Biometrics from a legal perspective

dr. Ronald Leenes
outline

• introduction
  • biometrics, use
• legal aspects
  • privacy/data protection
• biometrics as a privacy safeguard
• PRIVIUM
• discussion
biometrics

- biometric indicator:
  any human
  physiological or behavioural feature
  that can be measured and
  used for the purpose of
  automated or semi-automated
  verification or identification
biometrics

- physiological
  - height, weight, face
  - iris, retina, fingerprint, facial image, ear geometry, …
- behavioural
  - voice, signature, gait, keystroke sequence, …
- DNA?
  - not externally observable
biometric uses

- verification
  - are you who you claim to be?
  - one-to-one
  - centralised, decentralised

- identification
  - who are you?
  - one-to-many
  - central database
secondary use

- screening
- are you on my watch list?
- one-to-many
- resembles identification
<table>
<thead>
<tr>
<th></th>
<th><strong>private sector</strong></th>
<th><strong>public sector</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>fingerprint</strong></td>
<td>notebooks</td>
<td>Eurodac</td>
</tr>
<tr>
<td></td>
<td>Axsionics card</td>
<td>NY State</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ontario</td>
</tr>
<tr>
<td><strong>facial recognition</strong></td>
<td>German banks</td>
<td>Super Bowl XXXV</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EU passports</td>
</tr>
<tr>
<td><strong>iris</strong></td>
<td>PRIVIUM</td>
<td>PRIVIUM</td>
</tr>
</tbody>
</table>
legal requirements?
regulation

- little specific legislation on biometrics
- private sector:
  - consent based
- public sector:
  - mainly law enforcement
    - DNA, fingerprints
  - when obligatory > new legislation
    - e.g. passports
    - Ontario social security case
general frameworks

- European Convention on Human Rights
- ECHR
- Directive 95/46/EC on protection of individuals with regard to the processing of personal data and on the free movement of such data
- EU Data Protection Directive
legal aspects

- human rights
  - physical integrity

- privacy & data protection
  - biometrics as a threat
  - biometrics as a solution
biometrics: a privacy threat?
biometrics as a privacy threat

- what do biometrics reveal?
  - facial image
    - source:
      - race, gender, age …
    - template:
      - ?
biometrics as a privacy threat

- what do biometrics reveal?
  - fingerprints
  - source:
    - Down syndrome, Turner syndrome, Klinefelter syndrome
    - intestinal pseudo-obstruction, breast cancer, Rubella syndrome
    - homo-sexuality
  - template:
    - unlikely to reveal the above?

source

http://mehr.sharif.edu/~ipl/FingerprintIdentification.htm

reported in: Hornung 2004
IRIS

source:
- diabetes, arteriosclerosis, hypertension
- HIV
- misuse of alcohol and drugs
- race?

template
- ?

reported in: Hornung 2004
do we need regulation?
privacy issues

- raw biometric data may reveal sensitive data
- biometrics are irrevocable
- identification requires central data storage
- some biometric data can be collected without the subject being aware
broader concerns

- power accumulation
- further use of existing data
  - e.g. biometric passport
- do biometrics make the world safer?
- biometrics may lower privacy awareness
  - trade fingerprints for faster burgers
hence, careful consideration:
- when and why to allow biometrics
- proper safeguards against misuse
- and requirements for use
  - e.g. encrypted storage and transfer
privacy - The right to be left alone

- art. 8 (1) ECHR:
  Everyone has the right to respect for his private and family life, his home and his correspondence.

- dimensions
  - spatial
  - physical
  - relational
  - informational
article 8 (2) ECHR

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
95/46/EC
EU data protection directive
regulating personal data usage

- 95/46/EC - EU Data Protection Directive defines rights and obligations with respect to processing of personal data
art. 2 a: personal data

any information relating to an identified or identifiable natural person;

an identifiable person is

one who can be identified, directly or indirectly, in particular by reference to an identification number or

to one or more factors specific to his physical, physiological, mental (...) identity.
is biometric data personal data?

- raw data - yes
- template - yes, unless:
  - stored in a way that no reasonable means exist to identify data subject by
    - data controller or
    - any other person
95/46/EC - data protection directive

- concepts
  - personal data
  - principle of purpose
  - principle of proportionality
  - fair collection
  - legitimate processing
  - security measures
  - sensitive data
  - prior checking - notification
<table>
<thead>
<tr>
<th>purpose and proportionality</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>purpose/ finality</strong></td>
</tr>
<tr>
<td>art. 6 (b)</td>
</tr>
<tr>
<td>personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes</td>
</tr>
<tr>
<td><strong>proportionality</strong></td>
</tr>
<tr>
<td>personal data must be adequate, relevant and not excessive in relation to purpose</td>
</tr>
</tbody>
</table>
• test: can purpose be achieved in less obtrusive way?
  
e.g. CNIL case - fingerprints excessive for school restaurant, hand shape is ok

• privacy preference:
  • biometrics without leaving traces
  • decentralised storage
art. 6 (a) personal data must be processed fairly and lawfully

data subject must be informed of:

- purpose, identity of controller, further recipients of the data, whether reply is obligatory or voluntary, existence of access right to information

exception: national security, defence...
art. 7

data may be processed only if

- consent
- necessary for performance of a contract
- necessary for compliance with legal obligation
- protect vital interest of data subject
- performance of task in public interest
- legitimate interest of controller
security measures

art. 17

appropriate security measures must be taken to protect personal data against

unlawful destruction or accidental loss, alteration, unauthorized disclosure or access

especially where processing involves networks
security measures

- risks:
  - enrolment
  - data transmission
  - raw data
  - reversible templates
  - profiling/monitoring
  - id theft
  - indisputable evidence
article 8 (1)

Member states shall prohibit the processing of personal data revealing racial or ethnic origin,

political opinions, religious or philosophical beliefs, trade-union membership, and …

data concerning health or sex life

unless (2)

…
sensitive data

art. 8 (2)

consent

obligations and right of controller (employment)

vital interest of data subject (accident)

organization members

...

suitable safeguards
key points so far

- biometrics are compatible with 95/46/EC
- consider proportionality
- define purpose
- decentralized storage
- consent of data subject
- irreversible templates
- proper security measures
biometrics as a privacy safeguard
biometrics as privacy safeguard

- **identification** is privacy risk

- **verification** + credentials = privacy safeguard
  - smart card for 18+
  - biometrics to verify requirement

- allows biometrics to be under constant control of data subject
cases: PRIVIUM

- Schiphol Airport Group
- priority services card
  - convenient parking
  - speed check in
  - fast track border passage
- card contains
  - card number, iris template, name, date and place of birth
• border passage
• state function?
• border police
  • (Koninklijke Marechaussee)
• performed by Schiphol Group
• card communicates date, time and personal data to border police on passage
• enrolment
  • Border Police employee
    • checks passport
  • Schiphol employee
    • makes iris scan (2)
    • issues card
compatible with 95/46/EC?

- proportionality
- purpose
- sensitive data
- fair information collection
- legitimate processing
- proper security measures
- prior checking with DP authorities
General Terms and Conditions Privium

Privium Basic Level
1. Definitions
Automatic Border Passage:
Border passage using the Privium Card;
Privium:
Schiphol; Schiphol Nederland BV, having its registered office at Evert de Boeckerlaan 10, Luchthaven Schiphol, Amstelveen, the Netherlands, or a subsidiary designated by Schiphol Nederland BV;
Intermediary Party;
the party which, after having entered into a formal agreement with Schiphol, enables the Participant to enter into a Privium Participation Agreement through its interference and through settling the fee for the Privium Participation Agreement;
Privium Service:
The package of services offered specifically to the Participants by Schiphol;
Dedicated Security:
The combined security check of traveler and luggage at the airport, which, dependent on the situation, is either exclusively intended for Participants or provides Participants priority over other travelers;
Privium Participation Agreement:
The agreement between the Participant and Schiphol with regard to Privium Services;
Privium Card:
The identification (whether or not equipped with a magnetic strip) that enables the use of Privium Services.

2. Applicability and Privium Participation Agreement
2.1 These General Terms and Conditions apply to the Privium Participation Agreement.
2.2 The Privium Participation Agreement is formed by Schiphol’s acceptance of the application form filled in and signed by the potential Participant, which acceptance is considered to have taken place at the moment the Participant receives the Privium welcome package. If the Participant states at the Privium service desk that he wishes to become a member, the start of the making of the Iris scan shall be considered the moment of acceptance by Schiphol of the application from filled in and signed by the potential Participant. The iris scan is made on a voluntary basis, to the best of Schiphol’s knowledge, the iris scan does not involve health risks. Schiphol shall provide Privium Services exclusively to nationals of the European Union or the European Economic Area who are the rightful owners of a valid travel document (e.g. a passport), in which a date of birth is recorded.
2.3 After the formation of the Privium Participation Agreement, the Participant shall make an appointment with Schiphol for the making of a Privium Card. To this end, Schiphol will, inter alia, make an Iris scan of both eyes of the Participant. The Participant shall give any assistance required. Subsequently, Schiphol will convert the iris scan into a so-called template. In the event that it is impossible to make a good Iris scan that meets the norms of Schiphol (as a result of the Participant’s optical features), a Privium Card can be made for the Participant. In that case, Schiphol shall terminate the Privium Participation Agreement with immediate effect.

3. Privium Services
3.1 The range of Privium Services offered is determined by Schiphol and shall include in any case Automatic Border Passage and Dedicated Security.
3.2 Schiphol shall notify the Participant of any extensions or changes to the range of Privium Services offered.

4. Privium Card
4.1 The Privium Card shall be and remain the property of Schiphol. The Privium Card is strictly personal and cannot be used by any other person not the Participant, and is non-transferable. The Participant shall use the Privium Card in connection with the professional and/or commercial transportation of persons or goods. Any changes or alterations made to the Privium Card shall invalidate the Privium Card with immediate effect.
4.2 Upon expiry of the period of validity of the travel document (e.g., a passport) of the Participant used in the application, or in case of theft or loss of such travel document, the Participant’s right to make use of Automatic Border Passage that terminate. In that case, depending on the Privium level the Participant has registered for, the Participant can continue to use the other Privium Services (see below under “Special situations”). Upon acquisition of a new travel document (e.g., a passport), the Participant shall report this to Schiphol, whereupon Schiphol shall make an effort to allow renewed Automatic Border Passage with the Privium Card within a reasonable period of time. To this end, the Participant has to submit the new travel document for control to the Privium service desk at Schiphol.
4.3 The Participant shall immediately notify Schiphol in the event of loss and/or theft of the Privium Card. The notification of loss or theft shall be confirmed by the Participant in writing to Schiphol. At the first request of Schiphol, the Participant shall report the loss and/or theft of the Privium Card to the police, and the Participant shall provide Schiphol with a copy of such report. After the first notification by the Participant to Schiphol of the loss and/or theft of the Privium Card, Schiphol shall make an effort to render impossible the use of the lost or stolen Privium Card as soon as possible. A new Privium Card shall subsequently be made available to the Participant, for which purpose a new iris scan will have to be made.
4.4 In the event the Privium Card is damaged, the Participant shall return it to Schiphol. A new Privium Card shall then be made available to the Participant if Schiphol concludes that the damage in question renders all further use of the card impossible. In order to make a new card, Schiphol will make a new Iris scan at a time to be agreed upon with the Participant.
4.5 At the end of the technical life of the Privium Card, following notifica- tion thereof from Schiphol, the Participant shall make an appointment with Schiphol to have a new Privium Card made. On this occasion, a new iris scan of both eyes shall be made. The provisions of Article 2.3 shall apply by analogy.

5. Payment and choice of Privium level
5.1 In exchange for the provision of the Privium Card, Schiphol shall charge a fee, directly upon application and subsequently as of each 1 October, which fee shall be based on the current rates for Privium Services.
The fee will be charged either to the Participant, or to the Privium Participation Agreement. The fee charged to the Participant, for the use of the Privium Participation Agreement, will be charged to the Participant’s bank account, or by using the Participant’s credit card.
5.2 In the event that payment of the Privium Participation Agreement fee is settled by the Intermediary Party, Schiphol will not charge a fee to the Participant. The conditions for payment will be arranged in a separate agreement between the Intermediary Party and Schiphol. In the event that Schiphol did not receive the fee due in time, the Intermediary Party shall be liable in default and Schiphol shall be entitled to suspend Privium Services to the Participants concerned with immediate effect.
If charged to the Participant.
5.3 In exchange for the provision of the Privium Card, Schiphol shall charge a fee to the Participant directly upon application and subsequently as of each 1 October, which fee shall be based on the current rates for Privium Services. These rates shall be made public by Schiphol in a manner sufficiently knowable, including in any case by publication on the Privium website (www.privium.nl). The rates made public by Schiphol shall be in force throughout each period of 1 October up to and including 30 September. If the Participant applies at any other date than 1 October, the Participant shall pay a pro rata fee for the full number of calendar months between the date of application and 1 October.
5.4 With the exception of the fee payable upon application, the Participant must ensure every year that Schiphol receive the amount due prior to the subscription year to which the payment relates. In the event that Schiphol did not receive the fee in time, the Participant shall be in default as of 1 October and Schiphol shall be entitled to suspend Privium Services with effect from 1 October.
5.5 Schiphol may change the current rates. Schiphol shall notify the Participant of any such changes before the effective date of any subsequent subscription year. In the event of a rate increase, the Participant shall have the right - contrary to the provisions of Article 5 - to cancel the participation Agreement in writing with effect from the subscription year that the changed price relates to, without observing the notice period of two months.
5.6. The Participant may change to another Prinum level once per year, as of 1 October. If the Participant wishes to change to another Prinum level, he/she must notify Shiphol in writing of a change of membership to such other Prinum level as is available. He/she shall notify Shiphol in writing of a change of membership to another level as of 1 July by sending such notification to Shiphol Group, Prinum Service Point, Hoeksebaai 52/53, 1884 J.C.C.C.P.C.N. – 3098, 1110 VG Lichtenhein Shiphol, The Netherlands.

6. Other obligations of the Participant

6.1. The Participant shall only have the right to use Automatic Border Passage if (a) the Participant himself/herself subsequently departs from Shiphol by airplane, or has arrived at Shiphol by airplane, and (b) the Participant carries a valid travel document (e.g. a passport) and a valid boarding ticket (on-line ticket or boarding pass) that may be checked.

6.2. The Participant shall follow all instructions to be given by or on behalf of Shiphol for the purpose of order and safety at the airport and (b) all instructions to be given by the Dutch Border Police (Korps Politie, Mainzchaussee) in the interest of border control.

6.3. AnParticipant is entitled to block the use of the Prinum card by the Participant, whether or not temporarily, with immediate effect in the event that the Participant fails to comply with the instructions referred to in the previous paragraph, abuse the Prinum Card, or acts in violation of any part of the Prinum Participation Agreement.

7. Personal Data

7.1. Shiphol collects the personal data that the Participant filled in on the application form, as well as data on the use of the Prinum Card by the Participant. The statutory regulations as laid down in the Wet Persoons- registratie (Act on Personal Data/file) and the Wet Bescherming Persoonsgegevens (Personal Data Protection Act) are complied with by Shiphol.

7.2. In the Prinum Card, the card number, the template of the card, the name, place of birth and date of birth of the Participant are incorporated, as well as data derived from the data required for providing Prinum Services.

7.3. The purpose of processing personal data within the scope of Prinum Services is to support and facilitate to Participants the use of Shiphol Airport facilities in any designated way, and to grant preferential treatment to Participants in the broadest possible sense, based on careful examination of the data on the Participant’s use of the Prinum Card.

7.4. Within the scope of the above-mentioned purposes, the following personal data will be processed in any case when providing Prinum Services:

- the date and time at which the Prinum Card is inserted into the card reader of the Automatic Border Passage;
- within the scope of the Automatic Border Passage, the Dutch Border Police (Korps Politie, Mainzchaussee) shall be provided with the personal data required for the performance of its duties.

7.5. After the Participant has given his/her approval on the application form, Shiphol can grant the Participant tailor-made Prinum benefits in order to provide preferential treatment.

7.6. If the Participant objects to receiving tailor-made Prinum benefits, the Participant can make this known by sending an e-mail to prinum@shiphol.nl or by calling +31 (0)20-681 4222.

7.7. Shiphol shall, except in cases where the law requires and in cases mentioned in this Prinum Participation Agreement, not provide the Participant’s personal data to other persons or institutions outside Shiphol Group without the Participant’s consent. Shiphol will undertake every effort to regularly check personal data for accuracy and remove data no longer relevant in data.

7.8. The Participant can inspect his/her own personal data after having made a written request to that effect to Shiphol. At the request of the Participant, Shiphol shall provide an overview of the Participant’s data collected within the scope of Prinum Services. The Participant can request Shiphol, if deemed to correct inaccuracies, to add missing data and to remove irrelevant or superfluous data. The Participant can address all queries or complaints to prinum@shiphol.nl or telephone number +31 (0)20-681 4222.

7.9. The Participant shall immediately notify Shiphol in writing of any change in his/her personal data as mentioned on the application form.

8. Liability

8.1. The liability of Shiphol for damage that is in any way connected with the Prinum Card and/or Prinum Services shall be limited to the subscription fee to be paid annually by the Participant. This limitation of liability shall not apply if and insofar as Shiphol can be sued on the basis of mandatory applicable law (e.g. product liability law), as well as in the event of willful intent or gross negligence on the part of Shiphol or its executive staff.

9. Duration and termination

9.1. The Prinum Participation Agreement is concluded for an unlimited period of time. Either party shall have the right to terminate the Prinum Participation Agreement in writing as of 1 October with due observance of a notice period of two months.

9.2. In the event that the Prinum Participation Agreement has been established through the interference of the Intermediary Party and the Intermediary Party terminates its agreement with Shiphol (whether or not with regard to the participation of one Participant) or if the agreement between the Intermediary Party and Shiphol is being ended for other reasons, the termination of that agreement immediately involves simultaneous termination of the Prinum Participation Agreement between the Participant concerned and Shiphol.

The Intermediary Party shall inform Participant of the termination of its agreement with Shiphol. Shiphol will ask the Participant if he desires to continue the Prinum Participation Agreement at his own expense. If and when the Participant agrees to continue the Prinum Participation agreement, the Prinum Participation Agreement will remain in effect.

9.3. In the event the Participant fails to comply with the provisions of the Prinum Participation Agreement, Shiphol may dissolve the agreement without judicial intervention with immediate effect in whole or in part, if such failure justifies dissolution according to Shiphol’s reasonable judgment. In that case, Shiphol shall have the right to set off any amounts already paid by the Participant against the costs made by Shiphol in connection with the Participant’s failure and the dissolution of the Prinum Participation Agreement.

9.4. After termination of the Prinum Participation Agreement, the Participant shall no longer be entitled to use the Prinum Card. The Participant must return the Prinum Card upon termination of the Prinum Participation Agreement to Shiphol (by sending the Card to Shiphol Group Prinum Service Point, Hoeksebaai 52/53, 1884 J.C.C.C.P.C.N. – 3098, 1110 VG Lichtenhein Shiphol, The Netherlands).

10. Choice of law and resolution of disputes

The Prinum Participation Agreement is subject to the law of the Netherlands. Either Party may submit a dispute to the competent Dutch Court for resolution in the event that such Party is of the opinion that the conflict cannot be solved by mutual consultation. In case of disputes the Dutch version of these general conditions will prevail.

Special stipulations that apply only when another level than Prinum Basic is chosen:

Prinum Plus level

1. If the Participant has chosen the Prinum Plus level, the following additional conditions and conditions shall apply in addition to the above General Terms and Conditions Prinum Basis.

1.1. Dedicated Check-in

Checking in at one of the airline companies cooperating with Shiphol for the purpose of Prinum (often combined with use of the business class check-in desk).

Dedicated Parking

Parking in a parking space designated by Shiphol for use by Participants.

2. Article 3.1 is amended as follows:

The range of Prinum Services offered is determined by Shiphol and shall in any case include Dedicated Parking, Dedicated check-in, Automatic Border Passage and Dedicated Security.

3. One paragraph is added to Article 5, with the following text:

The fee shall not include the costs of Dedicated Parking. The Participant shall have to pay on site for the actual use of Dedicated Parking by means of the payment possibility or possibilities available on site.

4. A second paragraph is added to Article 7.4, with the following text:

- Dedicated Parking: the date and time of driving in and out as well as parking fees.
<table>
<thead>
<tr>
<th>Compliance with 95/46/EU?</th>
</tr>
</thead>
</table>
| **Purpose and proportionality (art 6)** | Stated border passage  
Limited data set |
| **Fair collection (art 10/11)** | Identity of controllers, purpose, address, recipients, right to access and **rectify** |
| **Processing legitimate (art 7)** | Consent  
Free and informed in writing |
| **Security (art 17)** | Encryption?  
Enrollment in controlled environment |
| **Prior checking (art 20)** | Yes, even awarded price |
questions

• is iris template only stored on card?
• which data is stored in the process?
• what data is communicated to border police?

• what is the legal relation between Schiphol Group N.V. – Border Police?
discussion
• do you subscribe to the privacy/data protection issues?
• can the requirements be met (in your context)?
• are the DP safeguards sufficient, or is additional regulation required?
Thank you for your attention


prior checking - notification

- central storage is discouraged
- member states can determine that processing operations likely to present risks to be examined by the data protection authorities