

Neue Datenschutzgesetzgebung

Was bedeutet dies für die Transportunternehmen
im Alltag?

Rechtstagung VÖV, 9. November 2023
Zentrum Paul Klee

Programm

- 8.30 Uhr Eintreffen der Teilnehmenden / Begrüssungskaffee
- 9.15 Uhr Begrüssung - Ueli Stückelberger, VöV
- 9.20 Uhr Peter König, BAV
- 9.50 Uhr Fragen an den Referenten
- 10.10 Uhr Anselm Filliger, SBB
- 10.40 Uhr Fragen an den Referenten
- 11.00 Uhr Pause
- 11.20 Uhr Tim Loosli, ASP / Philippe Kaufmann, ASP / Christian Sterchi, VöV
- 11.40 Uhr Fragen an die Referenten
- 12.00 Uhr Podiumsdiskussion

Anschliessend gemeinsamer Stehlunch

Der neue Datenschutzartikel im Personenbeförderungsgesetz

Peter König, Bundesamt für Verkehr (BAV)

Agenda

- Einordnung des Themas
- Wie funktioniert Datenschutz?
- Einwilligung ↔ gesetzliche Grundlage
- Was ist neu im DSGVO, was wird neu mit dem PBG?
- Anwendungsbeispiele: Fahrt in CH, Fahrt ins Ausland, Kauf Halbtaxabo
- Problembereiche, Fragen, Diskussion

Aus aktuellem (?) Anlass

Les CFF n'oublie
rien de nos habitudes

SAMMELWUT Bundesbahnen führen seit Jahren detaillierte Kundendossiers von Millionen von Swisspass-Inhaber

Die SBB fahren auf Ihre Daten ab

Datum: 23.08.2023



Abo Nouveau règlement

Partir incognito à l'étranger? Pas avec les CFF

Unerkannt ins Ausland? Nicht mit den SBB

Personalisierte Tickets Neuerdings wollen die Angestellten am Billettschalter wissen, wer mit dem Zug ins Ausland fährt. Das ist nur ein Beispiel dafür, wie die Bahn immer mehr Personendaten anhäuft.

Einordnung des Themas

Allgemein

- Datenschutz ist omnipräsent, sowohl in der EU als auch in der Schweiz – das zeigt auch Ihr Hiersein.
- «Ohne Daten kein Leben», wir sind alle auf die Bearbeitung und Bekanntgabe auch unserer Daten angewiesen.
- Missbrauchsbekämpfung ist sehr schwierig. «korrekter» Datenschutz überaus aufwendig.
- Nutzen DSGVO und DSG fraglich – viel Aufwand, hohe Kosten; wenig direkt sichtbarer Nutzen, viel Ungewissheit.
- «Irrationales» Nutzerverhalten – hier geben wir alles her, dort wollen wir lieber gar nicht. Wie ist damit umzugehen?

Unklar

- Braucht/e es überhaupt eine neue Datenschutzbestimmung im PBG, oder hätte die bestehende ausgereicht?

Einordnung des Themas

Günstig

- Die detaillierte Botschaft zu Art. 54 PBG kann voll herangezogen werden, dieser im Parlament ohne Diskussion durchkam.
- Die Branche hat bei der Formulierung konstruktiv mitgearbeitet und im Parlament auf Lobbyismus verzichtet.

Schwierig


- Sehr unterschiedliche Interessen der verschiedenen Seiten (TU, Passagiere, Behörden...)
- Fast parallele Revision zweier Gesetze; gegenseitige Abstimmung

Datenschutzerklärung SBB – wirklich auf «einen» Blick?


Datenschutz auf einen Blick.

 Allgemeine Personendaten.




 Standortdaten.



 Überlassene Daten.



 Erhobene Daten.



 Erhaltene Daten.



 Marketing.




 Produktentwicklung.



 Profiling.



 Datenweitergabe.



 Weltweit.



[Datenschutz | SBB](#)

Datenschutzerklärung ASP – ebenfalls sehr detailliert

Die richtigen Fragen (und Antworten)...

... aber sehr aufwendig zu suchen und zu finden.

Und wahrscheinlich etwas praxisfern; nur Wenige machen sich die Mühe, ihre Rechte zu wahren.

(Auch) deshalb ist eine saubere, **klare gesetzliche Regelung** von grossem Nutzen für beide Seiten.

1 Wer ist für die Datenbearbeitung verantwortlich?	+
2 Weshalb sammeln wir Personendaten?	+
3 Welche Daten werden gespeichert und wozu werden sie verwendet?	+
4 Wie lange werden Ihre Daten aufbewahrt?	+
5 Wo werden die Daten gespeichert?	+
6 Welche Daten werden im Zusammenhang mit dem Marketing bearbeitet?	+
7 Welche Daten werden zu Marktforschungszwecken bearbeitet?	+
8 Welche Rechte haben Sie in Bezug auf Ihre Personendaten?	+
9 Werden Ihre Daten an Dritte weitergegeben?	+
10 Wie werden Tracking Tools eingesetzt?	+
11 Was sind Cookies und wann werden sie eingesetzt?	+
12 Was sind Social Plugins und wie werden sie verwendet?	+
13 Anzeigen von Werbung auf unseren Internetseiten und in unseren Apps	+
14 Datensicherheit	+
15 Änderungen dieser Datenschutzerklärung	+

Fragestellungen

- Langer Streit über die Notwendigkeit einer Revision: Reichte der alte Artikel 54 PBG oder nicht?
- Unterschiedliche Vorstellungen, wie eine neue Bestimmung aussehen sollte.
- Kein datenschutzrechtlicher «Blankocheck»...
... aber auch keine unnötigen Hürden für die Unternehmen.
- Unterscheidung öffentliche Aufgabe (Transport) und weiterer Bereiche (Kommerz)
- Profiling ja oder nein?
- Umgang mit besonders schützenswerten Personendaten
- Zweckbindungsgebot bei der Datenbearbeitung
- Aufbewahrungsdauer der Daten
- Sonderfall Bundesorgane, oder anders gesagt: Art. 33 – 42 statt Art. 30 – 32 DSGVO
- Gesetzliche Grundlage vs. Einwilligung – im PGB kommt beides vor.
- Zwei fast parallele Gesetzesrevisionen – Datenschutz- und Personenbeförderungsgesetz.

Wie funktioniert Datenschutz?

Prinzip des Datenschutzes

- Wer Personendaten bearbeitet, darf die Persönlichkeit der Person nicht widerrechtlich verletzen (Art. 30 Abs. 1 DSGVO)
- Eine Persönlichkeitsverletzung ist **nicht widerrechtlich**, wenn sie durch **Einwilligung**, **überwiegendes öffentliches oder privates Interesse** oder durch **Gesetz** gerechtfertigt ist (Art. 31 Abs. 1 DSGVO, langer Katalog von Beispielen in Abs. 2)
- **Bundesorgane** dürfen Personendaten nur bearbeiten, wenn dafür eine **gesetzliche Grundlage** besteht.
- In drei Fällen braucht es sogar ein **Gesetz im formellen Sinn**, nämlich bei **besonders schützenswerten Personendaten**, für das **Profiling** und wenn **schwerwiegende Eingriffe in die Persönlichkeit** drohen.

Einwilligung vs. gesetzliche Grundlage

Was heisst das für den öV?

- Bislang war das Ganze oft eine Mischung aus «zähneknirschender Zustimmung zu allem» und aufwendiger Selektion. Auch war nicht immer klar, welche Daten die TU zwingend brauchen und welche nicht.
- Neben Unsicherheit hat das auch zu sehr umfangreichen **Datenschutzregelungen** und Kundenführungen geführt.
- Sind die **TU** «**Bundesorgane**»? Die Frage ist umstritten; klar ist immerhin, dass sie eine öffentliche Aufgabe ausüben.
- Interessanter ist die Frage, was ihnen erlaubt sein soll, ohne jedesmal fragen zu müssen. Es macht keinen Sinn, wenn jemand seine Zustimmung zur Datenbearbeitung verweigert, der ein GA kaufen will – dieses ist ja höchstpersönlich.
- Der GA-Kauf darf aber auch nicht an die Zustimmung zur Bearbeitung bspw. für Marketingzwecke geknüpft werden

Einwilligung vs. gesetzliche Grundlage

Lösungsansatz

- Alles, was es an **Datenbearbeitung zwingend** braucht für den **Transport**, ist **von Gesetzes wegen gestattet**
- Für **alles andere muss die Kundschaft ausdrücklich einwilligen**.
- Bei den «Mischformen» gilt jeweils das Recht für Private (Art. 30 – 32 DSGVO), Dies aus Gründen der Einheitlichkeit und des Handlings (es können ja nicht für ein und denselben Vorgang zwei Datenwelten gleichzeitig gelten).
- Beispiele sind Kombiangebote, z.B. mit Mietwagen, und Einbezug touristischer Leistungen, z.B. Hotelübernachtungen.
- **Datenaufbewahrung jeweils nur zulässig so lange wie nötig** – das kann aber recht unterschiedlich lang sein.

Was ist neu im DSG, was ist neu im PBG?

Neues DSG

- Teilweise Anpassung des Schweizer Rechts an die EU-DSGVO
- Teilweise neue Begrifflichkeiten (wie z.B. Profiling)
- Klarere und weitergehende Anforderungen an den Datenschutz
- Weiterhin Unterscheidung Private ↔ Bundesorgane
- Anpassung diverser andere Bundesgesetze, auch des Eisenbahngesetzes (hier kein Thema)
- etc.

Neues PBG (Art. 54)

- Diverse Vorschriften v.a. im Zusammenhang mit dem regionalen Personenverkehr RPV
- Verschiedene kleinere Anpassungen (wie bei fast jeder Vorlage)
- Fast «nebenher» auch eine Neufassung von Art. 54 PBG – ging das wirklich so einfach?
- Sehr lange, kontroverse, intensive Diskussion zwischen Branche und Behörden: Braucht es da? Wenn ja, in welcher Form?
- Nach unzähligen Versionen schien der gefundene Kompromiss gut genug – das Parlament hat keine Silbe dazu gesagt.

Die «Debatte» im Nationalrat, sehr kurz zusammengefasst

Nationalrat Wintersession 2021 Zweite Sitzung 30.11.21 08h00 21.039

Art. 36; 37-39; 51 Abs. 1; Gliederungstitel vor Art. 54; Art. 54; Ziff. II

Antrag der Kommission

Zustimmung zum Entwurf des Bundesrates

Art. 36; 37-39; 51 al. 1; titre précédant l'art. 54; art. 54; ch. II

Proposition de la commission

Adhérer au projet du Conseil fédéral

Angenommen - Adopté

Im Ständerat dito...

Ständerat Frühjahrssession 2021 Sechste Sitzung 08.03.22 08h15 21.039

Art. 37-39; 51 Abs. 1; Gliederungstitel vor Art. 54; Art. 54; Ziff. II

Antrag der Kommission

Zustimmung zum Beschluss des Nationalrates

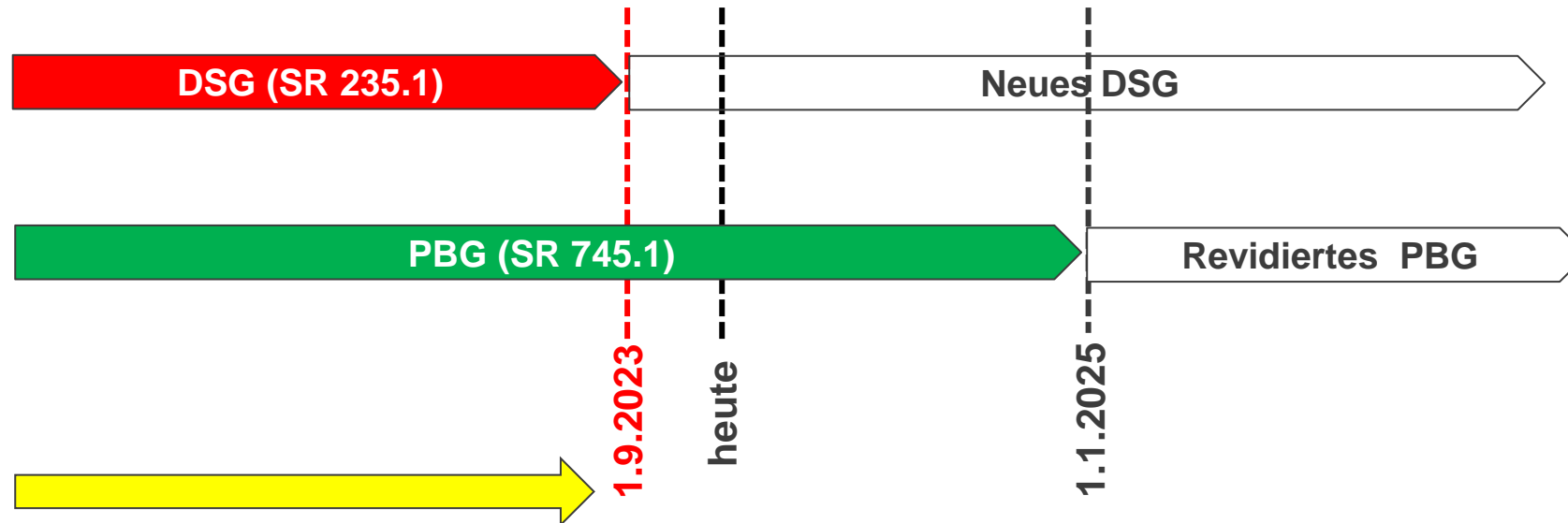
Art. 37-39; 51 al. 1; titre précédant l'art. 54; art. 54; ch. II

Proposition de la commission

Adhérer à la décision du Conseil national

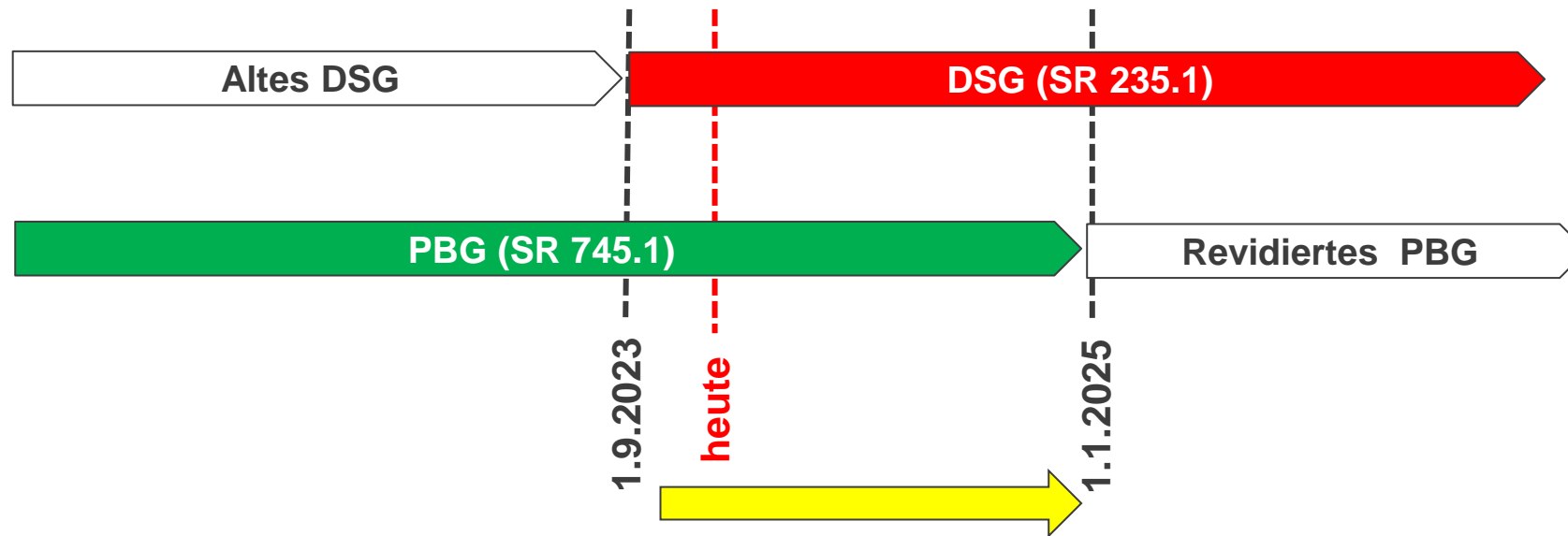
Angenommen - Adopté

Rechtslage bis 31.8.2023



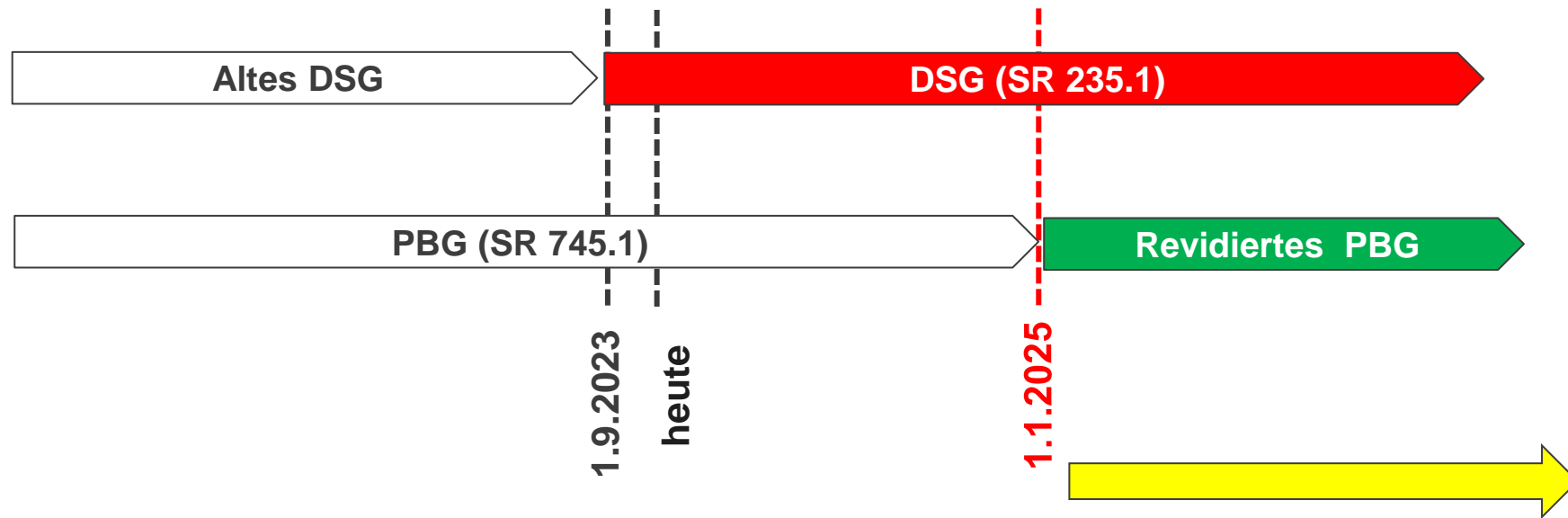
Bis Ende August galt das alte Datenschutzgesetz, und auch die Revision des Personenbeförderungsgesetzes war noch nicht in Kraft.

Rechtslage heute (seit 1.9.2023)



Heute gilt das neue Datenschutzgesetz schon, während die Revision des Personenbeförderungsgesetzes erst später in Kraft treten wird (voraussichtlich anfangs 2025)

Rechtslage ab voraussichtlich 1.1.2025



Voraussichtlich anfangs 2025 wird die Revision des Personenbeförderungsgesetzes in Kraft treten. Das neue Datenschutzgesetz gilt weiterhin.

PBG-Wortlaut bis 31.8.2023

Art. 54 Datenbearbeitung durch Unternehmen

¹ Die Unternehmen unterstehen für ihre konzessionierten und bewilligten Tätigkeiten den Artikeln 16–25^{bis} des Bundesgesetzes vom 19. Juni 1992⁷⁹ über den Datenschutz (DSG). Handeln sie dabei privatrechtlich, so unterstehen sie stattdessen den Artikeln 12–15 DSG.

² Sie können besonders schützenswerte Personendaten sowie Persönlichkeitsprofile bearbeiten, soweit dies für die Personenbeförderung und den Betrieb oder für die Sicherheit der Reisenden, des Betriebes oder der Infrastruktur erforderlich ist. Dies gilt auch für Dritte, die Aufgaben eines Unternehmens mit einer Konzession oder Bewilligung nach den Artikeln 6–8 wahrnehmen. Das Unternehmen bleibt für die Einhaltung der Datenschutzvorschriften verantwortlich.

³ Die Aufsicht richtet sich nach Artikel 27 DSG.

PBG-Wortlaut heute

Art. 54⁷⁹ Datenbearbeitung durch Konzessionsinhaberinnen

¹ Die Unternehmen unterstehen für ihre konzessionierten und bewilligten Tätigkeiten den Artikeln 33–42 des Datenschutzgesetzes vom 25. September 2020⁸⁰ (DSG). Handeln sie dabei privatrechtlich, so unterstehen sie stattdessen den Artikeln 30–32 DSG.

² Sie können besonders schützenswerte Personendaten bearbeiten, soweit dies für die Personenbeförderung und den Betrieb oder für die Sicherheit der Reisenden, des Betriebes oder der Infrastruktur erforderlich ist. Dies gilt auch für Dritte, die Aufgaben eines Unternehmens mit einer Konzession oder Bewilligung nach den Artikeln 6–8 wahrnehmen. Das Unternehmen bleibt für die Einhaltung der Datenschutzvorschriften verantwortlich.

PBG-Wortlaut ab voraussichtlich 1.1.2025

Art. 54 Bearbeitung von Personendaten

¹ Die Unternehmen können Personendaten **bearbeiten**, soweit dies für die Personenbeförderung und den Betrieb oder für die Sicherheit der Reisenden, des Betriebes oder der Infrastruktur erforderlich ist.

² Sie können:

- a. ein Profiling mit Ein- und Ausstiegsstationen der Reisenden durchführen, um den Fahrpreis zu ermitteln und in Rechnung zu stellen;
- b. **besonders schützenswerte Personendaten** über die **Gesundheit** von Reisenden mit Behinderungen bearbeiten, um Benachteiligungen beim Zugang zu Einrichtungen oder Fahrzeugen des Unternehmens zu beseitigen oder zu verringern.

³ Sie dürfen die Personenbeförderung **nicht von der Einwilligung der Reisenden in die Bearbeitung von deren Personendaten abhängig machen**.

PBG-Wortlaut ab voraussichtlich 1.1.2025

Art. 54 Bearbeitung von Personendaten

⁴ Sie müssen **zu vergleichbaren Bedingungen** Personentransportverträge anbieten, die **keine Bearbeitung von Personendaten erfordern**.

⁵ Sie unterstehen den Artikeln **30–32** des Datenschutzgesetzes vom 25. September 2020 für Mobilitätsangebote, die:

- a. auch **Beförderungsleistungen umfassen, die nicht diesem Gesetz unterstehen**;
- b. **wesentliche andere Dienstleistungen** wie touristische oder kulturelle Angebote umfassen.

⁶ Die Absätze 1 - 5 gelten **auch für Dritte**, die Fahrausweise nach diesem Gesetz verkaufen

VPB – aktueller Entwurfsstand (1)

Bis am **1.12.2023** läuft die Vernehmlassung zur ARPV. Mit ihr soll auch die VPB angepasst werden, darunter zwei Bestimmungen zum Datenschutz:

Art. 79a Datenbearbeitung durch Unternehmen (Art. 54, 20, 20a PBG)

¹ Unternehmen dürfen folgende **Personendaten** von Reisenden mit einem persönlichen Fahrausweis zur Sicherung der Einnahme des Fahrpreises oder von Reisenden zur Sicherung des Zuschlags nach Artikel 20 PBG bearbeiten:

- a. Name;
- b. Geburtsdatum;
- c. Wohnadresse;
- d. E-Mail-Adresse;
- e. Mobiltelefonnummer;
- f. Zahlungsmittel.

VPB – aktueller Entwurfsstand (2)

² Folgende **besonders schützenswerte Personendaten** dürfen bearbeitet werden:

- a. maschinenlesbare Fotos zur Identifizierung von Reisenden mit einem persönlichen Fahrausweis;
- b. Daten zur Ortung der Ein- und Ausstiegsstationen von Reisenden mit einem persönlichen Fahrausweis für die Berechnung des Fahrpreises;
- c. rechtskräftige Urteile über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen betreffend das Reisen ohne gültigen Fahrausweis zu den in Artikel 20a PBG genannten Zwecken.

³ Die **Daten zu den Ein- und Ausstiegsstationen der Reisenden**, anhand welcher der Fahrpreis ermittelt, und in Rechnung gestellt wird, dürfen allen Unternehmen bekanntgegeben werden, die Anspruch auf Beteiligung an den Einnahmen haben.

⁴ Personendaten dürfen nur **anonymisiert** zur Verbesserung der Vertriebsinfrastruktur verwendet werden.

VPB – aktueller Entwurfsstand (3)

Art. 56a Gemeinsame Vertriebsinfrastruktur (Art. 17a PBG)

¹ Die Unternehmen nach Artikel 17a Absatz 1 PBG betreiben gemeinsam die für die Erbringung von Reservations-, Verkaufs-, Abrechnungs- und Einnahmeverteilungsleistungen sowie für Kontrollfunktionen erforderlichen Systeme (Vertriebsinfrastruktur) und entwickeln diese bedürfnisgerecht weiter.

² Unternehmen, die den direkten Verkehr nach Artikel 16 PBG anbieten, müssen sich der Vertriebsinfrastruktur anschliessen. Weiteren konzessionierten Unternehmen sowie Unternehmen mit einer Bewilligung nach Artikel 7 oder 8 PBG ist der Anschluss zu diskriminierungsfreien Bedingungen zu gewähren.

³ Die Vertriebsinfrastruktur umfasst mindestens das Fahrausweissortiment des direkten Verkehrs nach Artikel 16 Absatz 1 PBG.

⁴ Zu den für den Vertrieb erforderlichen **Sach- und Personendaten** gehören insbesondere Fahrausweissortimente, Tarife, Kundendaten, beanspruchte Leistungen der Kunden sowie Kontrolldaten.

Beispiel 1: Reise im Inland (Bern – Poschiavo)

- Mehrere Unternehmen → Datenaustausch («Bekanntgabe»)
- Wann, wer, von wo nach wo, welcher Reiseweg? → Profiling!
- Zahlung jetzt oder später? Zahlungsmittel?
- Abonnemente, Ermässigungen?
- Alter?
- Wesentliche andere Nebenleistungen – oder nur unwesentliche? Abgrenzung?
- Kombiangebot, z.B. mit Mietwagen, Mobility?
- Besonders schützenswerte Personendaten? Rollstuhl, «Blindenausweis», IV-Ermässigung?
- Aufbewahrungsdauer der Daten; wie lange werden sie wirklich benötigt?
- Weitergabe an Dritte?



Beispiel 2: Reise ins Ausland (Schwarzenburg – München)

Im Wesentlichen die gleichen Fragestellungen wie bei Reisen im Inland

Zusätzliche Komplikationen:

- Mehrere Länder betroffen (hier sogar drei)
- EU-Staaten D und A → DSGVO
- Zusammenarbeit BLS – SBB – ÖBB - DB
- Datenbearbeitung im Ausland
- Datenbekanntgabe im Ausland
- Grenzpolizei
- Schengen
- etc.



Beispiel 3: Kauf Halbtax-Abonnement

- Persönlicher Ausweis → anonymes Reisen bzw. unpersönliche Ausstellung ist nicht möglich.
- Mehrere Unternehmen → Datenaustausch («Bekanntgabe»)
- Zahlung, Zahlungsmittel
- Alter? → Preis
- Besonders schützenswerte Personendaten? Rollstuhl, «Blindenausweis», IV-Ermässigung?
- Aufbewahrungsdauer der Daten: Wie lange werden sie wirklich benötigt?
- Weitergabe an Dritte?
- Verknüpfung mit Schwarzfahrerdatenbank?
- Etc.



Probleme, Diskussion, Fragen...?

Vielen herzlichen Dank!

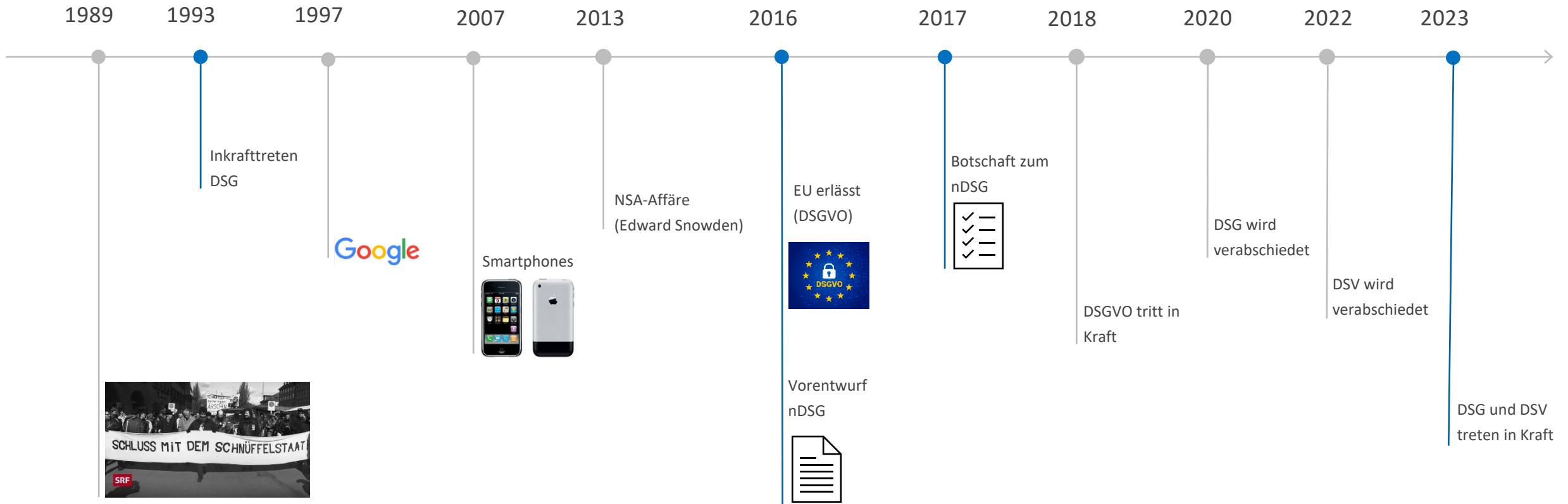
Umsetzung des neuen DSGVO – Kernpunkte und Aufpassfelder

Anselm Filliger, Datenschutzberater, SBB (RC-T)

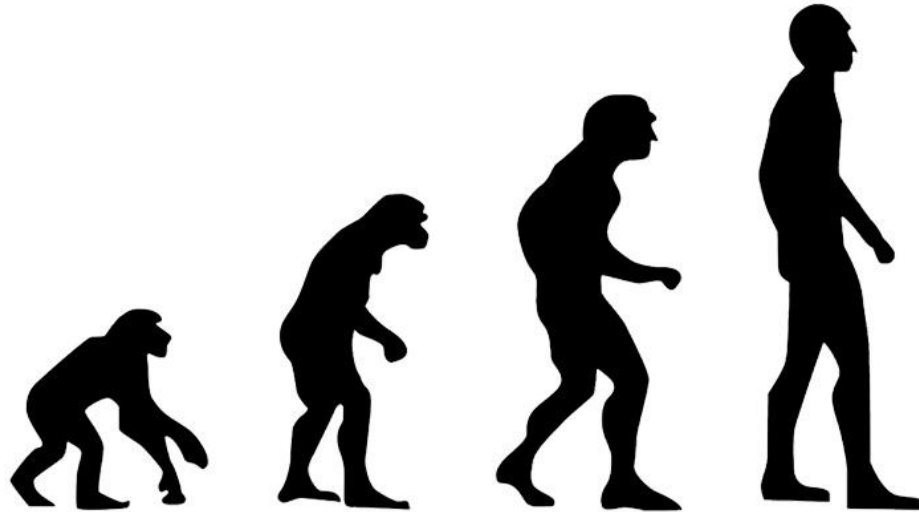
Agenda

- Das neue DSG (Herkunft / Stossrichtung)
- Die neuen Anforderungen des DSG
- Wichtigste Änderungen und Umsetzung der Kernpunkte: Die «neue» Rolle der TU

Gesetzgebungsprozess DSGVO



Stossrichtung des neuen DSGVO



Keine Revolution, sondern Evolution

- **Datenschutzgrundsätze** bleiben gleich
 - Rechtmässigkeit
 - Treu und Glauben
 - Verhältnismässigkeit
 - Zweckbindung
 - Datenrichtigkeit
 - Datensicherheit
 - Nur noch **natürliche Personen** werden geschützt
 - Von einer «statischen» Betrachtung zu einer mehr **«dynamischen» Sichtweise**
- ➔ Im einfachen **Tagesgeschäft** keine Änderungen spürbar. Aber....

Wichtigste Änderungen und Umsetzungspunkte des neuen DSGVO

- Neue **Dokumentationspflichten**: Datenbearbeitungsverzeichnis (DBV)
- «Neue» **Governance**: Datenschutzberater
- Neue **Prozesse**: Datenschutz-Folgenabschätzung (DSFA), Privacy by Design, Meldungen von Verletzungen der Datensicherheit
- Neue **Begriffe**: Profiling, automatisierte Einzelentscheide
- Neue **Bussen**
 - Information
 - Auskunft
 - Auftragsbearbeitung
 - Auslandstransfer
 - Datensicherheit (Protokollierung)

Neue Dokumentationspflicht: Datenbearbeitungsverzeichnis (DBV)

- DBV als Dreh- und Angelpunkt des neuen DSGVO: Dokumentationspflicht und Betroffenenrechte
- Nicht mehr Datensammlung (statisch), sondern Bearbeitung (dynamisch, prozessbezogen)
- Mindestinhalt:
 - Identität des Verantwortlichen
 - Zweck der Bearbeitung
 - Kategorien der Betroffenen (Mitarbeiter, Kunden); Kategorien der Personendaten (Stammdaten, Gesundheitsdaten, etc.)
 - [Aufbewahrungsdauer](#) (Löschkonzepte)
 - Massnahmen zur Gewährleistung der Datensicherheit
 - Bei Auslandstransfer: [Zielland](#) sowie Garantien (bei sog. unsicheren Drittstaaten)
- Keine Formvorschriften (Tool, Excel, Papier)
- Vorgehen: Wo haben wir Personendaten (Applikationen)? Wer bearbeitet Personendaten (Prozesse)?
- Jedes **Bundesorgan** (heisst: jedes TU) muss ein **DBV führen** und **dem EDÖB melden** (die KMU-Ausnahme greift nicht)
 - Ausschliesslich Datenbearbeitungen nach PGB sind zu melden (keine HR-Bearbeitungen)
 - [Meldeportal des EDÖB](#) (über EDÖB werden Anmeldungen öffentlich)

«Neue» Governance: Datenschutzberater / Weisung

- Jedes **Bundesorgan** muss **einen** Datenschutzberater ernennen. (Mehrere **Bundesorgane** können **gemeinsam** einen Datenschutzberater ernennen.)
- Der Datenschutzberater übt seine Funktion **fachlich unabhängig** und **weisungsungebunden** aus.
- Die **Verantwortung** für den Datenschutz trägt das «Business» und zwar derjenige, der über Mittel und Zweck der Bearbeitung entscheidet.
- **Weisung** zum Datenschutz (empfehlenswert):
 - Grundsätze (Bearbeitungsgrundsätze, Privacy by Design, ...)
 - Rollen / Verantwortlichkeiten (DSB, Verantwortlicher der Datenbearbeitung, ...)
 - Prozesse (z.B. Meldung von Vorfällen, DSFA, Auskunft, ...)

Neue Prozesse: Datenschutz-Folgenabschätzung (DSFA), Privacy by Design, Meldung von Verletzungen der Datensicherheit

- **Privacy by Design**: Datenschutz **ab Planung**. Datenschutz **durch Technik** (und Organisation)
- **DSFA**: dokumentierte Bewertung von risikoreichen Datenbearbeitungen
 - Was wollen wir machen? (Geplante Bearbeitung)
 - Welches sind die **Risiken für die Betroffenen**? (Risikobewertung)
 - Wie minimieren wir die Risiken? (Massnahmen zum Schutz der Persönlichkeit und Grundrechte)
 - Verbleibt ein hohes Risiko? **Konsultation des EDÖB**
- Meldung von **Verletzungen der Datensicherheit** an den EDÖB

Neue Begriffe: Profiling, automatisierte Einzelentscheide

- **Profiling**: jede Art der **automatisierten Bearbeitung** von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte **persönliche Aspekte**, die sich auf eine natürliche Person beziehen, zu **bewerten**, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu **analysieren** oder **vorherzusagen** (Art. 5 lit. f DSGVO)
- **Profiling mit hohem Risiko**: Profiling, das ein **hohes Risiko** für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer **Verknüpfung von Daten** führt, die eine **Beurteilung wesentlicher Aspekte der Persönlichkeit** einer natürlichen Person erlaubt (Art. 5 lit. g DSGVO)
- Rechtsfolgen:
 - Für **Private**: Praktisch keine Rechtsfolgen
 - Für **Bundesorgane**: Gesetzliche Grundlage
- **Automatisierte Einzelentscheidung**: eine Entscheidung, die **ausschliesslich** auf einer **automatisierten Bearbeitung** beruht und die für sie mit einer **Rechtsfolge** verbunden ist oder sie **erheblich beeinträchtigt**
- Rechtsfolgen:
 - Für **Private**: Informationspflicht, «menschliches» Gehör
 - Für **Bundesorgane**: Gesetzliche Grundlage, Kennzeichnung der Verfügung

Neue Bussen (Sanktionen)



- Verschärfte Sanktionen (Bussen)
- **Ausgewählte Tatbestände**
 - Informationspflicht
 - Auskunftsrecht
 - Auftragsdatenbearbeitung
 - Auslandstransfer
 - Datensicherheit (Protokollierung)
- Nur bei Vorsatz (**Eventualvorsatz**)
- Bussen zielen auf **handelnde Personen** (nicht auf Unternehmen ab)

Informationspflicht

- **Wo und wie:** Angemessene Information
 - Mitteilung in präziser, transparenter, verständlicher und leicht zugänglicher Form
 - Keine Formvorschriften (Text, Piktogramm, mündlich)
 - GDSE
 - Datenschutzerklärung für Kunden (Internet)
 - Datenschutzerklärung für Mitarbeitende (Intranet, oder OnePager) und Stellenbewerbende
 - Datenschutzerklärung für Websites-Besucher
- **Wann:** Beschaffung von Personendaten (planmässige Erheben von Personendaten)
- **Was:** Mindestinhalt:
 - Identität und Kontaktdaten des Verantwortlichen (Firma, Domizil)
 - Bearbeitungszweck
 - Kategorien der Empfänger
 - Bekanntgabe ins Ausland: **Zielland** und Garantien (bei unsicheren Drittländern)
 - automatisierte Einzelentscheide:
- **Bundesorgane:** Die Informationspflicht entfällt, wenn die Bearbeitung gesetzlich vorgesehen ist.
 - Aber: TU sind Unternehmen, Kundenbeziehungen, Treu und Glauben

Auskunft

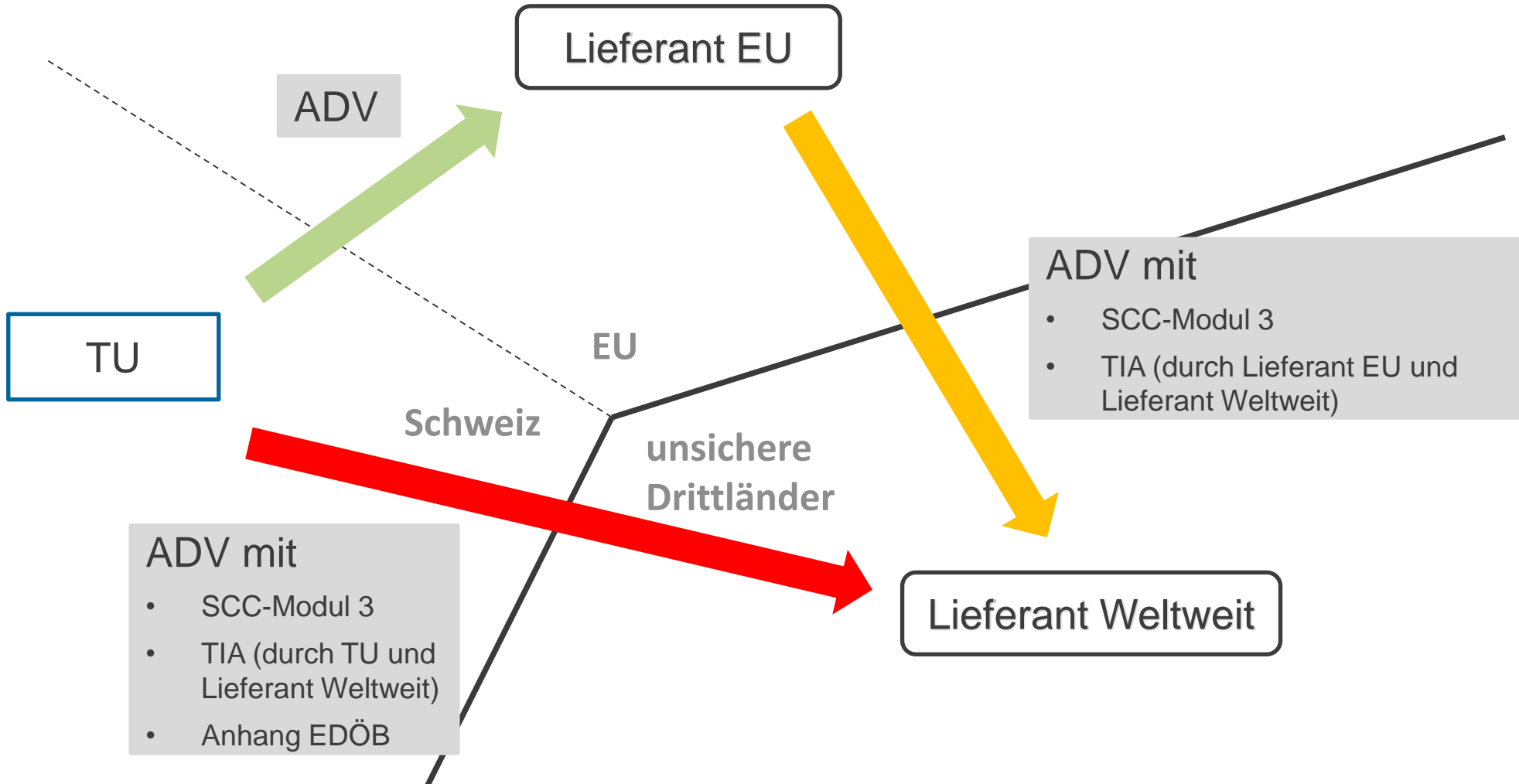
- **Ziel:** Betroffenen erhalten Information, damit sie ihre Rechte nach DSGVO (Löschen, Berichtigen) geltend machen können und eine transparente Datenbearbeitung gewährleistet ist
- **Mindestinhalt:**
 - Identität und Kontaktdaten des Verantwortlichen
 - die bearbeiteten Personendaten als solche
 - Bearbeitungszweck
 - **Aufbewahrungsdauer**
 - Angaben über die Herkunft der Daten
 - Automatisierte Einzelentscheidung: Logik, auf der die Entscheidung beruht
 - Kategorien der Empfänger
 - **Zielländer**
- Innert **30 Tagen** zu beantworten
- **Umsetzungshilfen:**
 - Prozess festlegen (z.B. in Richtlinie, Weisung)
 - Sicherstellen, dass Daten gefunden werden, gelöscht und berichtigt werden können
 - Standardschreiben verfassen
 - **Keine Vollständigkeit zusichern!**

Auftragsbearbeitung



- **Auftragsbearbeitung** verlangt zwingend (!) einen **Vertrag** (ADV)
 - Zweckbindung
 - Geheimnisschutz
 - Gewährleistung der Datensicherheit
- **Was ist zu tun?**
 - Welche Verträge haben wir?
 - Liegt eine Auftragsbearbeitung vor?
 - Liegt ein ADV vor?
 - Datensicherheit angemessen?
 - Bei Bedarf: Nachrüsten

Auslandstransfer



Datensicherheit (Protokollierung)

- **Umfang:** das Speichern, Verändern, **Lesen**, Bekanntgeben, Löschen und Vernichten der Daten ist zu protokollieren und müssen **mindestens 1 Jahr** getrennt vom Ursprungssystem aufbewahrt werden.
- **Private:** automatisierte Bearbeitung **besonders schützenswerte Personendaten** in grossem Umfang oder **Profiling mit hohem Risiko** - wenn sonst nachträglich nicht festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie beschafft oder bekanntgegeben wurden
- **Bundesorgane (jedes TU):** keine Eingrenzung, **jede Personendatenbearbeitung** muss protokolliert werden
- **Auftragsbearbeiter (Lieferanten):** der Auftraggeber hat seine Protokollierungspflichten dem Auftragnehmer zu überbinden
- **Übergangsfristen für Bundesorgane:** innert 3 Jahren umzusetzen
- **Kosten / Verhältnismässigkeit / Umsetzung:** risikobasierter Ansatz

Vielen Dank für Ihre Aufmerksamkeit

Fragen?

PAUSE



VÖV UTP

Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

Leitfaden zur korrekten Umsetzung des DSGVO

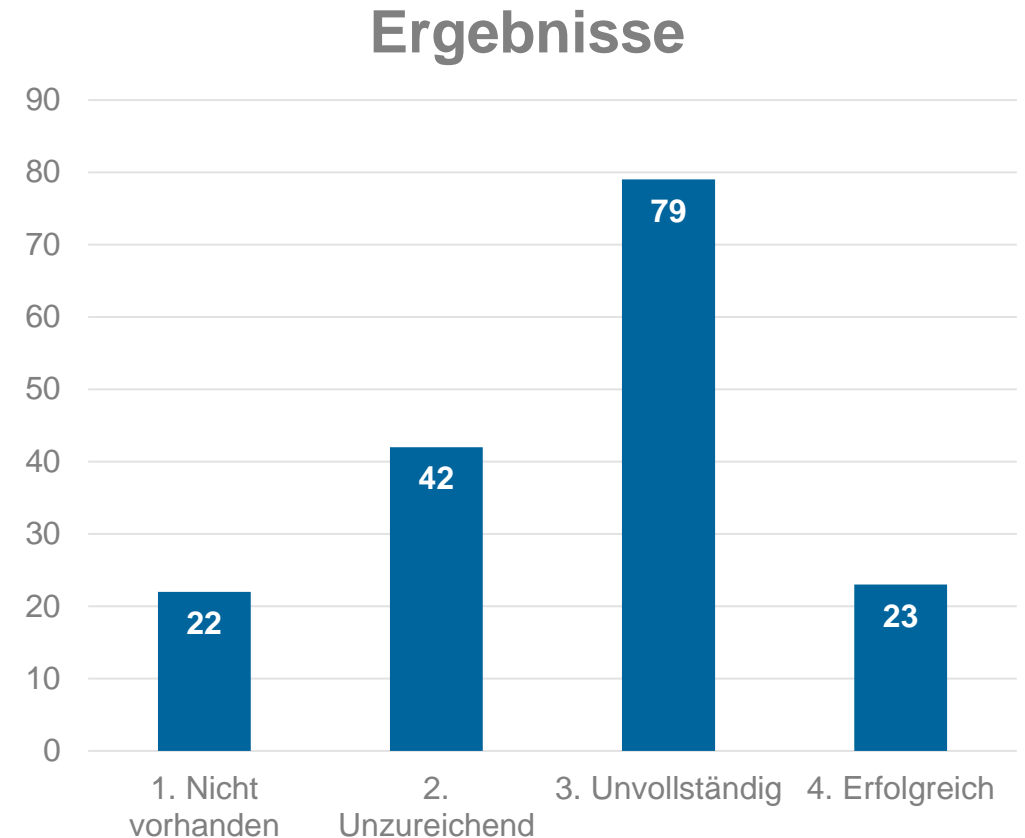
Tim Loosli, Alliance SwissPass

Philippe Kaufmann, Alliance SwissPass

Christian Sterchi, VÖV

Erste Ergebnisse Audit

- Prüfung von rund 230 Datenschutzerklärungen der Mitglieder der Alliance SwissPass
 - DSE wird anhand Online-Umfrage-Tool bewertet
 - 4 mögliche Outcomes:
 1. Nicht vorhanden
 2. Unzureichend
 3. Unvollständig
 4. Erfolgreich
- Aktuell 172 Datenschutzerklärungen geprüft
 - Etwa gleich viele haben gar keine DSE wie eine erfolgreiche haben (je ca. 14%)



Am häufigsten fehlen

Gemeinsame
Verantwortlichkeit
109 (67.7%)

Datenspeicherort
106 (64.6%)

Kundenversprechen
105 (62.5%)

Marktforschungsmassnahmen
103 (62.4%)

Prozesse der
Datenbearbeitungen

Am besten umgesetzt werden

Cookies werden mehr oder weniger gut ausgeführt

Personenrechte
verhältnismässig auch bei
unvollständigeren DSE eher
noch vorhanden

Korrekte Marketing-Permission
(schwierig beurteilbar)

Checkliste Datenschutz

- Auf der Website des VÖV und von Alliance SwissPass stellen wir eine Checkliste zur Verfügung, die die Transportunternehmen und Verbände bei der Umsetzung des neuen Datenschutzgesetzes mit Empfehlungen unterstützen soll.
- Sie ist gegliedert in vier Oberthemen
 - Datenbearbeitung klären
 - Prozesse definieren
 - Datenschutzerklärung überarbeiten
 - Datenschutzkonforme Website erstellen

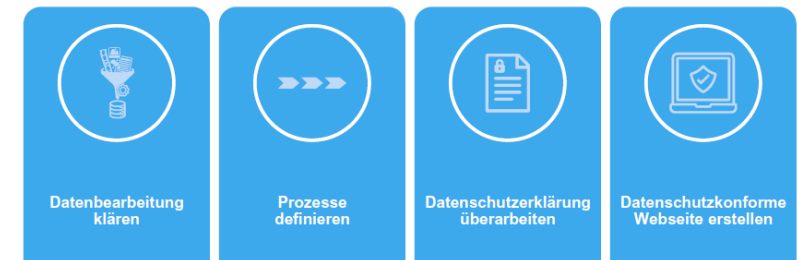


Umsetzung neues Schweizer Datenschutzrecht: Datenschutz-Checkliste

Ist Ihr Transportunternehmen bezüglich Datenschutzgesetz up to date?

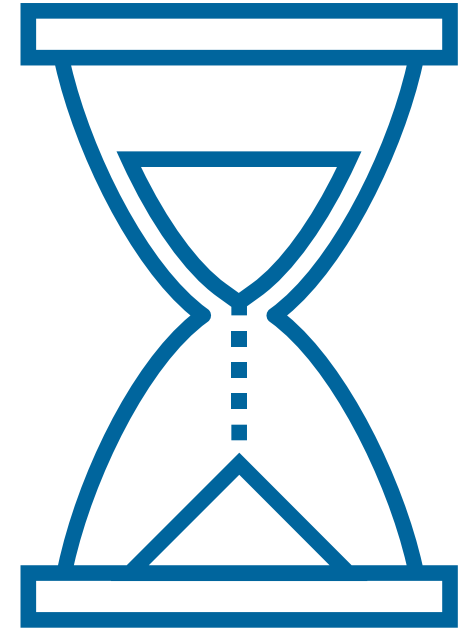
Das Schweizer Datenschutzgesetz (DSG) wurde revidiert und trat am 1. September 2023 in Kraft. Damit ändern sich wichtige Bestimmungen über die Bearbeitung von Personendaten. Im vorliegenden Dokument machen wir Sie auf die bevorstehenden Änderungen aufmerksam und bieten einen Überblick über die notwendigen Datenschutzmassnahmen. Detaillierte Bestimmungen zum Datenschutz sind in den Branchen-Regelwerken ([Regelwerk Gemeinsame Datenschutzerklärung Alliance SwissPass \[GDSE\]](#) und [Regelwerk Datennutzung öV \[ReDöV\]](#), auf der Webseite der Alliance SwissPass mit Login aufrufbar) ausführlich festgehalten.

Damit Ihr Transportunternehmen konform mit dem neuen Schweizer Datenschutzrecht ist, müssen vier Aspekte beachtet werden.

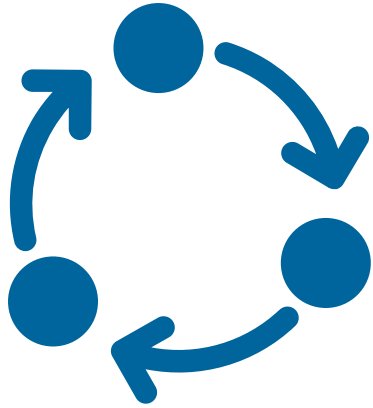


1. Datenbearbeitung klären

- Datensicherheit sicherstellen durch geeignete **technische und organisatorische Massnahmen**
- **Verantwortliche Person Datenschutz ernennen** (Empfehlung)
- **Datenverarbeitungsverzeichnis** erstellen
(Ausnahme für Unternehmen mit <250 Beschäftigten, sofern kein hohes Risiko für Verletzungen der Persönlichkeit)
- **Datenübermittlung prüfen**
- **Verträge prüfen** und ggf. **überarbeiten**



2. Prozesse definieren



- **Prozess für Auskunfts- und Lösungsbegehren erstellen**
 - **Meldeverfahren für Verletzungen des Datenschutzes einführen**
 - Prozess für die **Datenschutz-Folgenabschätzungen** etablieren
-
- **Periodische Bestandsaufnahme** inkl. **Löschung oder Anonymisierung** aller personenbezogenen Daten, sobald sie für den Zweck, der deren Bearbeitung rechtfertigte, nicht mehr benötigt werden.

3. Datenschutzerklärung erstellen oder überarbeiten

- **Datenschutzerklärung erstellen** bzw. überarbeiten

Die gemeinsame Datenschutzerklärung der Branche ist hier zu finden:

<https://www.allianceswisspass.ch/de/branchen-dienstleistungen/Datenmanagement>



- Die Datenschutzerklärung muss auf der Webseite **einfach auffindbar** sein!

4. Datenschutzkonforme Webseite

- **Website verschlüsseln** (Empfehlung)
- **Cookie-Banner einbinden** (Empfehlung)
- **Social-Media-Plug-Ins prüfen**



Datenverarbeitungsverzeichnis



- Welche Daten werden wo, wie lange und zu welchem Zeitpunkt gespeichert?
 - Was ist der Zweck der Datenverarbeitung?
 - Werden Personendatenbearbeitungen ausgelagert?
 - Wo ist der Bearbeitungsort (bzw. Serverstandort)?
 - Wer ist für die Datenbearbeitung verantwortlich?
- Die Geschäftsstelle Alliance SwissPass und der VöV bieten den TU und Verbände eine Vorlage an!

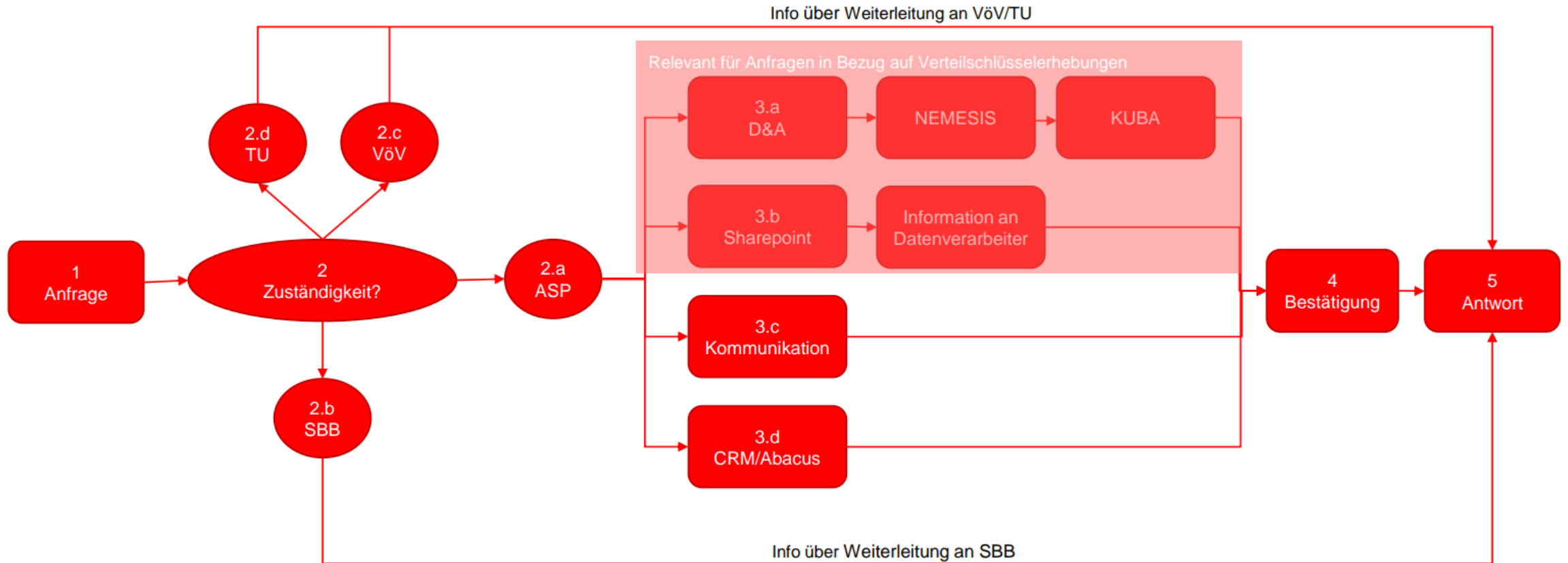
Vorlage Datenverarbeitungsverzeichnis (Teil 1)

Bezeichnung der Datenverarbeitungstätigkeit	Zweck der Verarbeitung	Rechtmässigkeit	Datenverarbeiter	Datenverantwortlicher	Weitergabe an Dritten
	<i>Was ist der Bearbeitungszweck?</i>	<i>Was ist der Erlaubnistatbestand?</i> - Einwilligung - Überwiegendes Interesse - Gesetz - Auftrags- / Vertragserfüllung	<i>Wer verarbeitet die Daten?</i>	<i>Wer ist für die Daten verantwortlich?</i> - jeweiliges Transportunternehmen - öV-Branche	<i>Die Informationspflicht verlangt die Nennung sämtlicher Empfänger von Daten.</i>
Bspw. Personalwesen intern	Das Personalwesen kümmert sich um alle Interessen und Abläufe, die im Zusammenhang mit dem Personal entstehen.	Auftrags- / Vertragserfüllung	TU X	TU X	Nein

Vorlage Datenverarbeitungsverzeichnis (Teil 2)

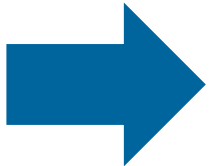
Personenbezogene Daten?	Personenkategorie	Datenkategorie	Aufbewahrungsdauer	Speicherort	Abteilung
<p><i>Handelt es sich um personenbezogenen Daten?</i></p> <p><i>Welche Personen sind betroffen?</i></p> <p><i>Welche Daten sind betroffen?</i></p> <p><i>Daten müssen gelöscht werden, sobald sie für die Erfüllung des Zwecks, zu dem sie erhoben wurden, nicht mehr erforderlich sind.</i></p> <p><i>Der Ort der Datenspeicherung ist zu nennen.</i></p> <p><i>Welche Abteilung ist verantwortlich?</i></p> <p><i>Personenbezogene Daten = Daten / Informationen mit direktem oder indirektem Bezug zu einer natürlichen Person</i></p>					
Ja	Mitarbeitende	<ul style="list-style-type: none"> - TU Kürzel - TU Bezeichnung - Nachname - Vorname - E-Mail <p>Die Aufzählung ist nicht vollständig.</p>	Die Daten werden nicht gelöscht, sondern unbefristet archiviert.	Datenbank der TU X	HR

Prozess für Auskunft- und Lösungsbegehren



Weitere Infos

- Die Checkliste finden Sie hier:
 - <https://www.voev.ch/de/Service/Recht-Datenschutz-und-Monitoring#Datenschutz>
 - [Datenmanagement im öV Schweiz - Alliance SwissPass](#)
- Bei Fragen zu Themen wie Datenschutz und anderen rechtlichen Themen stehen wir unter recht@voev.ch / datenschutz@allianceswisspass.ch gerne zur Verfügung



Halbjährlich aktualisiertes Rechtsmonitoring auf unserer Homepage verfügbar.

Vielen Dank für Ihre Aufmerksamkeit

Fragen?

Podiumsdiskussion