

College Bescherming Persoonsgegevens
Juliana van Stolberglaan 4-10
2595 CL DEN HAAG

31 mei 2012

Betreft: officiële melding tot onderzoek en verzoek tot instelling van sancties m.b.t. afname en opslag van biometrische persoonsgegevens uit hoofde van de Paspoortwet

Zeer geacht College,

Hiermee wend ik mij, mede namens cliënten, tot u met het oog op de bescherming van de persoonlijke levenssfeer gezien de afname en opslag van een of meer vingerafdrukken en een digitale gezichtsscan (alle zijnde zeer gevoelige persoonsgegevens) ten behoeve van Nederlandse reisdocumenten.

Ik wend mij tot u gezien uw uitdrukkelijk geformuleerde taakopdracht en bevoegdheden uit hoofde van Nederlandse wetgeving (waaronder de WBP), het EU-recht, het EVRM met protocollen, het Dataprotectieverdrag (van Straatsburg) 1981 en bijbehorend protocol 2001.

(zie: <http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm>)

Door deze melding bent u - op grond van artikel 60 WBP en art. 1 Protocol 2001 bij het Dataprotectie-verdrag van Straatsburg – verplicht een officieel onderzoek in te stellen naar de (rechtmatigheid van de) huidige verwerking van bedoelde biometrische persoonsgegevens uit hoofde van de Paspoortwet/cq – uitvoeringsregeling(en) en EU-Verordeningen 2252/2004 en 444/2009. En met name naar de verenigbaarheid hiervan met andere wet- en regelgeving en verdragen, in het bijzonder de WBP, het EVRM, het Dataprotectieverdrag 1981, de EU Privacy-richtlijn en het Handvest van de EU-Grondrechten.

Met name verzoek ik u aan te geven of en, zo ja, hoe de huidige biometrie-afname voldoet aan:

a) EU-verordening 2252/2004

Art. 1 lid 3

3. Deze verordening is van toepassing op door de lidstaten afgegeven paspoorten en reisdocumenten. [Zij is niet van toepassing op door de lidstaten aan hun onderdanen afgegeven identiteitskaarten](#) of op tijdelijke paspoorten en reisdocumenten die een geldigheidsduur van 12 maanden of minder hebben.

b) EU-verordening 444/2009

Art. 1 lid 2

2. Deze paspoorten en reisdocumenten bevatten een opslagmedium dat aan de hoogste veiligheidseisen voldoet en een gezichtsofname bevat. De lidstaten nemen ook twee platte vingerafdrukken in een interoperabel formaat op. De gegevens worden beveiligd en het opslagmedium heeft voldoende capaciteit en [is voldoende geschikt om de integriteit, de authenticiteit en de vertrouwelijkheid van de gegevens te garanderen](#).

c) Dataprotectieverdrag 1981

<http://conventions.coe.int/treaty/en/treaties/html/108.htm>

Article 5 – Quality of data

Personal data undergoing automatic processing shall be:

- a. obtained and processed fairly and lawfully;
- b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
- c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
- d. accurate and, where necessary, kept up to date;
- e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6 – Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

d) Het EVRM, artt. 3, 5, 6, 8, 13 en 14.

In het bijzonder verzoek ik u bij uw onderzoek te betrekken:

- 1) de brief van de Burgemeester van Roermond uit november 2009, m.b.t. een uitgevoerde test met als resultaat foutmarges van ruim 21% bij verificatie van vingerafdrukken bij uitgifte van reisdocumenten. Vergelijkbare foutmarges (tot zelfs 25%) zijn door de Minister van BiZa tijdens het Commissie-overleg BiZa d.d. 27 april 2011 reeds erkend;
- 2) de Kamerbrief van 26 april 2011 m.b.t. de huidige stand van de techniek rond biometrie en overwegingen t.a.v. de status van de identiteitskaart;
- 3) het onderzoeksrapport Bekker uit 2012 n.a.v. de hoorzitting in de Tweede Kamer van voorjaar 2011, die beide de voorzienbaarheid en toegankelijkheid van de wettelijke regeling ernstig ondergraven;
- 4) de Kamerbrief van 12 april 2012 waarin geen gerechtvaardigde reden voor afname van vingerafdrukken en gezichtsscan wordt aangevoerd.
- 5) het AO in de Tweede Kamer van 22 mei 2012, <http://t.co/3YNHpsAb> waarin is bevestigd dat om diverse redenen de doelen van de Paspoortwet niet (langer) kunnen worden behaald met behulp van biometrie, c.q. dit middel buiten proportie is;
- 6) het antwoord van B&W Nijmegen in 2011 en B&W Groningen in mei 2012 op raadvragen, dat afname van vingerafdrukken ineffectief is: [#5](http://bit.ly/L7IDCy) En dus onnodig is.

Dringend verzoek ik u te onderzoeken of:

- 1) Onnodig en onrechtmatig 4 in plaats van 2 vingerafdrukken worden afgenomen (waarna 2 scans zogenaamd 'onraadpleegbaar' worden gemaakt). Volgens uitspraak van het Franse Conseil d'Etat op 26 oktober 2011 dient deze praktijk onmiddellijk te stoppen;
- 2) Het opslagmedium **voldoende geschikt is om de integriteit, de authenticiteit en de vertrouwelijkheid van de gegevens te garanderen**, zoals vereist in art. 1 lid 2 EU-verordening.
Niet alleen databank- maar ook chip-opslag en afname van de vingerafdruk(ken) in ID-kaarten en paspoorten dient o.i. daarom onmiddellijk beëindigd te worden, aangezien uit de stand der techniek is gebleken dat dit middel niet effectief is in de zin van de WBP en art. 8 EVRM en de doelstellingen genoemd in de Memories van de Paspoortwet hiermee niet (langer) kunnen worden behaald;
- 3) De vereiste proportionaliteit van de bedoelde biometrie-afname ontbreekt, aangezien de lage cijfers van look-a-like-fraude (aangetoond door Wob-verzoek 2012 van Privacy First) deze niet wettigt.
Conform EHRM 'Marper e.a. vs VK' en 'Van der Velden vs Nederland' dient ook de angst voor toekomstig gebruik/misbruik mee te wegen bij de beoordeling van de rechtmatigheid van een privacy-inbreuk. Met de afname van vingerafdrukken wordt de infrastructuur voor een politiestaat geschapen, die op fundamentele gronden niet noodzakelijk kán zijn in een democratische samenleving;

4) Afname van een digitale gezichtsscan in combinatie met cameratoezicht en het op afstand uitlezen van persoonsgegevens het (o.i. ongewenste) einde zou betekenen van de anonimiteit in het openbaar. Hiermee wordt de infrastructuur voor een politiestaat verder verfijnd. Daarom achten wij ook de afname en opslag van deze biometrie-vorm onverenigbaar met een democratische samenleving.

5) EU-verordening 2252/2004 niet op ID-kaarten van toepassing is, zoals bepaald in art. 1 lid 3 EU-verordening, en derhalve met onmiddellijke ingang ID-kaarten dienen te worden verstrekt zonder vingerafdrukken. Het aanmerken van de ID-kaart als reisdocument (in tegenspraak met recente uitspraak van de Hoge Raad in de zaak rond de ID-leges) onmiddellijk dient te worden beëindigd;

Bij een zorgvuldige vervulling van de aan u toegewezen belangrijke toezichttaak op de HUIDIGE biometrie-afname bent u verplicht deze op korte termijn diepgaand te onderzoeken. En deze afname zo nodig spoedig te beëindigen, onder instelling van passende sancties.

Een dergelijk onderzoek is zeer opportuun (er is immers geen aanleiding tot onbevoegdheid/verhinderend van het College) en achten wij, ook gezien de maatschappelijke impact, dringend noodzakelijk.

Aangezien cliënten hun grondwettelijk recht tot reizen (en terugkeren) binnen en buiten Schengen-landen onverminderd willen uitoefenen en bovendien snel hun baan dreigen te verliezen zonder geldig paspoort, hebben zij direct belang bij uw onderzoek naar een 'Light'-versie van paspoort en ID-kaart, zonder afname en opslag van genoemde biometrische gegevens.

Graag zie ik uw - uitgebreid gemotiveerde - antwoord ook zo spoedig mogelijk tegemoet in verband met het spoedeisende karakter van de naderende aanvraag van reisdocumenten door cliënten.

Een kopie van deze melding zend ik heden aan Bits of Freedom, Burgerrechtenvereniging Vrijbit, Dep. SecGen Council of Europe, DeVrijePsych, EFF, EDPS, Europees Parlement, Europese Commissie, Humanistisch Verbond, NJCM, NO2ID, Ouders Online, Platform Bescherming Burgerrechten, Privacy First, Privacy International, Statewatch, Stichting KDVP, Stichting Meldpunt Misbruik ID-plicht en de Vaste Kamercommissie BZK.

Met dank bij voorbaat,
hoogachtend,