



Eidgenössischer Datenschutzbeauftragter
Préposé fédéral à la protection des données
Incaricato federale per la protezione dei dati
Incumbensà federal per la protecziun da datas

**Einsatz von Biometrie
beim Check-In und Boarding
im Rahmen des Pilotprojektes "Secure Check"
der Swissport International AG und
Checkport Schweiz AG am
Flughafen Zürich-Kloten**

Schlussbericht

vom 6. Juni 2005

sowie

Anhang

vom 24. Oktober 2005

**der Kontrolle des
Eidgenössischen Datenschutzbeauftragten (EDSB)
gemäss Art. 29 des Bundesgesetzes
über den Datenschutz (DSG)**

Veröffentlicht am 14. November 2005 auf www.edsb.ch

Inhaltsverzeichnis

Inhaltsverzeichnis.....	2
1. Ausgangslage	4
2. Umfang der Kontrolle	4
3. Chronologie der Kontrolle.....	4
4. Sachverhaltsabklärung vor Ort vom 16. Dezember 2004.....	5
4.1 Anwesende Personen.....	5
4.2 Enrollment am Check-In Schalter	5
4.3 Boarding am Gate.....	6
4.4 Weitere Datenerhebung.....	6
4.5 Einige Zahlen	7
4.6 Erstes Feedback des EDSB vor Ort.....	7
5. Sachverhaltsabklärung vor Ort vom 11. Februar 2005.....	9
5.1 Anwesende Personen.....	9
5.2 Biometrische Datenerfassung mit Gesichtsbild	9
6. Datenschutzrechtliche Beurteilung.....	10
6.1 Biometrische Daten als Personendaten.....	10
6.1.1 Ausgangslage	10
6.1.2 Beurteilung aus Sicht des EDSB.....	10
6.2 Zweck der Datenbearbeitung	10
6.2.1 Ausgangslage	10
6.2.2 Beurteilung aus Sicht des EDSB.....	11
6.3 Rechtmässigkeit der Datenbeschaffung/Einwilligung der Betroffenen	11
6.3.1 Ausgangslage	11
6.3.2 Beurteilung aus Sicht des EDSB.....	11
6.4 Bearbeitung nach Treu und Glauben/Transparenz.....	11
6.4.1 Ausgangslage	11
6.4.2 Beurteilung aus Sicht des EDSB.....	12
6.5 Verhältnismässigkeit der Datenbearbeitung.....	12
6.5.1 Verhältnismässigkeit in inhaltlicher Hinsicht – Ausgangslage.....	12
6.5.2 Beurteilung der inhaltlichen Verhältnismässigkeit aus Sicht des EDSB	13
6.5.3 Verhältnismässigkeit in zeitlicher Hinsicht – Ausgangslage	13
6.5.4 Beurteilung der zeitlichen Verhältnismässigkeit aus Sicht des EDSB.....	13
6.6 Zweckbindung der Datenbearbeitung.....	13
6.6.1 Ausgangslage	13
6.6.2 Beurteilung aus Sicht des EDSB.....	13
6.7 Datenrichtigkeit (Zuverlässigkeit, Anwendbarkeit).....	14
6.7.1 Ausgangslage	14
6.7.2 Beurteilung aus Sicht des EDSB	14
6.8 Datensicherheit	14
6.8.1 Ausgangslage	14
6.8.2 Anregungen aus Sicht des EDSB für den zukünftigen Einsatz von Biometrie	15
7. Ergebnisse	16
7.1 Bezüglich des Pilotprojektes.....	16
7.2 Bezüglich der Umsetzung des Pilotprojektes in ein Definitivum.....	16
8. Schlussfolgerung.....	17
8.1 Kontrolle des Einsatzes biometrischer Daten im Rahmen von Secure Check	17
8.2 Weiteres Vorgehen.....	17

Anhang vom 24. Oktober 2005 zum Schlussbericht.....	I
1. Vorbemerkung.....	I
2. Stellungnahme von Checkport	I
Zu Ziff. 6.1.2 des Schlussberichtes	I
Zu Ziff. 6.4.2 des Schlussberichtes	I
Zu Ziff. 6.7.2 des Schlussberichtes	I
Zu Ziff. 6.8.2 des Schlussberichtes	II
Zu Ziff. 7.2 des Schlussberichtes	II

1. Ausgangslage

Im Dezember 2004 hat *Swissport International AG* das *Pilotprojekt „Secure Check“* in Auftrag gegeben und gestartet. *Secure Check* dient der Verbesserung der Sicherheitsüberprüfung von Passagierdaten sowie den Reisedokumenten vor Abflug und soll dazu beitragen, die Wartezeiten für Flugpassagiere an den Checkpoints zu verkürzen. Das Pilotprojekt wurde von *Checkport Schweiz AG* (einer Tochtergesellschaft von *Swissport Schweiz AG*) und *Swissport Schweiz AG* (eine Tochtergesellschaft von *Swissport International AG*) in Zusammenarbeit mit *SWISS International Airlines* geführt.

Für die Testphase von Anfang Dezember 2004 bis Mitte April 2005 wurde der Flug Zürich-Montreal (CAN) ausgewählt. Flugpassagiere konnten an drei speziellen Schaltern einchecken. *Secure Check* läuft wie folgt ab: Für das Check-In werden die Ausweise der Flugpassagiere eingescannt und die Passdaten automatisch mit den Einreisebestimmungen des Destinationslandes (im Rahmen des Pilotprojektes Kanada) sowie mit bestehenden Blacklists verglichen. Die Passagier- und Passdaten werden zusammen mit den Flugdaten an das Destinationsland weiter geleitet. Zusätzlich erfolgt an jedem Checkpoint resp. am Gate eine Authentifizierung des Ausweisinhabers und Flugpassagiers *mittels biometrischer Daten (Templates)*, welche am Check-In Schalter nach der Ausweisüberprüfung vom Passagier erhoben werden. Die Datenschutzkontrolle konzentrierte sich auf die Erhebung und Bearbeitung dieser biometrischen Daten.

2. Umfang der Kontrolle

Die Datenschutzkontrolle bezog sich ausschliesslich auf das Pilotprojekt. Die Kontrolle umfasste nur die Datenabläufe im Zusammenhang mit der Erhebung und Bearbeitung der *biometrischen Daten* vom Check-In bis zum Boarding auf dem Flug Zürich-Montreal (CAN).

Nicht Gegenstand der Kontrolle waren alle weiteren mit dem Pilotprojekt *Secure Check* verbundenen Datenbearbeitungen, wie das Einscannen der Reiseausweise, der Abgleich mit den Blacklists und die Weiterleitung der Passagier- und Passdaten an das Destinationsland.

3. Chronologie der Kontrolle

- | | |
|-------------------|---|
| 4. November 2004 | Beschluss des EDSB zur Durchführung einer Datenschutzkontrolle bei <i>Swissport/Checkport</i> gestützt auf die Medienbekanntgabe der geplanten Durchführung eines Pilotprojektes mit biometrischen Daten. |
| 23. November 2004 | <i>Checkport</i> wendet sich telefonisch an den EDSB und möchte wissen, was beim Einsatz biometrischer Daten im Rahmen des Pilotprojektes <i>Secure Check</i> aus datenschutzrechtlicher Sicht beachtet werden muss. |
| 26. November 2004 | <i>Checkport</i> schickt per Email erste Informationen über das Projekt und lädt den EDSB zum internen Testlauf am 2. Dezember 2004 ein. Der EDSB sieht von einer Teilnahme am internen Testlauf ab und kündigt eine Sachverhaltsabklärung im Rahmen der vorgesehenen Kontrolle an. |
| 30. November 2004 | Der EDSB kündigt <i>Checkport</i> schriftlich eine Sachverhaltsabklärung mit Besichtigung der Anlagen vor Ort an. Zusätzlich wird <i>Checkport</i> gebeten, noch einige Fragen des EDSB zu beantworten. |

-
- | | |
|-------------------|--|
| 14. Dezember 2004 | Checkport schickt die noch ausstehenden Informationen im Vorfeld der Sachverhaltsabklärung vor Ort. |
| 16. Dezember 2004 | Sachverhaltsabklärung vor Ort am Flughafen Zürich-Kloten. Erstes Feedback des EDSB erfolgt mündlich. |
| 17. Dezember 2004 | Checkport reagiert umgehend auf das mündliche Feedback und ändert die Plakate am Check-In Schalter sowie die Informationsbroschüre. |
| 21. Dezember 2004 | Checkport kündigt per Email an, dass für die Löschung der Smart Cards sowie für die Schrift auf den Displays eine bessere Lösung gesucht werde. |
| 22. Dezember 2004 | EDSB reicht seine ersten Anpassungsvorschläge an Checkport schriftlich nach. In der Zwischenzeit hat Checkport bereits auf alle mündlich vorgebrachten Anpassungsvorschläge des EDSB reagiert. Im gleichen Schreiben schickt Checkport die ersten Antworten auf noch offene technische Fragen. |
| 24. Dezember 2004 | Checkport bestätigt per Email, dass sowohl der Löschvorgang der Smart Cards als auch die Schrift auf dem Display geändert wurden. |
| 11. Februar 2005 | Pilotprojekt wird um die Erfassung des Gesichtsbildes erweitert. Zweiter Augenschein vor Ort durch den EDSB. |
| 21. März 2005 | Checkport schickt die letzten fehlenden, technischen Daten für die Kontrolle. |
| April-Juni 2005 | Analyse und Auswertung aller Unterlagen und Sachverhalte sowie Ausarbeitung des Schlussberichtes durch den EDSB. |
| 6. Juni 2005 | Verabschiedung des Schlussberichtes durch den EDSB zuhänden Checkport. |

4. Sachverhaltsabklärung vor Ort vom 16. Dezember 2004

4.1 Anwesende Personen

Anwesend waren der Projektleiter Secure Check (Checkport), der Vice President Security (Swissport), eine Rechtskonsultantin (SWISS) sowie die Projektbegleiterin Secure Check (SWISS). Der EDSB war durch eine Juristische Beraterin und einen Informatikberater vor Ort vertreten.

4.2 Enrollment am Check-In Schalter

Das Pilotprojekt "Secure Check" wird derzeit nur beim Flug Zürich-Montreal (CAN) durchgeführt. Dazu stehen drei Check-In Schalter zur Verfügung, an denen sowohl First/Business- als auch Economy-Class Passagiere einchecken. Die Passagiere werden bei der Buchung auf das Pilotprojekt und die speziellen Check-In Schalter aufmerksam gemacht. Weiter kündigen grössere Plakate an den speziellen Check-In Schaltern das Pilotprojekt an, und ein Mitarbeiter von Checkport informiert die zur Abreise bereiten Passagiere persönlich über die Möglichkeit des Check-Ins/Boardings mittels biometrischer Daten, konkret mittels zwei biometrischer Fingerabdrücke (Templates).

Sofern ein Flugpassagier mit der Teilnahme am Pilotprojekt einverstanden ist, werden als erstes die Passinformationen des Passagiers ausgelesen. Diese Informationen werden in das Departure Control System (DCS) der SWISS gegeben, welches diese Daten aufbereitet und die Advanced Passenger Information Data (API-Data) in das entsprechende Destinationsland schickt. Dies war bereits vor dem Pilotprojekt der Fall. Die Daten werden nun aber effizienter in das System eingespeist. Zusätzlich wird ein Abbild der Datenseite des Passes eingescannt, falls dies von der Einreisebehörde des Destinationslandes verlangt wird. Mit dem Einlesen des Passes wird gleichzeitig die Einhaltung der Passbestimmungen des Destinationslandes verifiziert. Im Rahmen des Pilotprojektes erfolgt dieses Einlesen des Passes durch drei Notebooks. Da das Pilotprojekt nur mit einem bestimmten Flug pro Tag durchgeführt wird, sind die Flugdaten und die entsprechenden Passagiernamen bereits im Vorfeld vom Departure Control System (DCS) der SWISS übernommen worden. Die eingelesenen Daten sowie die eingescannte Passseite werden nach 48 Stunden aus dem Secure Check System (während der Pilotphase auf den drei Notebooks) automatisch gelöscht. Die Daten werden nicht ausgewertet und nur für den Fall gebraucht, dass ein Passagier Probleme bei der Einreise hat.

Des Weiteren werden im Rahmen des Pilotprojektes biometrische Daten der Flugpassagiere auf freiwilliger Basis erhoben. In einem zweiten Schritt werden dafür die Passagierdaten, die Passdaten, die Flugnummer und das Flugdatum auf eine Smart Card übertragen. Die Smart Card enthält einen Mikroprozessor, der bis auf eine Entfernung von 5 cm kontaktlos abgelesen werden kann. Ist die Übertragung der Daten erfolgt, so erscheint auf einem grossen Display, das sich direkt vor dem Passagier befindet, automatisch der Name des Passagiers, wie er im Pass festgehalten ist. Nun wird der Passagier aufgefordert, nacheinander seinen linken und seinen rechten Zeigefinger zum Ablesen auf eine Glasplatte, die sich unterhalb des Displays befindet, zu halten. Auf dem Display erscheint jeweils die Nachricht, ob das Ablesen (=Enrollment) funktioniert hat oder nicht. Das Template des Fingerabdrucks wird auf der Smart Card festgehalten. Die Daten auf der Smart Card sind nach 3DES-Standard verschlüsselt. Der Passagier behält die Smart Card bei sich und geht nun mit der Smart Card, seinem Flugticket und seinem Pass durch den Zoll in den Transitbereich. Am Zoll muss der Passagier seinen Pass und das Flugticket noch vorzeigen, während neu die Verifikation am Gate durch die Smart Card und die biometrischen Referenzdaten erfolgt.

4.3 Boarding am Gate

Flugpassagiere, welche am Pilotprojekt teilnehmen und daher eine Smart Card vom Check-In Schalter haben, legen diese Karte auf ein mobiles Gerät, das die Daten kontaktlos ablesen kann. Das Ablesegerät verfügt ebenfalls über ein Display, jedoch ist dieses kleiner als am Check-In Schalter und zusätzlich mit zwei Seitenklappen besser vor Blicken Dritter geschützt. Auf dem Display erscheint die Aufforderung, einen Zeigefinger auf die Glasplatte zu halten. Bei einem reibungslosen Ablauf dauert dieser Prozess nicht mehr als 5 Sekunden. Ein Mitarbeiter von Checkport steht neben dem Gerät und sammelt die Smart Cards der Flugpassagiere wieder ein. Nach erfolgreicher Verifikation des Flugpassagiers zeigt dieser noch seine Boarding Card, welche wie bei jedem anderen Fluggast anschliessend automatisch eingeleesen wird. Der anwesende Mitarbeiter bringt nach dem Boarding alle Smart Cards in das Büro des Projektleiters Secure Check (Checkport), wo sie noch am gleichen Tag gelöscht werden, um am darauffolgenden Tag für weitere Flüge zur Verfügung zu stehen. Die Smart Cards werden also (noch) nicht für weitere Flüge oder für den Ankunftstransit weiter verwendet.

4.4 Weitere Datenerhebung

Weiter werden auf dem Check-In System und auf dem Gate System statistische Daten erhoben, welche zur Verbesserung der Erkennung des Fingerabdrucks genutzt werden. Diese Daten sind: Alter, Nationalität, Wohnsitzland, Geschlecht und Wert der Biometrieerkennung. Es werden keine Namen oder Templates in der Statistik erfasst. Die Statistik dient aus-

schliesslich den Technikern zur Verbesserung der Erkennungsrate. Weitere Daten werden weder erhoben noch werden die vorhandenen Daten mit weiteren Daten oder Datenbanken verknüpft.

4.5 Einige Zahlen

Stand vom 16. Dezember 2004: Die Projektleitung hat bei Einführung des Pilotprojektes damit gerechnet, dass max. 50% der Passagiere, die in Zürich einchecken, sich am Pilotprojekt beteiligen würden. In den ersten zwei Wochen haben sich ca. 70% aller möglichen Passagiere am Projekt beteiligt und der biometrischen Erfassung ihrer Fingerabdrücke zugestimmt (pro Flug bedeutet dies konkret ca. 14 von 20 Fluggästen). Die grössten technischen Schwierigkeiten bestehen beim Enrollment von alten Menschen (v.a. bei Frauen). Kinder unter 12 Jahren sind vom Pilotprojekt ausgenommen, da ihre Fingerabdrücke schlecht eingelesen werden können.

Stand vom 4. Februar 2005: Insgesamt ist bis zum 4. Februar 2005 das Enrollment bei 725 Flugpassagieren gelungen und bei 22 Personen misslungen (vorwiegend ältere Personen). Am Gate wurden 4 Personen nicht wieder erkannt.

Stand vom 15. April 2005: Bis Ende des Pilotprojektes Mitte April 2005 konnte das Enrollment und die Verifikation bei 1400 Passagieren erfolgreich vorgenommen werden. Dies entspricht 79% der Passagiere, welche an den Spezialschaltern eingesteckt haben.

4.6 Erstes Feedback des EDSB vor Ort

Während der Besichtigung vor Ort erhält Swissport/Checkport von den beiden Mitarbeitern des EDSB ein erstes Feedback, welches mit Brief vom 22. Dezember 2004 des EDSB bestätigt wurde. Das Feedback bezog sich auf folgende Punkte:

- **Plakate am Check-In Schalter**

An den drei Check-In Schaltern sind gut sichtbar Plakate aufgestellt, die auf das Pilotprojekt und die damit verbundene Möglichkeit des vereinfachten Check-Ins und Boardings mittels biometrischer Fingerabdrücke aufmerksam machen. Jedoch wird aus der gewählten Formulierung nicht ausreichend ersichtlich, dass die Teilnahme am Pilotprojekt und insbesondere die Abgabe der Fingerabdrücke *freiwillig* erfolgt. Vielmehr werden die Passagiere, sofern sie sich nicht am Pilotprojekt beteiligen wollen, an das Bodenpersonal verwiesen (sog. Opting-out Lösung). Die Mitarbeiter des EDSB machen die Projektleitung darauf aufmerksam und bitten, die Formulierung dahingehend zu ändern, dass die Freiwilligkeit am Pilotprojekt teilzunehmen klarer zur Geltung kommt.

Die Projektleitung hat die Plakate noch am selben Tag geändert und dabei eine neue Formulierung gewählt, welche die Freiwilligkeit des Pilotprojektes verdeutlicht. Für die Passagiere wird nun klar, dass die Abgabe der Fingerabdrücke freiwillig ist. Ausserdem wird mit der neuen Formulierung klargestellt, dass die Passagiere von sich aus die Möglichkeit haben, am Pilotprojekt teilzunehmen, was eher der von Seiten des EDSB geforderten Opting-in Lösung entspricht.

- **Erwähnung des EDSB in der Informationsbroschüre**

Den Passagieren wird seit Beginn des Pilotprojektes eine Informationsbroschüre ausgehändigt. Dort findet sich unter dem Titel „Persönlicher Datenschutz“ folgender Satz: „Die Eidgenössische Datenschutzaufsichtsbehörde überprüft die Handhabung Ihrer persönlichen Daten während des Pilot-Projekts“. Die Mitarbeiter des EDSB bitten die Projektleitung, diese Passage ganz zu streichen oder eine andere Formulierung zu wählen, aus der klar hervor geht, dass der EDSB über das Pilotprojekt informiert ist und

klar hervor geht, dass der EDSB über das Pilotprojekt informiert ist und mit der Projektleitung in Fragen des Datenschutzes im Austausch steht. Jedoch hat sich der EDSB insbesondere vor dem Augenschein vor Ort am 16. Dezember 2004 noch nicht zur Datenschutzkonformität des Pilotprojektes geäußert.

Die Projektleitung hat diesen Satz noch am gleichen Tag aus der Broschüre gestrichen und im Anschluss daran die alten Informationsbroschüren gegen die neuen ausgetauscht.

- **Rückgabe und Löschung der Smart Card**

Bei der Besichtigung vor Ort überreichen die Passagiere nach erfolgter Verifikation vor dem Boarding am Gate die Smart Card einem Mitarbeiter von Checkport. Dieser bringt die Karten anschliessend in das Büro des Projektleiters Secure Check, wo sie noch am gleichen Tag vollständig gelöscht werden. Die Mitarbeiter des EDSB regen an, dass zur Verbesserung der Transparenz die Löschung der Smart Card – mit sichtbarer Bestätigung aller gelöschten Daten – von den Flugpassagieren selbst vor Ort vorgenommen wird. Die Passagiere sollten auch die Möglichkeit haben, die Löschung selbst noch einmal zu verifizieren. Die Projektleitung wurde aufgefordert, entsprechende Software-Lösungen mit dem Hersteller zu überprüfen.

Die Projektleitung hat nach der Sachverhaltsabklärung vor Ort durch den EDSB das Lösungsverfahren geändert. Die Smart Cards werden nun neu nach erfolgreicher Verifikation am Gate automatisch gelöscht. Die Löschung wird dem Passagier auf einem Display sogleich bestätigt. Ausserdem hat der Passagier die Möglichkeit, die Löschung mit nochmaligem Einleseversuch zu überprüfen.

- **Display am Check-In Schalter**

Die Mitarbeiter des EDSB machen darauf aufmerksam, dass am Check-In Schalter nach erfolgtem Einlesen der Passdaten und deren Übertragung auf die Smart Card der vollständige Name des Flugpassagiers auf einem grossen Display erscheint. Der Name kann aus einer Distanz von ca. 7 Metern von Dritten gut gelesen werden.

Die Projektleitung erkennt das Problem sofort und will prüfen, ob eine kleinere Schrift besseren Schutz bietet oder ob das Display mit anderen Massnahmen besser vor Blicken unbeteiligter Dritter geschützt werden kann. Die Projektleitung lässt die Schrift nach der Sachverhaltsabklärung vor Ort verkleinern. Sie kann nun nur noch aus geringer Nähe gelesen werden. Für die definitive Implementierung von Secure Check werden andere Lösungen (Schutzschilder) in Erwägung gezogen.

5. Sachverhaltsabklärung vor Ort vom 11. Februar 2005

5.1 Anwesende Personen

An der zweiten Sachverhaltsabklärung vor Ort waren der Projektleiter Secure Check (Checkport) sowie die Juristische Beraterin und der Informatikerberater des EDSB anwesend.

5.2 Biometrische Datenerfassung mit Gesichtsbild

In einer zweiten Phase des Pilotprojektes wird neu anstelle der biometrischen Fingerabdrücke das Gesichtsbild biometrisch erfasst. Für die Pilotphase wurde dazu ein Check-In Schalter mit einer Webcam ausgerüstet. Das Einlesen der Flug- und Passdaten erfolgt gleich wie bei der ersten Projektphase (vgl. oben Ziff. 4.2). Auf der Smart Card werden beim Enrollment nun aber nicht zwei Templates der Fingerabdrücke festgehalten, sondern die Templates zweier Gesichtsbilder.

Die Gesichtsbilder werden von einer VGA Kamera mit automatischer Kontrasteinstellung erfasst. Für das Enrollment stellt sich der Flugpassagier vor die Kamera. In sekundenschnelle erfasst die Kamera 9 Gesichtsbilder des Passagiers. Die aufgenommenen Gesichtsbilder erscheinen auf dem Bildschirm der Laptops des Bodenpersonals. Die Bilder werden sofort auf ihre Kompatibilität mit den angewandten Algorithmen analysiert. Diejenigen Bilder, bei denen die algorithmische Umwandlung problemlos funktioniert, erhalten einen grünen Rahmen (= akzeptiert). Alle anderen sind rot umrahmt (= nicht akzeptiert). Von den akzeptierten Bildern werden automatisch zwei ausgewählt, mit dem angewandten Algorithmus auf ein Template reduziert und dieses Template auf der Smart Card gespeichert.

Für die spätere Verifikation am Gate reicht es aus, die Smart Card auf das Ablesegerät zu legen und in eine zweite Kamera zu blicken. Das Template auf der Smart Card wird nun mit dem Gesichtsbild (ebenfalls Template) abgeglichen. Ist die Verifikation gelungen, erscheint nach ca. ein bis zwei Sekunden der Name des Flugpassagiers auf dem Display. Ist die Verifikation missglückt, wird dies auf dem Display mit einer Fehlermeldung angezeigt. Die Gesichtserkennung zeichnete sich während der Sachverhaltsabklärung des EDSB durch eine hohe Verlässlichkeit aus.

6. Datenschutzrechtliche Beurteilung

6.1 Biometrische Daten als Personendaten

6.1.1 Ausgangslage

Das Bundesgesetz über den Datenschutz (DSG; SR 235.1) findet dort Anwendung, wo mit Personendaten im Sinne des Art. 3 lit. a DSG operiert wird. Im vorliegenden Fall werden im Rahmen des Pilotprojektes Secure Check biometrische Daten bearbeitet (Templates von Fingerabdrücken und von Gesichtsbildern).

6.1.2 Beurteilung aus Sicht des EDSB

Biometrische Daten der Fingerabdrücke und der Gesichtsbilder in Form von Templates machen eine Person durch Abgleich mit einem Referenzdatum bestimmbar und können der Verifikation (resp. Identifikation) einer Person dienen. Im Rahmen des Projektes Secure Check ergibt sich die Bestimmbarkeit nicht nur aus der Abgleichsmöglichkeit, sondern auch klar aus der Kombination all derjenigen Daten, welche auf der Smart Card festgehalten werden, nämlich Templates sowie weitere Passagier- und Flugdaten der betroffenen Person (u.a. Name, Vorname, Geburtsdatum, Geburtsort etc.). *Die biometrischen Templates können in Verbindung mit diesen weiteren Daten klar einer Person zugeordnet werden und machen diese bestimmbar (Art. 3 lit. a DSG).*

Sowohl das Gesichtsbild als auch die eigenhändige Unterschrift auf den Identitätsdokumenten (Signatur) stellen biometrische Daten dar, welche nicht nach dem Einscannen auf die Smart Card kopiert werden sollten.

Bei der Umsetzung des Pilotprojektes in ein Definitivum sollte die Projektleitung diesen Umstand beachten und auf die Übertragung von Gesichtsbildern aus den Identitätsdokumenten (Rohdatum) sowie der eigenhändigen Unterschrift verzichten.

Die Algorithmen für Template-Extrahierungen von biometrischen Rohdaten sind heutzutage weder standardisiert noch transparent, deswegen ist es *derzeit nicht möglich, die Sensibilität (Elemente über Gesundheit/Rasse?) eines Templates formell einschätzen zu können.*

6.2 Zweck der Datenbearbeitung

6.2.1 Ausgangslage

Ziel des Projektes „Secure Check“ ist die *Vereinfachung des Abfertigungsprozesses* der Flugpassagiere vom Check-In über das Boarding bis zur Ankunft im Destinationsland. Mit der Erfassung der biometrischen Daten werden nach Auskunft der Projektleitung für die Flugpassagiere die Prozessabläufe bis zum Boarding einfacher gestaltet („fast-track system“). Für die Verifikation der Identität am Gate (oder jedem anderen Checkpoint, ausser dem Zoll) benötigt der Passagier das Flugticket und die Smart Card, ohne dass er den Reisepass noch einmal vorzeigen muss. Auch wird mit dem Einsatz biometrischer Daten den Schlepperbanden im Transitbereich eines Flughafens die Arbeit erschwert, da sowohl die Verifikation am Check-In Schalter als auch das Enrollment biometrischer Daten auf der Smart Card ein Austausch von Boarding Cards erheblich erschwert resp. verunmöglicht. Für die SWISS resp. Swissport/Checkport ist dies gemäss Auskunft der Projektleitung mit *Kosten- und Ressourceneinsparungen* verbunden. Denn für Fluggäste ohne gültige Einreisepapiere resp. für Fluggäste mit falschen oder gar keinen Flugtickets müssen die Fluggesellschaften im Destinationsland hohe Bussgelder bezahlen. Gemäss Information der Projektleitung belaufen sich diese Bussgelder dank der von Checkport bis anhin durchgeführten manuellen Kontrollen

unter einer Million CHF. Diese Bussgelder würden sich ohne manuelle Kontrollen im Rahmen eines höheren einstelligen Millionenbetrages bewegen. Ziel der Projektleitung ist es daher ebenfalls, mit dem Pilotprojekt aufzuzeigen, dass die effektiven Bussgelder und der Aufwand zur Vermeidung der Bussgelder verringert werden können. *Weiter soll der ganze Prozess die Sicherheit für die Passagiere und die Fluggesellschaft erhöhen.*

6.2.2 Beurteilung aus Sicht des EDSB

Das Pilotprojekt „Secure Check“ und die damit verbundene Erhebung biometrischer Personendaten verfolgt für die Fluggesellschaft und die Flugpassagiere nachvollziehbare Zwecke. *Der EDSB hat dazu keine Bemerkungen.*

6.3 Rechtmässigkeit der Datenbeschaffung/Einwilligung der Betroffenen

6.3.1 Ausgangslage

Biometrische Daten sind Personendaten im Sinne des Datenschutzgesetzes, für deren Bearbeitung ein Rechtfertigungsgrund (Art. 12 und 13 DSG) benötigt wird. Als Rechtfertigung der Datenbearbeitung kommt im vorliegenden Fall die Einwilligung der Betroffenen in Frage.

Die Flugpassagiere werden bei der Buchung und bei Ankunft am Flughafen Zürich-Kloten auf das Pilotprojekt aufmerksam gemacht. Ein Plakat am Check-In Schalter weist darauf hin, dass die Erhebung biometrischer Daten freiwillig erfolgt. Eine Informationsbroschüre, welche ebenfalls am Schalter aufliegt, informiert über das Pilotprojekt und die damit verbundene Erhebung biometrischer Daten. Zusätzlich steht am Schalter ein Mitarbeiter von Checkport bereit und gibt weitere Auskünfte zum Projekt.

Vor der Sachverhaltsabklärung vor Ort durch den EDSB kam die Freiwilligkeit der Erhebung biometrischer Daten zu wenig klar zum Ausdruck. Ebenso liess die von der Projektleitung gewählte Formulierung der Informationsplakate am Schalter eher auf eine sog. Opting-out Lösung schliessen. Auf Anraten des EDSB wurde diese Formulierung umgehend geändert und angepasst, wobei die Freiwilligkeit nun klar ersichtlich wird und eine Opting-in Lösung gewählt wurde.

6.3.2 Beurteilung aus Sicht des EDSB

Mit diesen Umwandlungen ist davon auszugehen, dass die Datenbeschaffung der Flugpassagiere *mit ihrer Einwilligung* erfolgt und diese umfassend über den *Zweck der Datenerhebung informiert* sind.

6.4 Bearbeitung nach Treu und Glauben/Transparenz

6.4.1 Ausgangslage

Die Bearbeitung von Personendaten muss nach Treu und Glauben erfolgen (Art. 4 Abs. 1 DSG). Dies bedeutet zum einen, dass die Datenbearbeitung für die betroffenen Personen transparent erfolgen muss. Zum anderen muss eine Datenbeschaffung und jede weitere Datenbearbeitung grundsätzlich für die Betroffenen erkennbar sein.

Die Passagiere werden sowohl bei der Buchung des Fluges als auch vor Ort mit einer Informationsbroschüre und Plakaten über das Pilotprojekt und die Erhebung biometrischer Daten informiert. Ein Mitarbeiter von Checkport steht jederzeit für weitere Fragen zur Verfügung.

Zudem muss ein Passagier aktiv tätig werden, damit seine biometrischen Daten erfasst werden können (Auflegen der beiden Zeigefinger resp. Blick in die Kamera). Ohne sein Zutun können keine biometrischen Daten erhoben werden.

6.4.2 Beurteilung aus Sicht des EDSB

Durch die breit angelegte Informationsstrategie (bei Buchung und vor Ort) der Projektleitung kann davon ausgegangen werden, dass die Datenbearbeitung für die Flugpassagiere *transparent erfolgt*. Da die biometrischen Daten nicht ohne Zutun der Betroffenen erhoben werden (können), erfolgt die Datenbearbeitung für diese auch *klar erkennbar* (Fingerauflegen oder Blick in die Kamera).

Für eine möglichst transparente Datenbearbeitung wäre es sinnvoll, die betroffene Person über die verschiedenen auf der Smart Card gespeicherten personenbezogenen Daten (Passdaten, Flugdaten, Templates, etc) zu informieren. Die Information im Sinne einer Zusammenfassung der ergriffenen Sicherheitsmassnahmen (Verschlüsselung) gegen unbefugte Bearbeitungen würde ebenfalls zu einer verbesserten Transparenz in der Datenbearbeitung beitragen. Hier besteht aus Sicht des EDSB eine Informationslücke.

Der EDSB schlägt der Projektleitung vor, dass die Transparenz der Datenbearbeitung durch diese Zusatzinformationen (welche Daten werden konkret auf der Smart Card gespeichert; welche Sicherheitsmassnahmen wurden zum Schutz dieser Daten ergriffen) bei der Umwandlung des Pilotprojektes in ein Definitivum erhöht wird.

6.5 Verhältnismässigkeit der Datenbearbeitung

Die Datenbearbeitung von Personendaten hat sich am Grundsatz der Verhältnismässigkeit auszurichten (Art. 4 Abs. 2 DSGVO). Dies bedeutet, dass ein Datenbearbeiter nur diejenigen Daten bearbeiten darf, die er für einen bestimmten Zweck objektiv tatsächlich benötigt und die im Hinblick auf den Bearbeitungszweck und die Persönlichkeitsbeeinträchtigung in einem vernünftigen Verhältnis stehen.

6.5.1 Verhältnismässigkeit in inhaltlicher Hinsicht – Ausgangslage

Eine Datenbearbeitung ist dann verhältnismässig, wenn sie sich inhaltlich auf das absolut Notwendige beschränkt, um ein bestimmtes Ziel zu erreichen. Die inhaltliche Verhältnismässigkeit fordert einen möglichst schonenden Umgang mit Personendaten. Dies bedingt auch, dass keine für den verfolgten Zweck nicht benötigten Überschussinformationen anfallen. Ebenso ist es unzulässig, Personendaten auf Vorrat zu erheben, sofern der damit verfolgte Zweck dies nicht unabdingbar erfordert.

Die Erhebung biometrischer Daten im Rahmen des Pilotprojektes beschränkt sich auf die *dezentrale Speicherung* der Templates auf der Smart Card. Insbesondere werden *keine Rohdaten* auf den Smart Cards festgehalten und *keine Rohdaten oder Templates zentral gespeichert*. Die Flugpassagiere, welche sich am Pilotprojekt beteiligen, tragen die Smart Card mit ihren biometrischen Daten während der Datenerfassung am Check-In bis zum Boarding bei sich.

Vor der Sachverhaltsabklärung vor Ort vom 16. Dezember 2004 erschien am Check-In Schalter beim Enrollment der Name des Flugpassagiers auf einem Display, dass von unbeteiligten Dritten auf ca. 7 m Distanz gut sichtbar und insbesondere lesbar war. Auf Anregung des EDSB liess die Projektleitung die Schrift auf dem Display verkleinern. Sie kann nun nur noch aus geringer Entfernung gelesen werden. Für die definitive Implementierung des Pilotprojektes in ein Definitivum werden gemäss schriftlicher Bestätigung der Projektleitung andere Lösungen (Schutzschilder) in Erwägung gezogen.

6.5.2 Beurteilung der inhaltlichen Verhältnismässigkeit aus Sicht des EDSB

Durch die Beschränkung der dezentralen Speicherung der Templates auf der Smart Card und insbesondere durch den Verzicht der Speicherung von Rohdaten erfolgt aus Sicht des EDSB die Bearbeitung der biometrischen Daten *in inhaltlicher Hinsicht verhältnismässig*. Es werden keine über die Erreichung des Projektzieles hinausgehenden Daten erhoben.

Mit den von der Projektleitung nachträglich ergriffenen Schutzmassnahmen zum verbesserten Schutz des Displays erscheint auch hier die Datenbearbeitung als *inhaltlich verhältnismässig*.

6.5.3 Verhältnismässigkeit in zeitlicher Hinsicht – Ausgangslage

Das Erfordernis der Verhältnismässigkeit begrenzt die Datenbearbeitung auch in zeitlicher Hinsicht. Sofern personenbezogene Daten für den verfolgten Zweck nicht mehr gebraucht werden, sind sie zu vernichten resp. zu löschen.

Vor der Sachverhaltsabklärung vor Ort vom 16. Dezember 2004 erfolgte die Löschung der auf der Smart Card gespeicherten biometrischen Daten jeweils im Büro des Projektleiters. Auf Anregung des EDSB wurde das Löschverfahren geändert. Die Smart Cards werden nun neu nach erfolgreicher Verifikation des Flugpassagiers am Gate automatisch gelöscht. Die Löschung wird dem Passagier auf einem Display sogleich bestätigt. Ausserdem hat der Passagier die Möglichkeit, die Löschung mit nochmaligem Einleseversuch zu überprüfen.

6.5.4 Beurteilung der zeitlichen Verhältnismässigkeit aus Sicht des EDSB

Mit den von der Projektleitung umgesetzten Änderungen des Löschvorgangs erfolgt die Datenbearbeitung nun *auch in zeitlicher Hinsicht verhältnismässig*.

6.6 Zweckbindung der Datenbearbeitung

6.6.1 Ausgangslage

Personendaten dürfen nur für den Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde oder der aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 4 Abs. 3 DSGVO).

Die Erhebung der biometrischen Daten und die Speicherung der Daten auf einer Smart Card dienen dem Zweck, die Prozessabläufe vom Check-In bis zum Boarding für die Flugpassagiere zu vereinfachen. Die Verifikation am Gate erfolgt nicht mehr wie üblich durch Vorweisen des Passes und des Flugtickets, sondern durch den Abgleich des eigenen Fingerabdrucks resp. Gesichtsbildes mit dem auf der Smart Card gespeicherten Referenzdaten und der Präsentation des Flugtickets. Die biometrischen Daten (Templates) sind also *dezentral auf der Smart Card gespeichert*, welche der Flugpassagier während des gesamten Prozessablaufes bei sich trägt. Das biometrische System an sich speichert ebenfalls keine biometrischen Daten (z.B. beim Einlesen auf dem Scanner oder von der Web-Kamera aus).

6.6.2 Beurteilung aus Sicht des EDSB

Dadurch, dass die biometrischen Daten dezentral auf der Smart Card gespeichert sind und der Flugpassagier die Karte während der ganzen Speicherzeit bei sich trägt, ist eine *Zweckentfremdung* in der Datenbearbeitung dieser Daten *so gut wie ausgeschlossen*.

Eine *Zweckentfremdung* im Sinne einer *Verknüpfung* mit anderen Datensammlungen (z.B. von der Flughafenpolizei oder sonstiger Datenbanken für erkennungsdienstliche Zwecke) oder eine *Weitergabe an unbefugte Dritte* erscheint aufgrund der fehlenden zentralen Speicherung der biometrischen Rohdaten oder Templates – zumindest derzeit – *ebenfalls als ausgeschlossen*.

6.7 Datenrichtigkeit (Zuverlässigkeit, Anwendbarkeit)

6.7.1 Ausgangslage

Das Vergleichsverfahren zwischen Referenz- und Musterdaten (hier Templates) basiert auf Wahrscheinlichkeitsberechnungen und ergibt einen Übereinstimmungswert, der grösser als eine vordefinierte Schwelle sein muss, um die Person zu erkennen. Von dieser einzigen Schwelle sind die beiden Werte "False Rejection Rate (FRR)" und "False Acceptance Rate (FAR)" umgekehrt abhängig. Aus Datenschutzgründen sollte vor allem die FAR vermindert werden, ohne aber die FRR zu stark zu erhöhen. Die Wahl eines optimalen Schwellenwertes für eine ausreichende Zuverlässigkeit des gesamten biometrischen Systems ist aus diesem Grund nicht einfach zu treffen.

Nicht ausser acht gelassen werden darf auch die Tatsache, dass gewisse Anwender (aufgrund fehlender Gliedmassen, Verletzungen, Narben oder aufgrund des Alters, wie z.B. Kinder oder ältere Personen) keine oder zu wenig gute biometrische Merkmale vorweisen und ihre Authentifizierung misslingt (vgl. dazu auch die Bemerkungen unter Ziff. 4.5).

6.7.2 Beurteilung aus Sicht des EDSB

Aus Datenschutzgründen sollte die FAR vermindert werden, ohne aber die FRR zu stark zu beeinträchtigen und ein optimaler Schwellenwert gewählt werden. Jedes biometrische System weist einen gewissen Prozentsatz an FAR auf. Die Authentifizierung kann infolgedessen nicht zu 100% zuverlässig erfolgen.

Es sollte daher eine multimodale Authentifizierung (durch Kombination mit anderen personenbezogenen Merkmalen wie z.B. einer PIN) eingesetzt werden.

Probleme ergeben sich insbesondere auch bei Personen, denen gewisse biometrische Merkmale fehlen oder nur schlecht lesbar vorhanden sind (Enrollment). Diese Personen müssen aber genauso sicher und ebenso effizient wie alle anderen authentifiziert werden können.

Für solche Ausnahmen muss daher eine äquivalente Anwendbarkeit des Erkennungssystems geplant und eingesetzt werden.

Die Projektleitung sollte diese Anregungen bei der Umsetzung des Pilotprojektes in ein Definitivum in ihre Überlegungen mit berücksichtigen.

6.8 Datensicherheit

6.8.1 Ausgangslage

Gemäss Art. 7 DSGVO müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten gesichert werden. Zu gewährleisten sind insbesondere die Vertraulichkeit, die Verfügbarkeit sowie die Integrität der Personendaten. Diese Anforderungen sind dann nicht mehr gewährleistet, wenn ein fremdes „Drittgerät“ die Daten abhören oder manipulieren könnte. Die Datensicherheit liegt in der Verantwortung derjenigen Stelle, welche die Datenherrschaft über die Personendaten inne hat (Art. 8 Abs. 1 Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (VDSDG; SR 235.11).

6.8.2 Anregungen aus Sicht des EDSB für den zukünftigen Einsatz von Biometrie

Bezüglich der Beurteilung der allfälligen Sensibilität und folglich dem angemessenen Schutzniveau von biometrischen Templates besteht aus heutiger Sicht eine Unsicherheit.

Deshalb sind alle personenbezogenen Daten in verschlüsselter Form auf der Smart Card abzulegen. Die Verschlüsselung ist auch bei der Umwandlung in ein Definitivum weiterhin vorzusehen.

Es kann nicht ausgeschlossen werden, dass ein in der Nähe verstecktes, aber sehr empfindliches Gerät, den ausgeführten Datenaustausch abhören könnte.

Daher sollte ein verlässlicher Authentifizierungsmechanismus zwischen Smart Cards und Lese-/Schreibgeräten eingesetzt werden, um jede unbefugte Kenntnisnahme oder Veränderung von Seiten Dritter zu verhindern. Dazu sollte die drahtlose Datenübertragung an sich auch in verschlüsselter Form erfolgen, obwohl die Smart Card direkt auf das Ablesegerät gelegt wird.

Des Weiteren stellt nach Meinung des EDSB nur eine mehrfache Überschreibung aller Datenbestände auf der Smart Card sicher, dass Personendaten nicht wieder hergestellt werden können.

Beim Löschverfahren von Personendaten auf der Smart Card muss daher gewährleistet werden, dass diese Daten physikalisch und nicht nur logisch vernichtet werden.

Der Umstand, dass das Lesegerät die Daten auf der Smart Card nicht mehr erkennen kann, bedeutet leider noch nicht, dass die darauf enthaltenen Daten auch tatsächlich alle vernichtet wurden.

Aus Gründen einer umfassenden Transparenz sollte für alle Kategorien von Personendaten (Passdaten, individuelle Flugdaten, Templates etc.) dem Flugpassagier eine Löschestätigung mitgeteilt werden, mit dem Hinweis darauf, dass die entsprechenden Daten alle unwiderruflich vernichtet wurden.

Bei der Umsetzung des Pilotprojektes in ein Definitivum sollten diese Anregungen von der Projektleitung mit berücksichtigt werden.

7. Ergebnisse

7.1 Bezüglich des Pilotprojektes

An der Sachverhaltsabklärung vor Ort vom 16. Dezember 2004 bestand aus Sicht des EDSB *Anpassungsbedarf* im Bereich der Einwilligung und Information der Flugpassagiere am Check-In Schalter, bei der Wiedergabe des Namens der Flugpassagiere auf einem Display nach erfolgtem Enrollment sowie bei der Löschung der Smart Cards nach dem Boarding.

Der EDSB hat in seinem Schreiben vom 22. Dezember 2004 den Projektverantwortlichen entsprechende Anpassungsvorschläge schriftlich unterbreitet. *Die Projektleitung hatte bereits am Tag der Sachverhaltsabklärung auf ein erstes mündliches Feedback des EDSB reagiert* und die Plakate am Check-In Schalter dahingehend geändert, dass die Freiwilligkeit der Teilnahme am Pilotprojekt sowie das Erfordernis des Opting-in besser zur Geltung gelangt. Mit Schreiben (Email) vom 24. Dezember 2004 bestätigt die Projektleitung die Implementierung einer neuen Lösung für das sofortige Löschen der Smart Card nach dem Boarding. Die Smart Cards werden nun neu nach erfolgreicher Verifikation am Gate automatisch gelöscht. Die Löschung wird dem Passagier auf einem Display sogleich bestätigt. Ausserdem hat der Passagier die Möglichkeit, die Löschung mit nochmaligem Einleseversuch zu überprüfen. Auch wurde die Schrift auf dem Display am Check-In Schalter verkleinert. Für die definitive Umsetzung von Secure Check zieht die Projektleitung andere Lösungen (z.B. Schutzschilder) in Erwägung.

Der EDSB kommt nach der durchgeführten Kontrolle zu einer **positiven Gesamtbeurteilung**. Gestützt auf diese Anpassungen sowie gestützt auf die eingereichten Unterlagen und die Sachverhaltsabklärung vor Ort kommt der EDSB zum Schluss, dass die Bearbeitung biometrischer Daten von Flugpassagieren im Rahmen des Pilotprojektes Secure **grundsätzlich datenschutzkonform** erfolgt. Zu begrüßen ist insbesondere die *dezentrale Speicherung* der Daten sowie der Umstand, dass *keine Rohdaten*, sondern die Templates auf dem Speichermedium (Smart Card) festgehalten werden.

7.2 Bezüglich der Umsetzung des Pilotprojektes in ein Definitivum

Der EDSB anerkennt, dass die im Rahmen des Pilotprojektes getroffenen Massnahmen für eine Umsetzung in ein Definitivum in die richtige Richtung weisen. Dennoch sollten aus Sicht des EDSB die in diesem Schlussbericht unter Ziff. 6 „Datenschutzrechtliche Beurteilung“ aufgeführten Überlegungen im Sinne von „Optimierungsvorschlägen“ des EDSB von der Projektleitung bei der Umsetzung in ein Definitivum **mit berücksichtigt und umgesetzt** werden (es sei an dieser Stelle auf den Bericht verwiesen).

Insbesondere sollten aus Sicht des EDSB folgende Punkte von der Projektleitung bei der konkreten Umsetzung von Secure Check in ein Definitivum **eingehend geprüft werden**:

1. Sofern die Projektleitung zwischen den biometrischen Fingerabdrücken oder den Gesichtsbildern *zu wählen* hat, ist dasjenige Verfahren zu favorisieren, welches für die betroffenen Flugpassagiere mit der *geringsten Gefahr einer Persönlichkeitsbeeinträchtigung* verbunden ist.
2. Es ist eine *klare Trennung* zwischen Authentifizierungsmechanismen für Smart Cards/Lesegeräte und Verschlüsselungsalgorithmen für Datenübertragung/-speicherung zu treffen (vgl. Ziff. 6.8.2). Die Transparenz der Datenbearbeitung sollte durch eine *klarere Information der Betroffenen über alle Kategorien von bearbeiteten Daten* (Identität, Flug, Biometrie, Statistik, etc.) erhöht werden, und dies ab der Erhebung der Daten bis zur ihrer Vernichtung. *Besonders geachtet werden sollte auf die Datenlöschung*, die insbesondere

physikalisch, zeitgerecht (d.h. frühestmöglich) und flächendeckend (inkl. temporärer Dateien!) erfolgen muss (vgl. dazu auch die Bemerkungen in *Ziff. 6.8.2*). Die Projektleitung wird aufgefordert, diese Punkte bei einer definitiven Implementierung von Secure Check umzusetzen.

3. Die nun erstmalig erfolgte Erhebung biometrischer Daten weckt *neue Begehrlichkeiten von Seiten Dritter*, wie z.B. der Flughafenpolizei oder ausländischen Immigrationsbehörden. Die Projektleitung wird aufgefordert, sich dieser Begehrlichkeiten bei der definitiven Umsetzung des Projektes Secure Check *bewusst zu sein* und insbesondere keine biometrischen Daten an aussenstehende Dritte (wie Behörden) *ohne Vorliegen eines Rechtfertigungsgrundes* (wie z.B. eine gesetzliche Grundlage; vgl. Art. 13 Abs. 1 DSGVO) herauszugeben. Ferner weisen wir darauf hin, dass eine Abänderung des Projektes Secure Check in Richtung einer zentralen Speicherung der biometrischen Daten oder in Richtung einer Speicherung von Rohdaten eine *differenzierte datenschutzrechtliche Beurteilung* erfordert, welche vom vorliegenden Kontrollbericht nicht abgedeckt wird. Ebenso wäre die Zweckbindung des Projektes Secure Check neu zu *überdenken* und zu *definieren*, sollten die erhobenen biometrische Daten in einer späteren Phase an aussenstehende Behörden weiter geleitet werden (vgl. dazu auch die Bemerkungen in *Ziff. 6.6*).

8. Schlussfolgerung

8.1 Kontrolle des Einsatzes biometrischer Daten im Rahmen von Secure Check

Die Kontrolle hat dem EDSB einen vertieften Einblick und eine umfassende Überprüfung der effektiv vorgenommenen Bearbeitung biometrischer Daten im Rahmen des Pilotprojektes Secure Check erlaubt. Durch die Sachverhaltsabklärung vor Ort konnte der EDSB sofort mit Anpassungsvorschlägen die Datenbearbeitung optimieren und auf Schwachstellen aufmerksam machen.

Mit der durchgeführten Kontrolle konnte das im Schreiben vom 30. November 2004 gegenüber der Projektleitung angekündigte und verfolgte Ziel des EDSB klar erreicht werden. Die Kontrolle hatte zum Ziel, die Datenbearbeitung im Rahmen des Pilotprojektes im Hinblick auf eine allfällige spätere Umwandlung in ein Definitivum, in eine datenschutzkonforme Richtung zu lenken. Denn mit dem Pilotprojekt werden die Weichen für eine definitive Umsetzung des Projektes Secure Check gestellt, welches in Zukunft einer Vielzahl von Flugpassagieren auf dem Flughafen Zürich-Kloten zur Verfügung stehen soll. Da im Rahmen des Pilotprojektes erstmalig eine neue Technologie zur Anwendung gelangte (biometrische Verfahren), bei welcher sensible Personendaten bearbeitet werden, drängte sich die Sachverhaltsabklärung und Datenschutzprüfung bereits im Vorfeld der Implementierung des Pilotversuches auf. Einerseits konnte der EDSB mit Anpassungsvorschlägen in die datenschutzkonforme Ausgestaltung von Secure Check einwirken und andererseits mit diesen Anpassungsvorschlägen und weiteren Überlegungen die allfällige Umsetzung in ein Definitivum mitgestalten und optimieren.

8.2 Weiteres Vorgehen

Die Entwicklungen im Bereich biometrischer Verfahren sind in vollem Gange (vgl. z.B. die geplante Einführung biometrischer Daten im Schweizer Pass; Zugangskontrolle zu Gebäuden mittels biometrischer Merkmale; Sicherung von technischen Geräten durch Verifikation mit biometrischen Fingerabdrücken etc.). Es ist Aufgabe des EDSB dafür zu sorgen, dass datenschutzrechtliche Überlegungen in geplante oder vollzogene Anwendungen biometrischer Verfahren einfließen und damit eine datenschutzkonforme Handhabung und Umsetzung biometrischer Systeme gewährleistet werden kann.

Aus diesen Gründen besteht aus Sicht des EDSB ein grundsätzliches Interesse daran, die Öffentlichkeit für die Datenbearbeitung im Bereich der Biometrie zu sensibilisieren und sie insbesondere über die erfolgte Datenschutzkontrolle im Rahmen des Pilotprojektes Secure Check am Flughafen Zürich-Kloten und über die diesbezüglichen Ergebnisse zu informieren. Der EDSB wird daher gestützt auf Art. 30 Abs. 2 DSG den vorliegenden Schlussbericht in angepasster Version (und bezüglich Namensnennungen anonymisiert) der **Öffentlichkeit zugänglich machen** und auf seiner **Website (www.edsb.ch) publizieren**. Selbstverständlich erfolgt die Publikation unter dem Vorbehalt, dass aus Sicht der Projektleitung von Checkport resp. von Swissport keine vertraulichen Daten, welche Geschäftsgeheimnisse offenbaren oder die Konkurrenzfähigkeit beeinflussen könnten, der Öffentlichkeit bekannt gegeben werden. Die Projektleitung von Secure Check wird daher aufgefordert, den Schlussbericht auf vertrauliche Inhalte hin zu überprüfen und dem EDSB **mit Frist von 30 Tagen** diesbezüglich schriftliche Rückmeldung zu erstatten.

Der vorliegende Schlussbericht enthält eine Reihe von Feststellungen und Optimierungsvorschlägen, welche von der Projektleitung grösstenteils bereits nach dem ersten mündlichen Feedback des EDSB umgesetzt wurde, sowie eine Reihe weiterführender und insbesondere grundsätzlicher Überlegungen und Anregungen zum Einsatz biometrischer Verfahren im Privatbereich. Diese grundsätzlichen Überlegungen und Anregungen sollten von der Projektleitung zur Kenntnis genommen resp. im Hinblick auf die definitive Überführung des Pilotprojektes in ein Definitivum einer eingehenden Überprüfung unterzogen werden. Die Projektleitung von Secure Check wird daher aufgefordert, vorliegenden Schlussbericht zur Kenntnis zu nehmen und dem EDSB **mit Frist von 30 Tagen** zu den Anmerkungen zum Pilotprojekt resp. zu den Grundsatzüberlegungen und Vorschlägen im Hinblick auf die definitive Umsetzung des Projektes (vgl. Ziff. 6 und 7) **eine Stellungnahme zuhanden des EDSB** abzugeben.

Die Projektleitung von Secure Check wird ferner gebeten, den EDSB nach erfolgter interner Analyse und Auswertung des Projektes **innerhalb der nächsten 30 Tage** darüber zu informieren, wie die Projektverantwortlichen die Erreichung der gesetzten Ziele und die Akzeptanz bei den Fluggästen nach Beendigung des Pilotprojektes bewerten und welche **eigene Schlussbilanz die Projektleitung** aus dem abgeschlossenen Pilotprojekt zieht.

Bern, den 6. Juni 2005

**EIDGENÖSSISCHER
DATENSCHUTZBEAUFTRAGTER**
Der Beauftragte:

Hanspeter Thür

Anhang vom 24. Oktober 2005 zum Schlussbericht

1. Vorbemerkung

Der vorliegende Anhang widerspiegelt die Stellungnahme von Seiten Checkport auf den Schlussbericht des EDSB vom 6. Juni 2005. Die Stellungnahme wurde dem EDSB fristgerecht innerhalb von 30 Tagen am 28. Juni 2005 eingereicht. Der Anhang bildet integralen Bestandteil des Schlussberichtes.

Der EDSB hat am 24. Oktober 2005 die Datenschutzkontrolle gemäss Art. 29 DSG über den Einsatz von Biometrie beim Check-In und Boarding im Rahmen des Pilotprojektes Secure Check für abgeschlossen erklärt.

2. Stellungnahme von Checkport

Zu Ziff. 6.1.2 des Schlussberichtes

Bezüglich der geäusserten Befürchtung des EDSB einer Erfassung von Rohdaten betont die Projektleitung, dass weder im Pilotprojekt, noch in Zukunft bei der definitiven Einführung von Secure Check Rohdaten auf die Smart Card übertragen werden.

Ferner macht die Projektleitung darauf aufmerksam, dass ein Abbild des Reisedokuments (hier geht es vor allem um das Abbild des auf der Passseite enthaltenen Gesichtsbildes und der Unterschrift) für 48 Stunden zentral gespeichert werde. Dies erfolge zur Absicherung der Fluggesellschaft im Falle des Verlustes des Reisedokuments durch den Passagier. Ein Zugriff auf diese Daten durch aussenstehende Dritte sei nicht möglich.

Zu Ziff. 6.4.2 des Schlussberichtes

Die Projektleitung räumt ein, dass dieser Punkt zur Erhöhung der Transparenz in einem nächsten Schritt verbessert werden müsse.

Zu Ziff. 6.7.2 des Schlussberichtes

Aus Sicht der Projektleitung muss die FAR so Nahe wie möglich bei Null sein. Dies werde durch Eingehen von Konzessionen bei der FRR erreicht. Die Projektleitung weist aber darauf hin, dass bei einer False Rejection alternativ auf einen manuellen Prozess zur Verifikation zurückgegriffen werden kann. Es dürfe aber aus Sicherheitsgründen unter keinen Umständen die falsche Person in das Flugzeug gelangen.

Der Einsatz einer multimodalen Authentifizierung für einen Prozess, der alternativ auch manuell durchgeführt werden kann, wird von der Projektleitung im Moment als nicht verhältnismässig erachtet. Als Begründung wird darauf hingewiesen, dass die errechneten Werte für die FRR im Pilotprojekt bei 4% lagen und bei der FAR nahe bei Null. Durch den Einsatz von 2 Templates von verschiedenen Fingern konnte die FRR über den ganzen Prozess auf 0.16% verringert werden.

Bezüglich der Anregung des EDSB, ein äquivalentes Erkennungssystem für Personen, deren biometrische Merkmale nicht eingelesen werden können (z.B. bei fehlenden Gliedmassen; aufgrund des Alters), zu planen, macht die Projektleitung geltend, dass Secure Check für die Passagiere freiwillig sei und alternativ weiterhin ein manueller Prozess beim Check-In und Boarding angeboten werde. Aus diesem Grunde könne die Projektleitung technisch nicht

garantieren, dass alle Passagiere das neue System Secure Check auch tatsächlich benutzen können.

Zu Ziff. 6.8.2 des Schlussberichtes

Bezüglich der Anregung des EDSB nach einem verlässlichen Authentifizierungsmechanismus zwischen den Smart Cards und den Lese-/Schreibgeräten weist die Projektleitung darauf hin, dass ein solcher Authentifizierungsmechanismus basierend auf verschiedenen Schlüsseln für den Schreib- und Lesezugriff bereits eingebaut sei. Eine Verschlüsselung des Datenverkehrs zwischen den Geräten mache Sinn.

Bezüglich der Gewährleistung der physikalischen und logischen Löschung der Daten auf der Smart Card verweist die Projektleitung auf Aussagen des Herstellers. Gemäss dieser Auskunft werden bei jedem Beschreiben der Daten auf der Smart Card alle Daten physisch überschrieben. Durch die Struktur des Schreibens sei eine nur logische Löschung gar nicht möglich. Eine Löschung sei nur durch Überschreiben der Daten mit Leerzeichen möglich.

Zu Ziff. 7.2 des Schlussberichtes

Die vom EDSB aufgeführten Punkte 1 und 2 sind gemäss der Projektleitung von den oben aufgeführten Antworten abgedeckt.

In Bezug auf Punkt 3 ist sich die Projektleitung bewusst, dass mit der Erfassung biometrischer Daten beim Check-In und Boarding neue Begehrlichkeiten von Behörden aufkommen könnten. Die Projektleitung versichert, dass sie allfällige Anfragen in jedem Einzelfall überprüfen und gemäss den geltenden Bestimmungen handhaben werde. Bei einer Veränderung der Sachlage des Systems Secure Check, wie sie vom EDSB unter Punkt 3 angesprochen wird (d.h. allfällige zentrale Speicherung der Daten oder Speicherung von Rohdaten), versichert die Projektleitung, dass der EDSB in diesem Falle informiert werde und die Sichtweise des EDSB angehört wird.

Der EDSB nimmt diese Stellungnahmen von Checkport zur Kenntnis und hat keine Bemerkungen dazu.

Bern, den 24. Oktober 2005

**EIDGENÖSSISCHER
DATENSCHUTZBEAUFTRAGTER**
Der Beauftragte:

Hanspeter Thür