden verwerkt en ook de pasfoto en andere gegevens op het document zijn voor zo'n kredietwaardigheidsonderzoek niet noodzakelijk. In plaats van een kredietwaardigheidsonderzoek wordt ook wel de bankpas gecontroleerd en gevraagd om € 0.01 te pinnen om aan te tonen dat de betaalrekening van de nieuwe klant actief is. Het kopiëren of scannen van de bankpas is niet noodzakelijk; door de betaling beschikt de ondernemer immers al over de nodige betaalgegevens, zoals het rekeningnummer en de tenaamstelling van de betaalrekening.

In zeer uitzonderlijke gevallen kan sprake zijn van het overnemen van gegevens van een identiteitsdocument of het kopiëren of scannen ervan. Een bedrijf of organisatie moet de noodzaak daartoe dan wel gedocumenteerd kunnen onderbouwen. In de praktijk zal een dergelijke situatie zich niet vaak voordoen, omdat bij een behoefte aan legitimatie het tonen van een identiteitsdocument in beginsel voldoende is.

Voorbeeld 7***Kopiëren van identiteitsdocumenten bij het huren of tijdelijk meenemen van een auto***

Voertuigenverhuurbedrijven die lid zijn van brancheorganisatie BOVAG kunnen bij de verhuur van een auto of voorafgaand aan een proefrit kopieën van identiteitsdocumenten maken. Voertuigenverhuurders worden regelmatig geconfronteerd met onwenselijke (criminele) gedragingen van huurders van onder meer auto's en motoren. Om deze voertuigcriminaliteit tegen te gaan, heeft BOVAG de bestaande zwarte lijst van de brancheorganisatie – ELENA Waarschuwingssysteem – uitgebreid met de mogelijkheid een kopie van de identiteitspapieren van de huurder te maken. Deze uitbreiding is opgenomen met als doel verbetering van het opsporen en vervolgen van verduistering van huurauto's. Binnen de Stichting Aanpak Voertuigcriminaliteit zijn hierover tussen de deelnemers – waaronder BOVAG en het Openbaar Ministerie – afspraken gemaakt. Deze afspraken zijn neergelegd in een circulaire van 11 februari 2009, die is vastgesteld in de Board Opsporing van de Raad van Hoofdcommissarissen. Het CBP heeft na een voorafgaand onderzoek op 16 januari 2011 verklaard de door BOVAG gemelde verwerking van persoonsgegevens rechtmatig te achten. Voordat voertuigenverhuurders overgaan tot het maken van een kopie van een identiteitsdocument, dient een belangenafweging plaats te vinden of de kopie noodzakelijk is. Indien dit het geval is, dient het BSN te worden afgeschermd. Dat geldt ook voor de pasfoto, tenzij de huurder of proefritmaker uitdrukkelijke toestemming geeft voor het maken van een kopie zonder afscherming van de foto. Het bedrijf treft passende technische en organisatorische maatregelen voor het beveiligen van gemaakte kopieën. Zodra de huurder of proefritmaker het voertuig veilig retourneert, worden de kopieën teruggegeven of vernietigd.

3 BEZIT SCHEPT VERPLICHTINGEN

- 1 Meldingsplicht *11*
- 2 Informatieplicht ten opzichte van consumenten, medewerkers e.d. *11*
- 3 De kwaliteit van gegevens *11*
- 4 Beveiliging *11*
- 5 Bewaartermijnen en vernietiging van gegevens *11*

Het verzamelen en gebruiken van persoonsgegevens is aan strenge wettelijke regels gebonden en leidt tot een reeks verplichtingen voor een bedrijf of organisatie. Dit zijn de meldingsplicht, de informatieplicht, de kwaliteitsbewaking van gegevens, de beveiligingsplicht en gemaximeerde bewaartermijnen en vernietiging van persoonsgegevens.¹⁶ Deze verplichtingen worden hierna toegelicht:

3.1 Meldingsplicht

Als het verzamelen van persoonsgegevens verder gaat dan het aanleggen van bijvoorbeeld een klanten- of ledenbestand, dan verplicht de Wbp tot het melden van die gegevensverzameling bij het CBP of de functionaris voor de gegevensbescherming. In het Vrijstellingsbesluit Wbp staan de verwerkingen van persoonsgegevens vermeld die zijn vrijgesteld van melding.¹⁷ Het maken en verzamelen van 'kopietjes paspoort' is niet vrijgesteld van melding.

3.2 Informatieplicht

Bedrijven en organisaties moeten personen van wie zij persoonsgegevens verzamelen ('betrokkenen' genoemd) adequaat informeren over het doel en de toelaatbaarheid daarvan. Dat betekent dat een bedrijf of organisatie ook informatie verstrekt aan betrokkenen over de rechten die zij kunnen uitoefenen aangaande het verzamelen van hun persoonsgegevens, zoals het recht op inzage, correctie en verzet. Met het verwijzen naar een 'standaardprocedure' of 'het hoofdkantoor' wordt niet aan de informatieplicht voldaan. Deze informatieplicht biedt klanten, medewerkers e.d. de gelegenheid om na te gaan of het bedrijf of de organisatie de gewenste persoonsgegevens mag verzamelen en om te besluiten om daar wel of niet aan mee te werken.

3.3 De kwaliteit van gegevens

Bedrijven en organisaties moeten persoonsgegevens aan de hand van een origineel identiteitsdocument op echtheid en geldigheid controleren, zodat zij de gegevens juist en nauwkeurig vastleggen. Het doel daarvan is om fouten, misverstanden en misbruik – zoals identiteitsfraude – te voorkomen. Ook mogen zij niet meer persoonsgegevens verzamelen en gebruiken dan nodig voor het doel waarvoor deze worden verzameld.

3.4 Beveiliging

Bedrijven en organisaties moeten verzamelde persoonsgegevens organisatorisch en technisch beveiligen tegen verlies, diefstal en ander onrechtmatig gebruik, zoals identiteitsfraude. Dat betekent dat niet iedereen in de organisatie of het bedrijf toegang mag hebben tot de gegevens. Voorkomen moet worden dat gegevens toegankelijk zijn voor onbevoegden ('datalek').

3.5 Bewaartermijnen en vernietiging van gegevens

Bedrijven en organisaties mogen persoonsgegevens niet langer bewaren dan noodzakelijk is of wettelijk verplicht. Daarna moeten de gegevens worden vernietigd, zodat zij niet later hergebruikt kunnen worden.

¹⁶ Het betreft resp. de artikelen 27, 33 en 35-40, 11, 13 en 10 Wbp.

¹⁷ Te vinden via: www.wetten.nl.

4 WAAROM HET 'KOPIETJE PASPOORT' ALLEEN ONDER STRIKTE VOORWAARDEN IS TOEGESTAAN

- 1 De pasfoto en het BSN *13*
- 2 Toezicht en handhaving door het CBP *13*

4.1 De pasfoto en het BSN

De Wbp kent een aantal categorieën persoonsgegevens die in beginsel niet mogen worden verwerkt. Daarvan een kopie of scan maken is dus eveneens verboden. Deze zogeheten bijzondere persoonsgegevens zeggen onder meer iets over ras, gezondheid of geloofsovertuiging of betreffen strafrechtelijke gegevens. Het zijn gevoelige persoonsgegevens die extra risico's met zich meebrengen, zoals discriminatie of uitsluiting van de betreffende persoon voor een bepaalde dienst of product.

Bij een verzoek om legitimatie en eventueel een 'kopietje paspoort' is met name het begrip 'ras' van belang. Dit begrip moet ruim worden uitgelegd en omvat zowel iemands nationaliteit als kenmerken waaruit zijn of haar etnische afkomst kan worden afgeleid, zoals bij een pasfoto.¹⁸ Daarom mag een pasfoto niet zomaar worden gekopieerd. De Wbp bevat een (limitatief) aantal uitzonderingen op het verbod op het gebruik van deze gegevens, waaronder het gebruik van een pasfoto als dat voor de identificatie van een persoon onvermijdelijk is.¹⁹ Als voorbeeld dient het gebruik van een pasfoto op een toegangspas van een groot concern. In overige gevallen is het gebruik verboden.

Een andere categorie 'verboden' persoonsgegevens is die van de persoonsidentificerende nummers, in het bijzonder het burgerservicenummer (BSN). Het risico van een grootschalig gebruik van het BSN is dat daarmee eenvoudig bestandskoppelingen kunnen worden uitgevoerd, veelal buiten het zicht van de betreffende persoon. Dit nummer mag daarom niet worden verzameld en gebruikt zonder dat daarvoor een wettelijke verplichting of andere wettelijke basis bestaat.²⁰ Behalve voor de loonadministratie zal deze voor bedrijven of organisaties over het algemeen niet bestaan.

Bij het vragen om een legitimatie moeten bedrijven en organisaties in de private sector zich houden aan het verbod op het verzamelen en gebruiken van rasgegevens en nummers als een BSN. Als geen uitzondering bestaat op het verbod op het verzamelen van deze gegevens, moeten deze bij het maken van een kopie of scan altijd worden afgeschermd of onleesbaar worden gemaakt.

4.2 Toezicht en handhaving door het CBP

Het CBP ziet toe op de naleving van de Wbp en kan bij overtredingen van de wet handhavende maatregelen treffen.²¹ Dat kan onder meer inhouden dat het CBP een bedrijf een last onder dwangsom oplegt om naleving van de wet af te dwingen.

Het CBP geeft in zijn handhavingsbeleid prioriteit aan onderzoeken naar ernstige en structurele overtredingen van de Wbp, die veel mensen treffen en waarbij het CBP door de inzet van handhavende maatregelen een effectief verschil kan maken. Daarnaast stelt het CBP jaarlijks aandachtsgebieden vast waarop verscherpt toezicht plaatsvindt. Daarbij zal ook aandacht zijn voor signalen van burgers over het onrechtmatig verzamelen en gebruiken van 'kopietjes paspoort'.

18 De Hoge Raad heeft die uitleg op 23 maart 2010 bevestigd (LJN: BK6331, te lezen via www.rechtspraak.nl).

19 Artikel 18 Wbp.

20 Op www.burgerservicenummer.nl wordt aangegeven welke instanties een BSN mogen verzamelen en gebruiken.

21 Voor meer informatie wordt verwezen naar de Beleidsregels handhaving door het CBP van 17 januari 2011 (Staatscourant 2011, nr. 1916); te raadplegen via www.wetten.nl.

BIJLAGE: IDENTITEITSDOCUMENTEN EN -KENMERKEN OP ECHTHEID CONTROLEREN

Verificatie van identiteitsdocumenten

Om er als verantwoordelijke²² zeker van te zijn dat u te maken heeft met een echt identiteitsdocument, moet u het op geldigheid en echtheid controleren. Dat kan aan de hand van enkele eenvoudige stappen:

1 Geldigheid

Op ieder identiteitsdocument is de geldigheidsduur ervan vermeld. Identiteitsdocumenten kennen op dit moment een geldigheidsduur van één jaar (vreemdelingendocument), vijf jaar (paspoort, identiteitskaart of vreemdelingendocument) of tien jaar (rijbewijs).

- Controleer of de geldigheidsduur niet is verstreken of de duur opvallend afwijkt van de genoemde termijnen.

NB: Een rijbewijs bevat geen informatie over de nationaliteit of verblijfstatus van een persoon en is daarom niet in alle gevallen een geldige wijze van identificatie, zoals bij de Belastingdienst, bij de aanvraag van een uitkering, bij indiensttreding bij een nieuwe werkgever en voor het toezicht op rechtmatig verblijf van vreemdelingen. In deze situaties is het tonen van een ander identiteitsdocument noodzakelijk.

2 Echtheid

Identiteitsdocumenten kennen diverse zichtbare én onzichtbare echtheidskenmerken om vervalsing tegen te gaan. Indien het identiteitsdocument voldoet aan onderstaande waarneembare echtheidskenmerken, heeft u vrijwel zeker te maken met een echt identiteitsdocument. Verschillende van deze echtheidskenmerken zijn eenvoudig zelf te controleren:

- Controleer allereerst of de foto op het document overeenkomt met de persoon die voor u staat.
- Naast de foto moet ook een tweede (identieke) weergave van de foto zichtbaar zijn, bestaande uit een geperforeerde afdruk (ook wel: ImagePerf). Deze wordt zichtbaar als u het document tegen het licht houdt. Onder in de foto staat in hoofdletters de nationaliteitsaanduiding (bijvoorbeeld: NLD).
- Het identiteitsdocument bevat bij de pasfoto een kinegram dat van kleur en vorm verandert wanneer u het document kantelt.
- Alle identiteitsdocumenten kennen verder een voelbaar reliëf, zowel bij de ImagePerf als aan de linker- en rechterzijde van het document of – bij vreemdelingendocumenten – aan de onderzijde van het document.
- Paspoorten, identiteitskaarten en vreemdelingendocumenten hebben onderaan twee of drie regels letters en cijfers, de zogeheten Machine Readable Zone (MRZ), waarin enkele gegevens van de kaart worden herhaald. Deze gegevens dienen identiek te zijn aan de gegevens op de kaart zelf. Via de MRZ kan worden gecontroleerd of een op zich geldig en echt identiteitsdocument is vervalst met andere gegevens.
- Een identiteitsdocument maakt een ‘metaalachtig’ geluid als het op een harde ondergrond (bv. tafel) valt.

3 Het BSN en de ‘elfproef’

Iedere rechtmatig in Nederland verblijvende persoon ontvangt van de Belastingdienst een burgerservicenummer (BSN). Het BSN is een informatieloze cijfercombinatie waaruit geen persoonsgegevens – zoals een geboortedatum – af te leiden zijn. Desondanks kan ook een BSN op echtheid worden gecontroleerd, met de zogenoemde elfproef. Dit is een test die in het Nederlandse elektronische betalingsverkeer wordt uitgevoerd op negen- en tiencijferige Nederlandse bankrekeningnummers, om te controleren of het nummer een geldig rekeningnummer kan zijn.

Een variant van de elfproef die gebruikmaakt van een controlecijfer, wordt toegepast bij het BSN. Bij de BSN-elfproef worden de afzonderlijke negen cijfers van een BSN ‘gewogen’ bij elkaar opgeteld, dat wil zeggen dat afhankelijk van de positie in de cijferreeks het cijfer met een vaste waarde wordt vermenigvuldigd en het laatste cijfer (het ‘controlecijfer’) – in afwijking van de standaard-elfproef – wordt vermenigvuldigd met het cijfer -1. Het resultaat van de som moet een getal opleveren dat deelbaar is door het getal 11. Als een of meerdere cijfers van een geldig BSN worden verwisseld, levert dit geen geldig BSN (meer) op.

De BSN-elfproef met BSN 123456782: $(9 \times 1) + (8 \times 2) + (7 \times 3) + (6 \times 4) + (5 \times 5) + (4 \times 6) + (3 \times 7) + (2 \times 8) + (-1 \times 2) = 154 : 11 = 14$.

²² Het begrip ‘verantwoordelijke’ doelt op degene die formeel-juridisch de zeggenschap over de verwerking heeft. Het gaat om degene die bevoegd is het doel van en de middelen voor de verwerking van persoonsgegevens vast te stellen.

DISCLAIMER: Deze bijlage bevat indicatieve informatie en beoogt geen volledig en actueel overzicht te geven van de echtheidskenmerken van de besproken identiteitsdocumenten, noch een uniforme werkwijze voor te schrijven voor de controle ervan. Kijk voor meer informatie daarover op de website van de Basisadministratie Persoonsgegevens en Reisdocumenten (BPR) van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties: www.bprbzk.nl of neem contact op met BPR voor specifieke vragen.

**Identificatie en verificatie
van persoonsgegevens**

College bescherming persoonsgegevens,
Den Haag, juli 2012.

© Niets uit deze uitgave mag worden veele-
voudigd en/of openbaar gemaakt door middel
van druk, fotokopie, microfilm of op welke wijze
dan ook, zonder voorafgaande schriftelijke
toestemming van het College bescherming
persoonsgegevens.

Het College bescherming persoonsgegevens houdt onder de Wet bescherming persoonsgegevens toezicht op de naleving van wetten die het gebruik van persoonsgegevens regelen. Onduidelijkheid over wet- en regelgeving kan ten koste gaan van de bescherming van de gegevens van burgers. Daarom geeft het College in zijn Richtsnoeren ten behoeve van toepassing in de praktijk nadere invulling aan de geldende wettelijke normen.

Rechterlijke uitspraken kunnen naast wetwijzigingen, technische ontwikkelingen en praktijkervaringen aanleiding geven tot aanvulling of herziening van deze richtsnoeren. Deze richtsnoeren treden in werking met ingang van 12 juli 2012, zijnde de datum van publicatie in de Staatscourant.



Postbus 93374
2509 AJ Den Haag

www.cbpweb.nl
www.mijnprivacy.nl

