Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Schlussbericht

betreffend die Kontrolle des

Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)

in Sachen SwissPass

des Verbands öffentlicher Verkehr (VöV) und der SBB AG

vom 4. Januar 2016

gemäss

Artikel 27 des Bundesgesetzes vom 19. Juni 1992

über den Datenschutz (DSG; SR 235.1)

Feldeggweg 1, 3003 Bern
Tel. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

Inhaltsverzeichnis

1. Einführung

1.1. Vorgeschichte

In einer gemeinsamen Medienmitteilung gaben der VöV und die SBB am 22. Februar 2013 die Einführung der öV-Karte bekannt. Darauf verlangte der EDÖB vom VöV und der SBB mit Schreiben vom 12. März 2013 verschiedene Präzisierungen, welche dem EDÖB mit Schreiben vom 23. April 2013 geliefert wurden. Zudem präsentierten der VöV und die SBB am 8. Juli 2013 dem EDÖB das Projekt öV-Karte.

Am 10. März 2014 fand ein allgemeiner Informationsaustausch zwischen Herrn Andreas Meyer, CEO der SBB, und Herrn Hanspeter Thür, damaliger Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, statt. Dabei betonte Herr Meyer, dass die Einhaltung des Datenschutzes für die SBB ein wichtiges Anliegen darstelle.

Ebenfalls in Zusammenhang mit dem Projekt öV-Karte prüften der VöV und seine Mitglieder, in welchen Fällen die konzessionierten Transportunternehmen bei der Bearbeitung von Kunden- und Kontrolldaten als private Unternehmen oder als Bundesorgane gemäss Art. 54 Abs. 1 PBG i.V.m. dem DSG gelten würden. Diesbezüglich fand am 8. Mai 2014 eine Sitzung zwischen dem VöV, einzelnen Transportunternehmen und dem EDÖB statt. Der VöV resp. ch-direct (= Direkter Verkehr Schweiz) unterbreiteten darauf dem EDÖB am 2. Juli 2014 eine schriftliche Analyse der vorgenannten Frage. Der EDÖB nahm mit Schreiben vom 25. August 2014 dazu Stellung.

Im Februar 2015 kontaktierte die SBB den EDÖB um ihm die geplante Einführung des SwissPass zu präsentieren. Diese Präsentation durch die SBB und den VöV fand am 3. März 2015 statt. Dabei handelte es sich um eine reine Vororientierung des EDÖB, ohne dass dieser eine vertiefte Analyse oder eine Sachverhaltsabklärung als Aufsichtsbehörde machte. Am 10. März 2015, somit eine Woche später, orientierten die SBB und ch-direct die Medien über die Einführung des SwissPass. Auf Wunsch der SBB bestätigte der EDÖB mit Schreiben vom 6. Juli 2015, dass ihm der SwissPass im März 2015 präsentiert worden war. Der EDÖB wies aber darauf hin, dass es sich dabei um eine reine Vorinformation handelte, und dass der EDÖB keine vertiefte Abklärung und insbesondere keine Sachverhaltsabklärung durchgeführt habe.

1.2. Anlass und Zweck

Seit dem 1. August 2015 werden alle General- und Halbtaxabonnemente laufend durch den SwissPass ersetzt. Zusätzlich bietet der SwissPass Zugang zu Partnerdiensten (wie Mobility Carsharing, Publibike, SchweizMobil, einige Skigebiete). In den Medien wird immer wieder über den SwissPass berichtet, wobei vor allem die Befürchtung ausgesprochen wird, dass aus den Kontrolldaten Bewegungsprofile erstellt werden könnten. Der EDÖB hat viele Anfragen besorgter Bürger und Medien erhalten und musste oft klarstellen, dass er das Projekt weder genehmigt noch bewilligt hat. Auf Bundesebene gab es zudem im Parlament verschiedene Vorstösse betreffend den SwissPass. Mit dem SwissPass samt Partnerdiensten werden die Personendaten einer sehr grossen Anzahl Personen bearbeitet. In diesem Zusammenhang stellen sich auch viele datenschutzrechtliche Fragen.

Aus diesen Gründen entschied der EDÖB eine Sachverhaltsabklärung betreffend den SwissPass und die damit verbundenen Datenbearbeitungen durchzuführen.
Zweck dieser Sachverhaltsabklärung ist es zu prüfen, ob mit dem SwissPass, insbesondere mit der Kontrolldatenbank, die datenschutzrechtlichen Voraussetzungen eingehalten werden.

1.3. Modalitäten

Der EDÖB führt seine Kontrollen gestützt auf das DSG als unabhängige Datenschutzaufsichtsbehörde durch (vgl. Art. 27 DSG). Bei der Abklärung kann er Akten herausverlangen, Auskünfte einholen und sich Datenbearbeitungen vorführen lassen. Die Bundesorgane müssen an der Feststellung des Sachverhaltes mitwirken. Gemäss Personenbeförderungsgesetz (PBG; SR 745.1) unterstehen die Unternehmen für ihre konzessionierten und bewilligten Tätigkeiten einerseits, sowie wenn sie privatrechtlich handeln andererseits, dem DSG. Die Aufsicht unterliegt dabei dem EDÖB und richtet sich nach Art. 27 DSG (vgl. 54 PBG).

1.4. Gesetzliche Grundlagen

Es gelten folgende gesetzliche Grundlagen:

- Art. 54 PBG (SR 745.1);
- DSG (SR 235.1; insb. Art. 4 ff., 13 ff., 27 und 29)
- VDSG (Verordnung zum DSG; SR 235.11)

1.5. Chronologie

14.09.2015	Ankündigung der Sachverhaltsabklärung an VöV und Angabe von zwei Daten für die Kontrolle vor Ort;
02.10.2015	Mail VöV an EDÖB um das Datum der Kontrolle vor Ort mitzuteilen;
15.10.2015	Antwortmail EDÖB an VöV;
16.10.2015	Versand per Mail und Post der Unterlagen durch VöV
ab 16.10.15	Prüfung durch den EDÖB der erhaltenen Antworten und der vorhandenen Dokumentation;
20.10.2015	Kontrolle vor Ort;
21.10.2015	Mail EDÖB an VöV mit Zusatzfragen und Herausverlangen zusätzlicher Unterlagen
30.10.2015	Antwort VöV auf Schreiben EDÖB vom 21.10.2015
21.10.-12.11.15	Verfassen der Sachverhaltsfeststellung
12.-27.11.2015	Konsultation des VöV zur Sachverhaltsfeststellung;
27.11.2015	Mitteilung der Ergänzungen und Änderungswünsche zur Sachverhaltsfeststellung durch den VöV;
04.01.2016	Versand des definitiven Kontrollberichts des EDÖB an den VöV und die SBB

1.6. Anwesende Personen

Bei der Kontrolle vor Ort vom 20. Oktober 2015 waren folgende Personen anwesend;

VöV / ch-direct

- A
- B

SBB:

- C
- D
- E
- F

EDÖB:

- G
- H
- I

2. Feststellungen

2.1. Allgemeines

2.1.1 Karte SwissPass

Der SwissPass wird in Form einer Plastikkarte im Kreditkartenformat ausgegeben und ist in der Regel fünf Jahre gültig. Auf der Karte ist kein Hinweis zur gekauften Leistung (Art und Gültigkeitsdatum) aufgedruckt. Ersichtlich sind auf der Vorderseite: Kundenfoto, Titel (falls angegeben), Name, Vorname, Geburtsdatum, Geschlecht, Grundkartennummer, CKM (= eindeutige Kundenidentifikationsnummer) und auf der Rückseite: RFID Logo, öV-Piktogramme, QR-Code (für Kontrolle und Mehrwerte), Barcode (für Kontrolle und Mehrwerte) und die Kartennummer.

Die SwissPass Karte ist mit zwei RFID-Chipmodulen ausgestattet, die auf Impuls eines entsprechenden Lesegerätes ihre gespeicherten Daten an dieses übertragen. Die beiden Chipmodule unterstützen jeweils unterschiedliche Anwendungsbereiche. Kernanwendung von Chip A ist die Gültigkeitskontrolle von öV-Leistungen (darunter insbesondere GA und Halbtaxabo). Mit Chip B wurde die in Skigebieten als Skipass verwendete Technologie adaptiert und dient für die Anwendung von Partnerdienstleistungen. Die Datenübertragung erfolgt berührungslos. Die Auslesedistanz für Chip A beträgt 3 cm, diejenige für Chip B 30 cm. In Chip A wird als einziges Personendatum eine technische Kennnummer (MedienID) gespeichert. Die MedienID ist in einem vom öV signierten elektronischen Zertifikat eingebettet. Der SwissPass kann, beispielsweise bei Verlust oder Diebstahl, gesperrt werden. Der SwissPass kann auch ohne öV-Leistung, d.h. für Partnerdienstleistungen, gekauft werden (= SwissPass Plus) (vgl. Ziff. 2.5).

2.1.2 Träger des SwissPass

In seiner Antwort vom 16. Oktober 2015 hielt der VöV Folgendes fest: „*Bei den im Rahmen des SwissPass bearbeiteten Kunden- und Leistungsdaten handelt es sich um Daten des Direkten Verkehrs (DV). Inhaberin dieser DV-Daten ist die Gesamtheit der am DV beteiligten Transportunternehmen [TU], welche eine einfache Gesellschaft darstellt. Weil eine einfache Gesellschaft keine eigene Rechtspersönlichkeit aufweist, also nicht Inhaberin von Rechten und Pflichten sein kann, ist nicht der DV Inhaber der Daten, sondern jedes einzelne am DV beteiligte Transportunternehmen ist Mitinhaberin. Zuständig für den Entscheid, was mit den Daten, welche durch den Verkauf der DV-Abonnemente (HTA, GA, Gleis 7, Junior- und Enkelkarten, Streckenabonnemente oder der SwissPass als Trägermedium) erhoben werden, geschieht, sind die verschiedenen Gremien des DV.*“

Die SBB wurde mit der Marktbearbeitung von ch-direct (darunter auch SwissPass) sowie mit dem Betrieb der zentralen Basisvertriebssysteme des DV (darunter auch die zentrale Kunden- und Abonnementsdatenbank [KUBA] und die Kontrolldatenbank) beauftragt.

2.2. Beschreibung des Prozesses

2.2.1 Kauf des SwissPass

Der SwissPass kann an jeder bedienten Verkaufsstelle des öV gekauft werden. Bei der Bestellung des SwissPass übermittelt der Kunde die benötigten Personendaten, nämlich Name, Vorname, Adresse, Geburtsdatum, E-Mail-Adresse (fakultativ), Telefonnummer (fakultativ), Foto. Diese Kundendaten werden unmittelbar nach dem Kauf in die zentrale Kunden- und Abonnementsdatenbank (KUBA) eingetragen. Gemäss den AGB können diese zu Marketingzwecken benutzt werden. Der Kunde kann jederzeit formlos festhalten, dass seine Daten nicht zu Marketingzwecken benutzt werden sollen (vgl. Ziff. 2.3). So kann das Opt-out direkt am Schalter (an jeder bedienten Verkaufsstelle) oder telefonisch oder per Mail an den SBB Contact Center geltend gemacht werden. Auf der Online-Plattform von SwissPass (www.swisspass.ch) kann sich der Kunde oder die Kundin einloggen und das Opt-out für den Erhalt von SwissPass-Newslettern anbringen.

2.2.2 Kontrollvorgang in den Transportunternehmen

Bei den Kontrollen benützt das Zugbegleitpersonal ein Lesegerät. Dieses enthält eine lokale Kopie der in KUBA enthaltenen Abonnementsdaten (Teilsystem KUBA). Diese Kopie wird in regelmässigen Abständen aktualisiert (bei der SBB alle 5 Minuten).

Das Zugbegleitpersonal identifiziert sich auf dem Lesegerät mittels Benutzernamen und Passwort. Gleichzeitig gibt es an, in welchem Zug und in welcher Klasse (1. oder 2. Klasse) er/sie sich befindet.

Beim Kontrollvorgang legt das Zugbegleitpersonal das Lesegerät auf den SwissPass um diesen zu scannen. Dabei liest das Lesegerät die auf dem RFID-Chip A gespeicherte MedienID und referenziert diese auf die im Lesegerät lokal gespeicherten abonnierten Leistungen. Wenn eine Übereinstimmung gefunden wurde, werden Name, Vorname, Geburtsdatum, Geschlecht, Kundennummer, sowie Art des Abonnements und dessen Gültigkeit (gültig, teilgültig, ungültig) auf dem Bildschirm des Lesegerätes angezeigt. Ist ein Abonnement gültig, erscheint das Wort auf grünem Hintergrund, ist es ungültig, auf rotem Hintergrund.

Wenn das Zugbegleitpersonal einen Zweifel zur Identität der kontrollierten Person hat (das auf der Karte aufgedruckte Foto hat eine tiefe Auflösung), kann es online auf die Datenbank zugreifen und das Foto auf sein Lesegerät laden (= Kundensuche). Gleichzeitig wird auch die letzte durch das Transportunternehmen durchgeführte Kontrolle mit Datum, Zeit und Angabe des Transportunternehmens auf dem Bildschirm angezeigt. Diese Angabe wird benötigt um allfällige Missbräuche zu verhindern (wenn beispielsweise zwei Personen im gleichen Zug dieselbe Karte benützen). Kontrollen, die durch andere Transportunternehmen erfolgten, werden nicht aufgezeigt. Auf dem Bildschirm des Lesegeräts wird zudem speziell signalisiert, wenn ein SwissPass innerhalb von [redacted][1] Minuten zum zweiten Mal kontrolliert wird.

Die Kontrolldaten werden anschliessend in die Kontrolldatenbank hochgeladen und dort während 90 Tagen aufbewahrt (vgl. Ziff. 2.4 unten).

[1] Die Schwärzung erfolgt aus Sicherheitsgründen

2.2.3 Information der Kunden

Die Kunden werden in den AGB für den Erwerb und die Nutzung des GA bzw. Halbtaxabonnements sowie im Personentarif T600 über die gemachten Datenbearbeitungen informiert.

Auskunftsgesuche sind schriftlich mit einer Kopie eines amtlichen Ausweises einzureichen und werden anschliessend gemäss internem Prozess bearbeitet. In seinem Schreiben vom 16. Oktober 2015 hielt der VöV fest, dass zurzeit ein Kundenmaster erarbeitet werde, der die Beantwortung der Einsichtsgesuche erleichtern werde.

2.3. Kundendaten (KUBA)

Die Kunden- und Leistungs- resp. Abonnementsdaten werden in der zentralen Kunden- und Abonnementsdatenbank (KUBA) eingetragen (vgl. Ziff. 2.2.1 oben). Die Vertragsdaten werden in SAP CRM gespeichert. Die SBB wurde damit beauftragt, diese Datenbank zu führen und ist auch für die Behandlung von Auskunftsgesuchen zuständig. Zu den Kundendaten zählen: Name, Vorname, Adresse, Geburtsdatum, E-Mail-Adresse, Telefonnummer, Foto und demografische Daten (Alterssegment, Wohnkanton, etc.). Abonnements- bzw. Leistungsdaten enthalten Informationen über die gekaufte Leistung wie Artikel- und Vertragsnummer, Artikelbezeichnung, Vertragsgültigkeit, Preis. Die Kunden- und Leistungsdaten dienen dazu, die vom Kunden beanspruchten Leistungen (GA, Halbtax, etc.) zu erbringen. Kundendaten werden nur dann gespeichert, wenn der Kunde/die Kundin auch ein Abonnement kauft bzw. einen Vertrag abschliesst (z.B. GA oder Halbtaxabo). Gemäss Vertrag sichert die SBB als Mandatsträgerin den am direkten Verkehr (DV) Teilnehmenden für den Verkauf von DV-Produkten den ungehinderten, zeitgemässen und kundengerechten Zugriff auf die zentralen Verkaufsdaten in KUBA zu.

Die Kunden- und Leistungsdaten werden, sofern kein ausdrücklicher Einwand des Kunden resp. der Kundin erhoben wurde, auch zu Marketingzwecken verwendet. Die Verwendung zu Marketingzwecken und die Möglichkeit des Opt-out sind in den AGB zum GA sowie in den AGB zum Halbtaxabonnement aufgeführt. Bei der Kontrolle vor Ort wies die SBB den EDÖB auf dessen Frage darauf hin, dass die AGB neu formuliert würden. Grund sei die zu wenig klar umschriebene Möglichkeit des Opt-out der Verwendung der Daten zu Marketingzwecken. Mit Schreiben vom 30. Oktober 2015 schickte der VöV dem EDÖB die Entwürfe der neu formulierten AGB für GA und Halbtaxabonnemente. In den Entwürfen wird neu ausdrücklich erwähnt, wo das Opt-out geltend gemacht werden kann und auf Folgendes hingewiesen: „Nach einem Opt-out werden Sie nicht weiter über Marketingmassnahmen kontaktiert, Ihre Daten verbleiben jedoch weiterhin in unseren Datenbanken, sofern Sie über eine oder mehrere gültige Leistungen (Halbtax, GA, Partnerleistungen etc.) verfügen.“ Trifft ein Opt-out-Gesuch bei der SBB ein, wird dies im System speziell vermerkt, damit die Daten der betroffenen Person nicht mehr personenbezogen zu Marketingzwecken benutzt werden. Ohne Opt-out wird ein Kunde/eine Kundin pro Jahr maximal 10 Mal zu Marketingzwecken kontaktiert. Die SBB ist als Mandatsträgerin prioritär befugt, die Daten zu Marketingzwecken zu bearbeiten. Die anderen Transportunternehmen und die Verbunde müssen sich, wenn sie Daten zu Marketingzwecken benutzen wollen, an die SBB wenden, welche ihnen via eine gesicherte FTP-Plattform die ausgewählten Adressen für die Werbekampagne schicken. Damit wird sichergestellt, dass ein Kunde/eine Kundin maximal 10 Mal Werbung erhält. Zudem wurde ein internes Regelwerk zur Nutzung von Kundendaten der DV-Abonnemente zur Marketingzwecken (kurz Regelwerk Datennutzung) erstellt.

Die Kundendaten werden, sofern keine gültige Leistung mehr besteht, 5 Jahre nach der letzten Mutation automatisch gelöscht. Abonnements- oder Leistungsdaten werden 18 Monate nach Ablauf gelöscht, sofern während dieser Dauer keine weiteren Leistungen gekauft werden. NewAboPOS (nachfolgend NAP) ist ein Verkaufsarbeitsplatz (User Interface) und keine Datenbanklösung. NAP bezieht sämtliche Daten aus der zentralen Abonnements- und Kundendatenbank bzw. aus SAP CRM. Wird ein Kunden- oder Leistungsdatensatz gelöscht, so ist dieser auch nicht mehr über NAP abrufbar. Es wird angestrebt, die Anzeige von Partnerdienstleistungen im NAP auf bis zu 3 Monate nach Ablauf der Leistung zu senken.

Die bei KUBA angewandten Massnahmen zur Datensicherheit entsprechen den für Personendaten geltenden technischen und organisatorischen Standards.

2.4. Kontrolldaten

Die Kontrolldaten werden in einer separaten Datenbank während 90 Tagen aufbewahrt. Dabei handelt es sich um Daten, die im Rahmen einer elektronischen Kontrolle eines SwissPass registriert werden. Wenn das Zugbegleitpersonal mit seinem Lesegerät einen SwissPass kontrolliert, wird ein Datensatz mit folgenden Informationen online übermittelt und in die Kontrolldatenbank gespeichert: Zug-/Kursnummer (nur zum Teil), Uhrzeit, Personalnummer des kontrollierenden Mitarbeitenden, Gerätenummer (IMEI) des Kontrollgeräts, Typ der kontrollierten Leistung (HTA oder GA), Klasse der kontrollierten Leistung (1./2. Klasse), Kontrollergebnis (gültig, teilgültig, ungültig), Verknüpfung zur Kunden-, Grundkarten- und SwissPass-Ausweisnummer sowie Kontrollreferenznummer. Im Zeitpunkt der Kontrolle vor Ort zählte die Kontrolldatenbank 3,2 Mio Einträge, wobei damals 300‘000 SwissPass-Karten ausgestellt worden waren. Es ist damit zu rechnen, dass in Zukunft rund 3 bis 4 Mio SwissPass-Karten benutzt werden. Seit dem 5. Oktober 2015 werden die Daten ab dem aktuellen Tag minus 90 Tage mittels eines Löschjobs täglich gelöscht.

Die Kontrolldaten werden weder zu Marketingzwecken bearbeitet noch an Dritte bekannt gegeben. Das Regelwerk Datennutzung (vgl. Ziff. 2.3 oben) hält zwar fest, dass Kontrolldaten in pseudonymisierter Form zu Analysezwecken verwendet würden. Allerdings wurde nach der Inkraftsetzung der seit dem 1. Juni 2015 geltenden Version des Regelwerks vom Mandatsträger entschieden, auf diese Analyseoptionen zu verzichten, da keine Rückschlüsse oder Erkenntnisse daraus in weiteren Aktivitäten (sei dies Marketing, Produktmanagement oder sonstige) verwendet werden könnten.

Gemäss Angaben des VöV und der SBB (Schreiben vom 16. Oktober 2015) dient die Kontrolldatenbank dazu, allfällige Kundenanliegen im Nachgang einer Reise zu beantworten (z.B. für Rückerstattungsanfragen oder auch Missbräuche). Bei der Kontrolle vor Ort hielt D fest, dass die Kontrolldaten auch dazu dienen würden feststellen zu können ob Personen, die aufgrund eines Unfalls nicht reisen konnten und eine Rückerstattung geltend machten, tatsächlich nicht gereist seien. B hielt fest, dass die Kontrolldaten allenfalls für die Entwicklung neuer Produkte in den nächsten Jahren nützlich sein könnten. In seinem Schreiben vom 30. Oktober 2015 führte der VöV folgende Gründe für die Aufbewahrung der Kontrolldaten auf:

- *Kontrolldaten werden im Falle einer „Reise ohne gültigen Fahrausweis" oder „Reise mit teilgültigem Fahrausweis" sowie bei Missbrauchsverdacht nicht in der RogF-Datenbank gespeichert. Die Kontrolldaten sind lediglich in der Ihnen vorgeführten Kontrolldatenbank ersichtlich.*
- *Erhöhung der Betriebssicherheit seitens IT*

- *im Falle von Systemausfällen/Betriebsunterbrüchen oder Fehleranalysen sind detaillierte Abklärungen nötig, was ein Zugriff auf die Kontrolldaten in der Kontrolldatenbank erfordert.*
  Beispiele:
  - *wenn es Probleme beim Einlesen einer Karte gibt, benötigen wir Zugriff auf die Kontrolldaten um nachvollziehen zu können, ob das Problem bei der Karte oder beim Gerät liegt;*
  - *Es gibt z.B. im Moment einen Fehler, bei welchem Leistungen beim Kontrollgerät als „hinterlegt" angezeigt werden, obwohl die Hinterlegung beendet ist. In diesem Fall sind wir für die Nachvollziehbarkeit des Fehlers auf den Zugriff auf die Kontrolldatenbank angewiesen[2];*
  - *Analyse von Systemausfällen und Betriebsunterbrüchen ~ dies betrifft nicht nur die SBB, sondern auch andere Transportunternehmen (z.B. Synchronisationsprobleme bei Kontrollgeräten von PostAuto).*
- *Gemäss Tarif T600.9 können Billette bis ein Jahr nach Gültigkeitsdauer erstattet werden. Der Beweis der Nichtbenützung des Billetts liegt beim Kunden. Die Kontrolldaten unterstützen die Transportunternehmen bei der Überprüfung einer Nichtbenützung und beim Entscheid einer allfälligen Erstattung als Beweisfunktion. Gründe für solche Erstattungen können folgende sein: Reiseunfähigkeit, Betriebsunterbrüche, Rückwirkende Kündigung/Annullation des Abonnements.*
- *Damit genügend Zeit für Abklärungen bei Kunden und den Transportunternehmen bleibt, werden die Kontrolldaten für 90 Tage aufbewahrt. Denn IT-seitige Abklärungen können sich aufgrund der Anzahl betroffenen Kunden, des Fehlerbildes und der nötigen Korrekturen in die Länge ziehen. Ebenfalls ist zu berücksichtigen, dass sich Kunden nicht unmittelbar nach der Fahrt nach Reiseunfähigkeit bei den Transportunternehmen melden, um eine Erstattung ihrer Tickets/Abonnemente in die Wege zu leiten.*
- *Wie am Treffen bereits aufgezeigt, sind die Kontrolldaten verschlüsselt abgespeichert und es hat nur ein kleiner Kreis von Anwendern Zugriff auf die Kontrolldaten.*

Der Zugriff auf die Kontrolldatenbank ist beschränkt. C für die Anwendung Kontrollservice, sowie das Entwicklungsteam (im Zeitpunkt der Sachverhaltsabklärung aus 7 Personen bestehend) können auf die Kontrolldatenbank mit Lese- und Schreibberechtigung zugreifen. Die in der Kontrolldatenbank nötigen Datenbearbeitungen erfolgen auf Anfrage von D, sowie von auf E. Seit der Einführung des SwissPass und bis zum Zeitpunkt der Kontrolle vor Ort waren einzig zwei Suchaktionen, beide in Zusammenhang mit bei der SBB eingereichten Auskunftsgesuchen, erfolgt. Gemäss Schreiben vom 16. Oktober 2015 gibt es zudem Mitarbeiter bei den Transportunternehmen, welche mit einem Lesezugriff auf SAP BO zugreifen um Reportings zu machen (z.B. wie viele Belege „SwissPass vergessen" ausgestellt wurden).

2.5. Andere Daten

Für Leistungen ausserhalb des öV-Sortiments (so genannte Partnerdienstleistungen) wird der RFID-Chip B (ISO 15693) auf dem SwissPass eingesetzt (vgl. Ziff. 2.1.1 oben). Mit jedem Partnerdienst werden die Einzelheiten der Zusammenarbeit und der Datenbearbeitungen jeweils separat vertraglich geregelt. Die Partnerdienstleistungen müssen von den jeweiligen Leistungsanbietern (SwissPass – Partner) auf Chip B referenziert resp., was die Skidaten betrifft, geladen werden. Der Zugriff erfolgt via einen Schnittstellenzugang SOAP-Schnittstelle.

[2] Gemäss VöV (02.02.16) trifft dieses Beispiel in der Kategorie Erhöhung der Betriebssicherheit seitens IT nicht mehr zu.

Weder die SBB noch die anderen konzessionierten Transportunternehmen haben einen Zugriff auf diesen Chip B. Transportunternehmen wie Bergbahnen können den Chip B als Träger für Skileistungen mitnutzen. Die SBB erhält vom Kartenproduzenten lediglich die UID des Chips übermittelt, hat aber keinen Einblick in den Chip. In der Verkaufsapplikation ist jedoch ersichtlich, welche Leistungen der Kunde beim Partnerdienst gekauft hat, um die Kunden korrekt zu beraten (z.B. Ersatz einer Karte, Anlaufstellen für Support). Die SwissPass Plus-Leistungsdaten (d.h. der Partnerdienste) werden in der Kundenmehrwerte-Anwendung gehalten. Im Falle der Skiabos wird die UID als Unique Key in der Datenbank des jeweiligen Skigebietes abgelegt. Damit ist der Kunde/die Kundin beim Passieren des Drehkreuzes mit der Karte „verbunden“, was einen Zugriff ermöglicht.

Die Partnerdienste haben auf folgende Daten der „Ausweisverwaltung“ in KUBA Zugriff:

- Gültigkeit des SwissPass. Beim Zugriff müssen die SwissPass-Nr. und die Postleihzahl eingegeben werden.
- Kaufprozess: mit jedem Partnerdienst wird separat festgelegt, auf welche Daten dieser zugreifen kann. Dabei handelt es sich insbesondere um die Datenbank „Ausweisverwaltung“ für Kartendaten und um einige Attribute aus KUBA für Personendaten und Leistungen.
  Im Falle von Mobility sind dies Name, Vorname, Anrede, Geburtsdatum, PLZ und die Ausweis-Nummer, die für den Kaufprozess benötigt werden.
  Im Falle von Skidata erhalten die Verkaufsstellen (POS) nur die Information über die Leistung, d.h. ob der Kunde/die Kundin ein GA oder ein Halbtaxabo besitzt. Bei einem Online-Kauf eines Skitickets erfolgt der Prozess der Datenaufnahme analog Mobility. Bei den Skiregionen sind es für den Online-Kauf damit ebenfalls Name, Vorname, Anrede, Geburtsdatum, PLZ und die Ausweis-Nummer.
- Ersatzkarten: Die Partnerdienste erhalten Angaben über gesperrte oder ersetzte Karten je nach Vertrag im „Push-“ oder im „Pullverfahren“.

3. Rechtliche Beurteilung

3.1. Inhaber der Datensammlung

Am SwissPass sind alle Unternehmen beteiligt, die ebenfalls am DV teilnehmen. Folglich stellt sich die Frage, wer vorliegend Inhaber der Datensammlung ist.

Art. 3 Bst. i DSG definiert den Inhaber der Datensammlung wie folgt: private Personen oder Bundesorgane, die über den Zweck und den Inhalt der Datensammlung entscheiden. Dem Dateninhaber unterliegen gemäss Gesetz verschiedene Pflichten. So kann beim Dateninhaber unter anderem das Auskunftsrecht nach DSG geltend gemacht werden, weiter ist er für die Anmeldung der Datensammlungen und die Erfüllung der Informationspflichten verantwortlich (vgl. Art. 8 ff., 11a, 14 und 18a DSG).

Die Frage nach dem Inhaber der Datensammlung beurteilt sich nicht nach dem formalen, sondern nach den tatsächlichen Verhältnissen. Werden Daten im Auftragsverhältnis durch einen Dritten bearbeitet, kommen sowohl Auftraggeber als auch Auftragnehmer als Inhaber der Datensammlung in Betracht, je nachdem wer von beiden die Verantwortung für die Datenbearbeitung innehat, was gewöhnlich mit der Bereitstellung des Datenmaterials einhergeht. (vgl. Gabor P. Blechta in Maurer-Lambrou/Blechta, BSK Kommentar Datenschutzgesetz, 3. Auflage, Helbing Lichtenhahn Verlag, Art. 3, N. 87 f.). Nach der ratio

legis ist indes in erster Linie danach zu fragen, von wem man sinnvollerweise die Erfüllung der an die Inhaberschaft geknüpften Auskunfts- und Informationspflichten verlangen kann (Astrid Epiney/Daniela Nüesch in Handbücher für die Anwaltspraxis, Datenschutzrecht, Helbing Lichtenhahn Verlag, § 3 N. 57). Inhaber einer Datensammlung können auch mehrere Personen gemeinsam sein, wie z.B. die Gesellschafter einer einfachen Gesellschaft. Gemeinsame Inhaberschaft setzt allerdings voraus, dass die verschiedenen Personen voneinander wissen und einander die Ausübung ihrer jeweiligen Kontrolle gestatten (vgl. David Rosenthal, Handkommentar zum DSG, Zürich 2008, Art. 3, N 112).

Um den Dateninhaber bestimmen zu können, muss nachfolgend somit aufgrund der tatsächlichen Verhältnisse geprüft werden, wer über Zweck und Inhalt der Datensammlungen, in denen die SwissPass-Daten bearbeitet werden, entscheidet und von wem man sinnvollerweise die Erfüllung der an die Inhaberschaft geknüpften Auskunfts- und Informationspflichten verlangen kann.

Der VöV vertritt, wie erwähnt, die Auffassung, dass Inhaberin der DV-Daten und somit der SwissPass-Daten die Gesamtheit der am DV beteiligten Transportunternehmen, somit eine einfache Gesellschaft, sei. Weil eine einfache Gesellschaft keine eigene Rechtspersönlichkeit aufweise, sei nicht der DV Inhaber der Daten, sondern jedes einzelne am DV beteiligte Transportunternehmen sei Mitinhaberin (vgl. Ziff. 2.1.2). In seinem Schreiben vom 30. Oktober 2015 hielt der VöV zudem fest, der Umstand, dass die Daten technisch und organisatorisch nur von der SBB gemäss Art. 10a DSG verwaltet würden ändere nichts am gemeinsamen Charakter der Inhaberschaft.

Informationen zum Direkten Verkehr (DV) sind auf der Internetseite des VöV publiziert. Danach bilden zurzeit insgesamt 248 Transportunternehmen den DV. Folgt man der Auffassung des VöV würde dies dazu führen, dass insgesamt 248 Unternehmen über Zweck und Inhalt der Datensammlung entscheiden könnten, für die Informations- und Auskunftspflichten verantwortlich wären und einander die Ausübung ihrer jeweiligen Kontrolle gestatten müssten. Eine solche Lösung erscheint wenig resp. nicht praktikabel. So hält der VöV selbst fest, dass die verschiedenen Gremien des DV entscheiden, welche Datenbearbeitungen zu erfolgen haben (vgl. Ziff. 2.1.2).

Es ist zu prüfen, wie der DV organisiert ist und wer über Zweck und Bearbeitung der Daten entscheidet. Die rechtliche Basis des DV bilden die Artikel 16 und 17 PBG, welche die Transportunternehmen zur Kooperation verpflichten, sowie Art. 56 der Verordnung über die Personenbeförderung (VPB; SR 745.11). In Ausführung dieser Bestimmungen wurde das Übereinkommen 510 über die Organisation der Zusammenarbeit der am direkten nationalen Personenverkehr (DV) Teilnehmenden (Ue510) abgeschlossen. Dieses Ue510 sowie dessen Änderungen müssen vom Bundesamt für Verkehr (BAV) genehmigt werden (Ziff. 6.2 Ue510). Nach dem Ue510 gehören die Halbtax- und Generalabonnemente zum gesamten DV (vgl. Ziff. 1.3.4 Ue510). Der DV (ch-direct) hat auch den allgemeinen Personentarif T600, in welchem u.a. der SwissPass geregelt ist, erstellt. Organisatorisch besteht der DV aus verschiedenen Gremien, eines dieser Gremien ist ch-direct, ein anderes der Strategische Ausschuss des DV (StAD; Ziff. 3.1. Ue510 und Anlage 1 Ue510 [Organisationsreglement]).

Ch-direct besorgt die Geschäftsführung (Ziff. 3.5 Ue510) und ist organisatorisch dem VöV angegliedert (Geschäftsbericht 2014 VöV, S. 23). Ch-direct steht den Mitgliedern des StAD und der Revisionsstelle DV sowie den Verantwortlichen beim DV-Mandatsträger für Koordinationsaufgaben aller Art zur Verfügung (Ziff. 3.1 Anlage 7 Ue510 [Pflichtenheft ch-direct]).

Der StAD ist u.a. für das Treffen strategischer Entscheide (so zu den Themen Sortiment, Kundeninformationssysteme) bzw. das Festlegen von Grundsätzen zu DV-spezifischen Themen (z.B. Preise der DV-Produkte) und für die Genehmigung des Pflichtenhefts des DV-Mandatträgers zuständig (vgl. Ziff. 3.3.2 Ue510 i.V.m. Ziff. 3.1 c und Ziff. 3.2 f Anlage 2 Ue510 [Pflichtenheft StAD]). Der StAD setzt sich aus 7 bis 9 stimmberechtigten Mitgliedern (je 1 SBB, PostAuto und ZVV sowie 4 - 6 Mitglieder der übrigen am DV Teilnehmenden) zusammen. Der Bund, vertreten durch das Bundesamt für Verkehr, ist grundsätzlich mit einem Mitglied mit beratender Funktion im StAD vertreten. Der VöV und ch-direct nehmen mit je einer Person an den Sitzungen des StAD mit beratender Stimme teil, besitzen aber kein Stimmrecht (vgl. Ziff. 3.3.1 Ue510). Der StAD befindet endgültig über alle Geschäfte, die nicht der Gesamtheit der am DV Teilnehmenden zur Genehmigung vorbehalten sind (Ziff. 3.3.3 Ue510).

Der DV ist somit sehr eng mit dem VöV verbunden. So ist die Geschäftsleitung (ch-direct) organisatorisch dem VöV angegliedert. Weiter hat ch-direct (Geschäftsleitung) resp. der DV die gleiche Postadresse wie der VöV. Dementsprechend ist auf dem Briefpapier von ch-direct auch der VöV aufgeführt. Weiter sind Informationen zum DV inkl. seinen Gremien auf der Webseite des VöV publiziert zudem wurden die Geschäftsberichte 2014 des VöV und von ch-direct im gleichen Dokument veröffentlicht. Schliesslich ist der Direktor des VöV gleichzeitig auch Präsident des StAD.

Auf der anderen Seite kommt auch der SBB ein grosses Mitbestimmungsrecht zu. So ist sie zwar Auftragnehmerin des DV-Mandats (vgl. Anlage 9 Ue510 [Pflichtenheft DV-Mandat]), allerdings geht dieses Mandat sehr weit. Gemäss Pflichtenheft besteht das Mandat unter anderem in der Marktbearbeitung inkl. Preis- und Sortimentsentwicklung und Tarifmassnahmen, in der Verantwortung über die zentralen Basisvertriebssysteme und Kontrollsoftware und in der Führung der gemeinsamen Kundendatenbank (darunter KUBA und Kontrolldatenbank). Das Pflichtenheft hält auch ausdrücklich fest, dass die Nutzung personalisierter Kundendaten von SwissPass sowie der SwissPass Partnerdienste zu Marketingzwecken dem DV-Mandatsträger in erster Priorität zur Marktbearbeitung des DV gestattet ist. Zudem wird auf der Webseite www.swisspass.ch unter „Datenschutz und Rechtliches“ aufgeführt, dass der gesamte Inhalt von swisspass.ch der SBB gehöre. Gleichzeitig ist die SBB für die Datensicherheit und für die Behandlung der Auskunfts-, Berichtigungs- und Löschungsgesuche zuständig. Schliesslich besitzt die SBB auch einen wesentlichen Einfluss im StAD. Dementsprechend ist der StAD nur bei Anwesenheit von mindestens 5 stimmberechtigten Mitgliedern entscheidfähig, wobei die SBB zu den Anwesenden zählen muss. Ein Antrag ist angenommen, wenn er die Mehrheit der Stimmen, darunter diejenige der SBB, auf sich vereinigt (qualifiziertes Mehr). Enthält sich die SBB der Stimme, gilt das Einfache Mehr (Ziff. 3.3.3 Ue510). Da der StAG das Pflichtenheft DV-Mandat genehmigt (Ziff. 6 Abs. 3 Pflichtenheft DV-Mandat), besitzt die SBB folglich auch einen grossen Einfluss auf der Auftraggeberseite.

Zusammengefasst ergibt sich somit Folgendes: wie vom VöV resp. ch-direct festgehalten, werden die Entscheide (Inhalt und Zweck) betreffend den SwissPass von den Gremien des DV getroffen. Allerdings kann ein Gremium, dem keine eigene Rechtspersönlichkeit zukommt, nicht Dateninhaber im Sinne des DSG sein. Wie dargelegt, besteht zwischen der Genossenschaft VöV – mit eigener Rechtspersönlichkeit – und der einfachen Gesellschaft DV eine sehr enge Verknüpfung. Zudem sind die am DV teilnehmenden Gesellschaften zumindestens zum grössten Teil auch Mitglied des VöV. Gleichzeitig hat ebenfalls die SBB einen grossen Einfluss auf die Entscheide. In dieser Konstellation haben aufgrund der weiter oben aufgeführten Gründe sowohl der VöV als Genossenschaft und Auftraggeber (der Direktor des VöV ist wie erwähnt Präsident des StAD) als auch die SBB als Auftragnehmerin einen

massgebenden Einfluss auf Zweck und Inhalt der Datensammlungen betreffend SwissPass. Aus diesen Gründen geht der EDÖB davon aus, dass sowohl der VöV als auch die SBB gemeinsam Dateninhaber der Datensammlungen in Zusammenhang mit dem SwissPass sind und für die vorgenommenen Datenbearbeitungen, die Datensicherheit, die Gewährleistung des Auskunftsrechts und die Anmeldung der Datensammlungen verantwortlich sind. Diese Annahme wird noch dadurch gestützt, dass auf der einen Seite die Kontrolle vor Ort bei der SBB stattfand und von ihr gestaltet wurde. Auf der anderen Seite wurden die verschiedenen Stellungnahmen in der vorliegenden Sachverhaltsabklärung jeweils gemeinsam vom Direktor des VöV und dem Leiter von ch-direct unterschrieben. Auch die Tarifänderungen des T600 erfolgten durch das Tarifmanagement des VöV.

Der VöV und die SBB, aber auch die anderen am DV beteiligten Unternehmen sind sich der oben beschriebenen Problematik betreffend Dateninhaberschaft bewusst. So enthält Ziff. 3 des Regelwerks Datennutzung Ausführungen zur Dateninhaberschaft der DV-Kundendaten. Dabei wird festgehalten, dass für die Kunden in der Regel die SBB als Dateninhaber auftrete, obwohl gemäss AGB die SBB nur im Auftrag des DV handle. Zur Behebung der Diskrepanz wurde eine interne Arbeitsgruppe eingesetzt. Folglich müssen der VöV und die SBB allenfalls innerhalb der vorgenannten Arbeitsgruppe oder mit anderen Beteiligten dafür sorgen, dass betreffend Dateninhaberschaft auch gegen aussen Transparenz geschaffen und allfällige Diskrepanzen behoben werden.

Vorschlag Nr. 1

Aufgrund der Erwägungen macht der EDÖB den folgenden Vorschlag: Um gegenüber Kunden und anderen Dritten Transparenz zu schaffen, stellen der VöV und die SBB sicher, dass in den verschiedenen Unterlagen zum SwissPass im Sinne der obigen Erwägungen auf klarere und transparentere Weise aufgeführt wird, wer Inhaber der Datensammlungen in Zusammenhang mit dem SwissPass ist. Der VöV und die SBB teilen dem EDÖB mit, ob sie mit diesem Verbesserungsvorschlag einverstanden sind und informieren den EDÖB über die diesbezüglich unternommenen Schritte.

3.2. Bearbeitung der Kontrolldaten

Die Kontrolldaten werden nach der Kontrolle in die Kontrolldatenbank hochgeladen und dort während 90 Tagen aufbewahrt (vgl. Ziff. 2.2.1 und 2.4). Unbestritten ist, dass Transportunternehmen überprüfen dürfen, ob Reisende einen gültigen Reiseausweis besitzen (Art. 16 i.V.m. 20 PBG). Zu prüfen ist jedoch, ob die in Zusammenhang mit dem SwissPass eingeführte Aufbewahrung der Daten in der Kontrolldatenbank während 90 Tagen datenschutzrechtlich zulässig ist.

3.2.1. Verhältnismässigkeit

Die Bearbeitung von Personendaten muss verhältnismässig sein (vgl. Art. 4 Abs. 2 DSG). Verhältnismässigkeit liegt vor, wenn nur diejenigen Daten bearbeitet werden, die für den verfolgten Zweck unbedingt nötig und geeignet sind. Nicht mehr benötigte Daten sind zu löschen. So wird auch in der Literatur festgehalten, dass ein Datenbearbeiter nur diejenigen Daten beschaffen und bearbeiten darf, die er für einen bestimmten Zweck objektiv tatsächlich benötigt und die mit Blick auf den Bearbeitungszweck und die Persönlichkeitsbeeinträchtigung in einem vernünftigen Verhältnis stehen (vgl. Urs Maurer-Lambrou/Andrea Steiner in Maurer-Lambrou/Blechta, BSK Kommentar Datenschutzgesetz, 3. Auflage, Helbing Lichtenhahn Verlag, Art. 4, N. 11 mit Hinweisen).

In der Kontrolldatenbank werden unter anderem die Uhrzeit, Zug-/Kursnummer und die Verknüpfung zur SwissPass-Ausweisnummer gespeichert. Auch wenn nicht aufgeführt wird, von wo bis wo eine Person gereist ist, kann nicht ausgeschlossen werden, dass aufgrund der Kontrollzeitpunkte eruiert werden kann, an welchen Bahnhöfen eine Person ein- und/oder ausgestiegen ist. Aufgrund der Aufbewahrung von 90 Tagen kann zudem nicht ausgeschlossen werden, dass dabei bei bestimmten Personen ein, wenn auch nicht detailliertes, Bewegungsprofil entstehen kann (z.B. immer nur Kontrollen zwischen Bern und Zürich). Bei einer solchen Persönlichkeitsbeeinträchtigung ist der Grundsatz der Verhältnismässigkeit besonders sorgfältig zu prüfen.

Gemäss Angaben des VöV und der SBB dient die Kontrolldatenbank dazu, allfällige Kundenanliegen im Nachgang zu einer Reise zu beantworten. Es wurden verschieden Gründe und Beispiele aufgeführt (vgl. Ziff. 2.4). Diese werden nachfolgend geprüft.

Zunächst ist darauf hinzuweisen, dass bei Reisenden ohne gültigen Fahrausweis nur dann Kontrolldaten in die hier beschriebene Kontrolldatenbank übertragen werden können, wenn die betroffene Person einen SwissPass vorweist. Ohne SwissPass-Karte können die Daten nicht vom Lesegerät gelesen und in die Kontrolldatenbank übermittelt werden. Abgesehen davon wird bei Reisenden ohne gültigen Fahrausweis in der Regel ein separates Formular (Formular 7000 „Reisende ohne gültigen Fahrausweis“ oder internes Formular eines Transportunternehmens) ausgefüllt, auf welchem auch der Zeitpunkt der Kontrolle aufgeführt ist. So sieht auch der vom Parlament verabschiedete aber noch nicht in Kraft getretene[3] Art. 20a Abs. 2 Bst. c PBG vor, dass bei Reisenden ohne gültigen Fahrausweis der Zeitpunkt der Erhebung des Zuschlags erhoben werden kann (vgl. AS 2015 3205 f.). Der VöV führt weder aus, weshalb genau es nötig ist, die Daten für Reisende ohne gültigen Fahrausweis in der Kontrolldatenbank aufzubewahren, noch wie damit Missbrauchsfälle entdeckt werden können. Zu beachten ist, dass in der Kontrolldatenbank die Daten sämtlicher Reisender, somit auch von solchen mit einem voll gültigen Fahrausweis, aufbewahrt werden. Dieser vom VöV aufgeführte Grund erweist sich somit als nicht stichhaltig.

Aber auch die anderen vom VöV aufgeführten Gründe überzeugen nicht. So wird das Zugbegleitpersonal während der Kontrolle merken, ob sein Gerät bei allen Karten funktioniert und auf die Abonnementsdaten zugreifen kann oder nicht und eine allfällige Störung sofort melden können. Fälle, in denen eine Karte trotz Beendung der Hinterlegung als hinterlegt erscheinen kommen sicher sehr selten vor und können einzelfallweise ohne Kontrolldatenbank gelöst werden[4]. Der VöV führt nicht weiter aus, weshalb die Kontrolldatenbank bei der Analyse von System- und Betriebsausfällen, die voraussichtlich vor allem den Zugriff auf Abonnementsdaten (KUBA) betreffen, nötig ist. In den in Z. 12.000 und 12.001 T600.9 aufgeführten Fällen sollte eine Rückerstattung ohne Kontrolldaten möglich sein. Auch wenn ein Reisender/eine Reisende die Rückerstattung aufgrund einer Nichtbenützung infolge Krankheit oder Unfall erst nachträglich verlangt, erübrigt sich ein Zugriff auf die Kontrolldatenbank, da in diesen Fällen ein entsprechendes Arztzeugnis beizubringen ist (vgl. Z. 60.005 T600.9).

Im Zeitpunkt der Kontrolle vor Ort (mehr als 2 ½ Monate nach Einführung des SwissPass) waren, wie erwähnt, abgesehen für die Behandlung von zwei Auskunftsgesuchen, keine Zugriffe auf die Kontrolldatenbank nötig gewesen. Auch das UVEK hat in seiner Stellungnahme vom 21. September 2015 an die Präsidentin und den Präsidenten der

[3] Art. 20a PBG ist am 1. Januar 2016 in Kraft getreten.

[4] Vgl. Fussnote 2.

Kommissionen für Verkehr und Fernmeldewesen betreffend die Petition 15.2018 festgehalten, dass aus den Datenschutzbestimmungen nicht klar hervorgehe, dass eine personalisierte Auswertung der Kontrolldaten ausgeschlossen sei. Dadurch, dass überhaupt gespeichert werde, in welchem Zug ein Reisender kontrolliert wurde, entstehe aber zumindest die Gefahr, dass solche Daten missbräuchlich personalisiert verwendet werden könnten.

Schliesslich ist noch darauf hinzuweisen, dass in Zusammenhang mit den Fragen des EDÖB zum Regelwerk Datennutzung die SBB ausdrücklich festhielt, auf die ursprünglich vorgesehene Analyseoption der Kontrolldaten in pseudonymisierter Form verzichtet zu haben (vgl. Ziff. 2.4 oben).

Daraus folgt, dass die Aufbewahrung der Kontrolldaten in der Kontrolldatenbank weder nötig noch geeignet und somit unverhältnismässig ist. Wie erwähnt kann zudem nicht ausgeschlossen werden, dass in der Kontrolldatenbank Bewegungsprofile entstehen. Dabei ist irrelevant, dass die Aufbewahrung in verschlüsselter Form erfolgt und nur ein kleiner Kreis von Anwendern Zugriff auf die Daten hat.

3.2.2. Rechtmässigkeit

Unabhängig davon stellt sich auch die Frage der Rechtmässigkeit der Aufbewahrung der Kontrolldaten. Wie im Schreiben des VöV vom 30. Oktober 2015 festgehalten wurde, handeln die Transportunternehmen in Zusammenhang mit den Kontrolldaten als Bundesorgan. Folglich müssten die Führung der Kontrolldatenbank und das Informationssystem selbst in einer gesetzlichen Grundlage geregelt sein. Diesbezüglich kann auch auf die Bearbeitung von Daten in Zusammenhang mit Reisenden ohne gültigen Fahrausweis verwiesen werden. Für diese wurde ebenfalls eine gesetzliche (da es sich um besonders schützenswerte Personendaten handelt eine formellgesetzliche) Grundlage geschaffen (vgl. AS 2015 3205 f.). Vorliegend fehlt somit auch eine gesetzliche Grundlage, welche die Einzelheiten der Kontrolldatenbank (Regelung des Informationssystems, der Datenbearbeitungen, der Datenaufbewahrung, Zugriffberechtigungen, usw.) regelt. Eine Regelung in einem Tarif, der von den Transportunternehmen erstellt wird, würde nicht genügen. Es muss sich mindestens um eine gesetzliche Grundlage im materiellen Sinn (z.B. eine Bundesratsverordnung) handeln. Werden besonders schützenswerte Personendaten bearbeitet, braucht es eine formelle gesetzliche Grundlage (z.B. Bundesgesetz). Zudem müsste das Informationssystem selbst in der gesetzlichen Grundlage geregelt werden. Gleichzeitig müsste der VöV die Datenbank beim EDÖB anmelden. Daraus folgt, dass die Kontrolldatenbank auf keiner genügenden gesetzlichen Grundlage beruht und somit nicht rechtmässig ist.

In seiner Korrespondenz mit dem EDÖB betreffend die Petition 15.2018 vertrat auch das BAV die Auffassung, dass die Kontrolldatenbank weder verhältnismässig ist noch auf einer genügenden gesetzlichen Grundlage beruht. So hat das BAV im September 2015 gegenüber dem EDÖB festgehalten, dass es nicht erforderlich sei, die Daten aufzubewahren, nachdem die Kontrolle einen gültigen Fahrausweis ergeben habe. Zudem gäbe es keine Rechtsgrundlage, um die Daten von Reisenden mit gültigem Fahrausweis zu speichern. Folglich hielt das BAV fest, dass die Identität des Reisenden, die von einem Gerät zur Kontrolle der Gültigkeit des Fahrausweises erfasst würden, automatisch in dem Moment zu löschen seien, in dem das Gerät die Gültigkeit seines Fahrausweises bestätigt habe.

Daraus folgt, dass die in Zusammenhang mit der Kontrolldatenbank durchgeführten Datenbearbeitungen weder das Verhältnismässigkeitsprinzip einhalten noch auf einer genügenden gesetzlichen Grundlage beruhen.

Empfehlung Nr. 1

Aufgrund der Erwägungen macht der EDÖB folgende Empfehlung: Der VöV und die SBB stellen sicher, dass die SBB die Kontrolldaten unverzüglich löscht und die Kontrolldatenbank nicht mehr weiter betreibt sowie die Transportunternehmen entsprechend informiert resp. die Lesegeräte entsprechend konfiguriert werden und die Daten nicht mehr (systematisch) übermittelt werden. Der VöV und die SBB informieren den EDÖB über die erfolgte Löschung und die diesbezüglich getroffenen Anpassungen.

3.3. Datenbearbeitung zu Marketingzwecken

Eine Datenbearbeitung der SwissPass-Daten erfolgt nur, wenn der Kunde/die Kundin kein Opt-out geltend gemacht hat (vgl. Ziff. 4.3). Aufgrund der zu wenig klar umschriebenen Verwendung der Daten zu Marketingzwecken und der Opt-out-Möglichkeit, legte der VöV dem EDÖB einen Entwurf der neu formulierten AGB zum GA und zum Halbtaxabonnement vor.

Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung erst gültig, wenn sie nach angemessener Information freiwillig erfolgt (Art. 4 Abs. 5, 1. Satz DSG).

In den im Zeitpunkt der Kontrolle vor Ort geltenden AGB wurde einerseits auf die Opt-out-Möglichkeit hingewiesen, andererseits musste sich die Nutzerin oder der Nutzer unter anderem damit einverstanden erklären, dass „die SBB und/oder die TU der Schweiz diese personenbezogenen Daten zu Marketingzwecken bearbeiten“. Zudem wurde darauf hingewiesen, dass die personenbezogenen Daten der Partnerangebote durch die SBB mit technischen Mitteln ausgewertet werden könnten um das SwissPass-Partnerangebot bedürfnisorientiert weiterentwickeln zu können.

Die AGB wurden inzwischen geändert. Die neu formulierten AGB sehen ausdrücklich vor, dass die Ermächtigung zur personenbezogenen Datenbearbeitung zu Marketingzwecken entzogen werden kann und führen aus, wo dieses Opt-out geltend gemacht werden kann. Zudem wurde der vorgenannte Absatz gestrichen. Allerdings erweckt der letzte Satz des Kapitels „Marketing und Auswertungen von personenbezogenen Daten“ der AGB („Nach einem Opt-out […] verfügen“) den Eindruck, dass bei einem Opt-out einzig keine Kontaktaufnahme erfolgt und die Daten trotzdem zu Marketingzwecken bearbeitet werden können. Dieser Satz müsste somit präziser formuliert werden und könnte beispielsweise durch folgende Formulierung ersetzt werden: „Nach einem Opt-out werden Ihre Daten nicht mehr personenbezogen zu Marketingzwecken bearbeitet und Sie werden nicht weiter zu Marketingmassnahmen kontaktiert. Sofern Sie über eine oder mehrere gültige Leistungen (Halbtax, GA, Partnerleistungen etc.) verfügen, verbleiben Ihre Daten jedoch weiterhin zur Erbringung dieser Leistungen in unseren Datenbanken.“

Um eine angemessene Information zu gewährleisten, ist die neue Version der AGB somit im Sinne der obigen Erwägungen anzupassen. Gleichzeitig müssen die neuen AGB von allen betroffenen Transportunternehmen übernommen werden.

Vorschlag Nr. 2

Aufgrund der Erwägungen macht der EDÖB den folgenden Vorschlag: Der VöV und die SBB stellen sicher, dass die neue Version der AGB zum GA sowie die AGB zum Halbtaxabonnement im Sinne der obigen Erwägungen angepasst wird und von sämtlichen beteiligten Transportunternehmen übernommen und publiziert werden. Der VöV und die SBB teilen dem EDÖB mit, ob sie mit diesem Verbesserungsvorschlag einverstanden sind und informieren den EDÖB über die diesbezüglich unternommenen Schritte.

3.4. Regelwerk

Das Regelwerk Datennutzung sah im Moment der Kontrolle vor Ort vor, dass die Kontrolldaten in pseudonymisierter Form zu Analysezwecken verwendet würden. Auf diese Analyseoption wurde jedoch von Anfang an verzichtet (vgl. Ziff. 2.4).

Daraus folgt, dass das Regelwerk Datennutzung entsprechend angepasst werden muss. Aufgrund der Empfehlung des EDÖB, die Kontrolldaten zu löschen und die Kontrolldatenbank nicht mehr zu betreiben müsste zudem geprüft werden, ob noch andere Teile des Regelwerks Datennutzung sowie andere Dokumente, welche die Kontrolldatenbank regeln, anzupassen sind.

Vorschlag Nr. 3

Aufgrund der Erwägungen macht der EDÖB den folgenden Vorschlag: Der VöV und die SBB passen das Regelwerk Datennutzung im Sinne der vorliegenden Erwägungen an. Gleichzeitig prüfen sie, ob noch weitere Dokumente angepasst werden müssen und passen diese gegebenenfalls an. Der VöV und die SBB teilen dem EDÖB mit, ob sie mit diesem Verbesserungsvorschlag einverstanden sind und teilen dem EDÖB mit, welche Unterlagen geändert werden müssen und unterbreiten diese dem EDÖB sobald diese angepasst wurden.

3.5. Schlussbemerkung

Was die Verbesserungsvorschläge betrifft, verzichtet der EDÖB derzeit auf den Erlass einer Empfehlung. Der EDÖB behält sich vor, je nach Stellungnahme des VöV und der SBB, auf diesen Entscheid zurück zu kommen.

Der Beauftragte ad interim:

Jean-Philippe Walter

Die zuständige Mitarbeiterin:

Caroline Gloor Scheidegger
Juristin

CC:
- Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation, Generalsekretariat, 3003 Bern
- Bundesamt für Verkehr (BAV), Rechtsdienst, 3003 Bern