Zusammenfassung

Datenschutzrecht Master

- *Einführung in Thematik*
- *Verfassungsrechtlicher und zivilrechtlicher Persönlichkeitsschutz*
- *Datenschutzrecht des Bundes im Überblick*
- *Datenschutzrechtliche Grundsätze*
- *Transfer von Personendaten ins Ausland*
- *Personendatenbearbeitung durch Bundesorgane und Private*
- *Rechte Einzelner*
- *Aufsicht und Verfahren*
- *Europäischer Datenschutz*
- *Kantonaler Datenschutz*
- *Schengener Datenschutzgesetz*
- *das totalrevidierte DSG*

Einführung/Grundlagen

z.B. Online-Bewerbung (Einreichung auf Online-Plattform) bei Firmen.

z.B. Erstellen eines Profils auf Social Media – der Anbieter hat Daten der Benutzer.

z.B. Angaben von Daten (Wohnort, Telefonnummer, etc.) im Restaurant wegen dem Contact Tracing. Covid-Verordnung bestimmt, dass die Daten angegeben werden müssen.

z.B. Überwachung durch Kameras im öffentlichen Raum (muss den Personen eröffnet werden, dass sie überwacht werden) Prinzip der Transparenz im Datenschutzrecht

„Data Breaches“ – Anhäufung von ungeschützt zugänglichen Personendaten und Schaden der Privatsphäre; Datenpanne bei Swisscom.

E-ID Abstimmung: Umstritten ist die Aufgabenteilung zwischen Staat und Privaten und mithin der Datenschutz. E-ID-Anbieter muss Antrag einer Privatperson an den Staat/Fedpol weiterleiten. Der E-ID Anbieter wird von einer unabhängigen Aufsichtsbehörde überwacht.

E-ID: Datenbekanntgabe an einen Online-Dienstanbieter durch E-ID-Anbieter ist nur dann erlaubt, wenn dies für die Identifizierung der betreffenden Person beim Dienstanbieter zur Erfüllung vertraglicher Pflichten notwendig ist und der Nutzer vor der ersten Datenweitergabe informiert wurde. Diese Datenbekanntgabe muss in einer Vereinbarung zwischen IdP und Onlinedienstanbieter geregelt und dem EDÖB zur Prüfung vorgelegt werden.

Datenschutz: Geschützt werden nicht die Daten, sondern die Personen, über die Daten bearbeitet werden. Siehe Art. 1 DSG („Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen…“)

Datenschutzrecht: Rechtsnormen, welche dem Schutz der Persönlichkeit und der informationellen Selbstbestimmung dienen sowie Formen oder Zwecke der Bearbeitung von Personendaten regeln. Das Recht regelt, was man darf (erlaubte Datenbearbeitung) bzw. nicht darf.

Personendaten (3a DSG): Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Personendaten regeln die Anwendung des Datenschutzgesetzes – bzw. kommt das DSG zur Anwendung, wenn Personendaten bearbeitet werden.

Personendaten – dürfen nach 4 DSG nur rechtmässig bearbeitet werden

Personendaten als Objekt der Bestimmungen über die Bearbeitung von Personendaten durch private Personen (12 ff. DSG) und Bestimmungen von Personendaten durch Bundesorgane (16 ff. DSG)

Elemente: Müssen bejaht werden, damit man von Personendaten sprechen kann.

- *Angaben/Informationen oder Aussagen*

Es spiel keine Rolle, ob es sich um objektive (Namen, Beruf, Vermögenssituation, Blutgruppe) oder um subjektive Angaben (Werturteile, Angaben zur Kreditwürdigkeit, Angaben zur Arbeitsleistung im Arbeitszeugnis) handelt. Auch Angaben, die die betroffene Person selber an die Öffentlichkeit bringt, sind „Angaben“

z.B. Finger an sich ist kein Personendatum – sondern ein Träger eines Personendatum. Der Fingerabdruck ist aber eine Angabe

Auch ein Werturteil über eine Person (z.B. Beurteilung über den Arbeitnehmer) ist eine Angabe

- *Personenbezug (Angaben weisen Personenbezug auf)/über eine Person*

Personenbezug liegt vor, wenn die Angabe einen hinreichenden Personenbezug hat. Hinreichend ist der Bezug, wenn sich die Information ihrer Natur nach auf eine Person bezieht. Ein Personenbezug liegt vor, wenn Angaben vorliegen, die nicht personenbezogene Angaben zum Inhalt haben, aber aufgrund ihres Kontext oder Zusatzinformationen auch Aussagen über Personen enthalten (wie Sitzungsprotokolle oder Unfallberichte).

Medizinische Ergebnisdaten im Patientendossier (sofern eine Person identifiziert werden kann) oder Fingerabdruck haben einen Personenbezug. Im Patientendossier ist der Datenschutz betroffen, weil die Daten einer Person zugeordnet werden kann.

Foto eines falsch parkierten Autos kann einen Personenbezug haben wegen dem Kennzeichen auf dem Auto (Person kann identifiziert werden) Es wird nicht direkt eine Person fotografiert, jedoch lässt sich aus dem Foto ein Bezug zu einer Person herstellen.

Schätzwert einer Immobilie kann einen Personenbezug haben, wenn man auf dem Dokument z.B. den Eigentümer feststellen kann.

Höhe eines Berges ist per se nicht Personenbezogen – es handelt sich um die Messung eines Objektes. Jedoch kann die Angabe einen Personenbezug haben, wenn z.B. eine Person mit einer GPS-Uhr eine Messung macht (Bergtour mit Garmin-Uhr)

- *Bestimmtheit oder Bestimmbarkeit der Person.*

Bestimmbarkeit einer Personenangabe liegt dann vor, wenn aufgrund der vorhandenen Angaben auf die Identität der entsprechenden Person geschlossen werden kann.

Nicht jede theoretische Möglichkeit der Identifizierung führt zum Erfüllen der „Bestimmbarkeit". Ist der Aufwand für die Bestimmung der betroffenen Personen derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird, liegt keine Bestimmbarkeit vor.

Um die Bestimmbarkeit zu beurteilen, **muss aus der Sicht der Person, welche die Angaben bearbeitet, beurteilt werden**. Abzuklären ist, ob der Datenbearbeiter oder ein Dritter mit Hilfe der ihm zur Verfügung stehenden technischen Mittel **in der Lage wäre, die Person aufgrund der vorhandenen Angaben ohne übermässigen Aufwand zu identifizieren**.

IP-Adressen sind Personendaten, da sie die Kommunikation zwischen Computern ermöglichen. Über die IP-Adressen können Personen identifiziert werden, weshalb es auch einen Personenbezug gibt. Die Personen sind zudem bestimmbar (der Aufwand ist nicht derart gross) – in einem Fall einer Urheberrechtsverletzung konnte der Staatsanwalt den Verletzer mittels technischen Mitteln identifizieren.

Sachlicher Geltungsbereich

DSG regelt das Bearbeiten von Daten (Personendaten) von natürlichen und juristischen Personen.

DSG ist anwendbar für juristische Personen (2 Ziff. 1 DSG). Zu den juristischen Personen gehören Personen, denen das Zivilrecht Rechtspersönlichkeit zuspricht – Vereine, Stiftungen, Aktiengesellschaften, GmbHs, Genossenschaften, etc.

Aber auch öffentlich-rechtliche Anstalten und Körperschaften des öffentlichen Rechts – wenn ihnen Zivilrechtsfähigkeit zuerkannt wird, aber auch Personengesellschaften ohne Rechtspersönlichkeit – sofern sie gegen aussen rechtsfähig sind (Kollektiv- und Kommanditgesellschaft, Stockwerkeigentümergemeinschaft)

a) Besonders schützenswerte Personendaten (3 lit. c DSG) und b) Persönlichkeitsprofil (3 lit. d DSG)

a) Unterkategorie von Personendaten. Diese geniessen einen höheren Schutz, insbesondere bei der Bearbeitung. Prüfkriterium ist nur, ob es sich um eine Angabe nach 3 lit. c DSG handelt.

b) Sammlung mehrerer Angaben über eine bestimmte oder bestimmbare natürliche Person, welche für sich alleine keine besonders schützenswerte Personendaten darstellen,

zusammengenommen aber eine Beurteilung wesentlicher Aspekte der Persönlichkeit ermöglichen.

Im DSG gibt es für solche Daten strengere Bearbeitungskriterien (sowohl für Private als auch für Bundesorgane)

Besonders schützenswerte Daten kommen nur bei natürlichen Personen zur Anwendung – Personendaten über juristische Personen können dann besonders schützenswert sein, wenn sie ein weltanschaulich ausgerichtetes Unternehmen betreffen oder Daten über strafrechtliche Verfolgungen und Sanktionen beinhalten.

Persönlichkeitsprofile können nur aus Daten von natürlichen Personen erstellt werden.

Im Gegensatz zum DSG kennt der grundrechtliche Anspruch auf Schutz vor Missbrauch persönlicher Daten keine Unterscheidung zwischen gewöhnlichen und besonders schützenswerten Personendaten bzw. Persönlichkeitsprofilen. Bei den Voraussetzungen nach BV 36 muss dies aber berücksichtigt werden (insbesondere Verhältnismässigkeit)

„Bearbeiten“ 3 lit. e DSG

Jede Tätigkeit, die Personendaten betrifft, fällt in den Anwendungsbereich des DSG. Mit welchen Mitteln die Bearbeitung erfolgt, ist unerheblich – sowohl manuelle als auch automatisierte Bearbeitung fallen darunter.

„Bekanntgabe“ ist damit gemeint, dass jedes Verhalten darunter fällt, welches einem Dritten ermöglicht, Personendaten einzusehen.

Persönlicher Geltungsbereich des DSG

DSG regelt die Bearbeitung von Personendaten sowohl durch Privatpersonen als auch durch Bundesorgane. Massgeblich ist, ob das Verhältnis zur betroffenen Person hoheitlich ist oder nicht bzw. ist die Rechtstellung für die Qualifizierung massgeblich.

- Bundesorgane: Behörden und Dienststellen des Bundes, sowie Personen, die mit öffentlichen Aufgaben des Bundes betraut sind (3 lit. h DSG). Auf die Bearbeitung von Personendaten durch kantonale Organe ist das DSG nicht anwendbar – selbst wenn eine Kantonale/Kommunale Behörde eine Bundesaufgabe erfüllt oder Bundesrecht vollzieht, handelt es sich nicht um ein «Bundesorgan».

Erfüllt einer Privatperson eine kantonale Aufgabe, kommt das kantonale Datenschutzrecht zur Anwendung.

Das DSG setzt Eingriffe in Grundrechte (Voraussetzung nach BV 36) durch staatliche Organe (Bundesorgane) um.

Personendaten dürfen nur gestützt auf eine genügende Rechtsgrundlage bearbeitet werden, die Bearbeitung muss im öffentlichen Interesse liegen und verhältnismässig sein.

- Privatpersonen: DSG sieht vor, dass gewisse Bearbeitungen von Personendaten ohne Rechtfertigungsgrund zu einer Persönlichkeitsverletzung führen können (12 ff. DSG)

Räumlicher Geltungsbereich

Keine explizite Regelung vorhanden. Aber betreffend Vorschriften mit **öffentlich-rechtlichem** Charakter gilt das Territorialitätsprinzip (bei staatlicher Bearbeitung) Anknüpfungspunkt ist der Ort der Bearbeitung der Personendaten. Auch die Bekanntgabe ins Ausland fällt unter den Begriff der Bearbeitung. Ebenso anwendbar ist das DSG für Sachverhalte, die Auswirkungen in der Schweiz entfalten – z.B. das Aufschalten von Bildern, die in der Schweiz abrufbar sind.

Betreffend widerrechtlicher Datenbearbeitung **durch Private** ist mit Blick auf die fragliche Persönlichkeitsverletzung im internationalen Verhältnis IPRG 139 Ziff. 1 massgeblich; die Betroffenen haben ein Wahlrecht.

Ausschluss der Anwendung des DSG (2 Ziff. 2 DSG)

1) Privatgebrauch. Bearbeitungen, die eine natürliche Person ausschliesslich zum persönlichen Gebrauch vornimmt und nicht an Aussenstehende weitergibt. Das DSG soll nicht gelten, wenn eine natürliche Person im Privatbereich Daten bearbeitet. Z.B. sind Privatgespräche oder Tagebücher dem DSG entzogen bzw. fallen erst unter das DSG, wenn der Inhaber sich entschliesst, die Daten an Aussenstehende weiterzugeben.

Als „Aussenstehende" gelten Personen **ausserhalb des vertrauten Kreises**.

- Gespräche unter Arbeitskolleginnen und Geschäftspartner fallen nicht unter den Tatbestand des Privatgebrauchs. Wenn Personendaten betroffen sind, ist das DSG anwendbar

- Klatsch mit den besten Kollegen ist als Privatgebrauch von Personendaten zu qualifizieren, auch wenn Informationen an die besten Kollegen weitererzählt werden

2) Öffentliche Register des Privatrechts. (z.B. Grundbuch, Register für Schuldbetreibung, Zivilstandsregister, etc.) Solche Register werden durch kantonale Behörden umgesetzt bzw. unterliegen die kantonalen Behörden sowieso nicht dem DSG, sondern hier finden die kantonalen Datenschutzgesetzgebungen Anwendung.

3) Internationales Komitee vom Roten Kreuz.

4) Parlamentsverfahren.

5) Hängige Verfahren (2 Ziff. 2 lit. b DSG). Grund dafür ist, dass während solcher Verfahren selber Normen gibt bzw. das Verfahrensrecht die Rechte der Beteiligten regeln – z.B. St PO regelt selber, wie Strafbehörden mit den Daten der Betroffenen umzugehen haben.

Allgemeines (formelles) vs. Bereichspezifisches (materielles) Datenschutzrecht

- **Allgemeines Datenschutzrecht:** DSG (Regelt die grundrechtlichen und persönlichkeitsrechtlichen Regeln über die Datenbearbeitung)

Das DSG ist ein «Rahmengesetz». Speziell ist, dass die Grundsätze von 4 – 11 DSG sowohl für Private als auch für Bundesorgane gelten. Ab 12 ff. folgen spezifische Regeln für Private und ab 16 ff. DSG für Bundesorgane.

- **Bereichspezifisches Datenschutzrecht**: Regelt, welche Datenbearbeitungen möglich, eingeschränkt oder verboten sind.

Verwaltungsrecht: Die meisten Spezialgesetze zum Datenschutz finden sich im Verwaltungsrecht. Z.B. Ausländer- und Asylrecht, Polizei- und Staatsschutzrecht

Strafrecht: Strafbare Handlungen gegen den Geheim- oder Privatbereich (179), Verletzung des Berufsgeheimnis (321) oder Amtsgeheimnis

Ebenso gibt es im DSG strafrechtliche Bestimmungen.

Privatrecht: Relativ wenig spezialgesetzliche Normen – Die Personendatenbearbeitung ist grundsätzlich zulässig, solange die Regeln des DSG 13 ff. und ZGB 28 ff. respektiert werden.

Verhältnis von DSG und ZGB

Das Grundkonzept von 28 ZGB wird im DSG beibehalten. Jedoch sieht das DSG eine Konkretisierung vor in 4 ff. DSG bei den Bearbeitungsgrundsätze; wird einer dieser Grundsätze verletzt, so gilt die Vermutung, dass eine Persönlichkeitsverletzung vorliegt. Kommt es zu einer Verletzung, stehen sowohl die Rechtsbehelfe nach 28 ZGB und des DSG zur Verfügung.

Verhältnis von DSG und zwingenden Vertragsbestimmungen

Zum Teil gibt es im Vertragsrecht zwingende Bestimmungen, die zum DSG alternativ stehen. Z.B. 328b (Datenbearbeitung des Arbeitnehmers durch den Arbeitgeber).

Verhältnis von DSG und StGB

Zwischen 35 DSG (Verletzung der beruflichen Schweigepflicht) und 320/321 StGB besteht unechte Konkurrenz. Die Verletzung von 35 DSG wird von 320/321 StGB konsumiert.

Sonst besteht Normenkumulation; z.B. Verletzung von 179bis StGB (Aufnahme eines fremden nicht öffentlichen Gesprächs) ist gleichzeitig eine Verletzung von dem Grundsatz des DSG, dass Daten nur rechtmässig erhoben werden dürfen.

Verhältnis DSG und Spezialgesetz

1. Anwendung des DSG prüfen

DSG ist nicht anwendbar, wenn

- Datenbearbeitung durch kantonale Behörden (kantonales Datenschutzrecht ist anwendbar)

- keine Personendaten im Sinne des DSG

- Daten betreffen einen hängigen Prozess (Datenbearbeitung richtet sich nach dem Prozessrecht)

Wenn Anwendung DSG bejaht wird, muss der nächste Schritt geprüft werden

2. Prüfen, ob selbständige datenschutzrechtliche Ansprüche erhoben werden

Soweit Ansprüche aus 8, 20 oder 25 Ziff. 3 DSG erhoben werden, ist das DSG anwendbar. Das DSG ist jedoch nicht anwendbar, wenn ein Spezialgesetz die dem Einzelnen nach DSG zustehenden Rechte verweigert, einschränkt oder aufschiebt und diese Regeln im Einklang stehen mit der Verfassung und dem Völkerrecht. Vgl. 9 Ziff. 1 lit. a DSG.

Werden diese Ansprüche geltend gemacht und gibt es keine Ausnahmeregelung in einem Spezialgesetz, dann ist das DSG anwendbar.

Handelt es sich aber nicht um selbständige datenschutzrechtliche Ansprüche handelt (8, 20 oder 25 Ziff. 3 DSG), muss geprüft werden, ob das Spezialgesetz anwendbar ist. Ist es anwendbar, muss geprüft werden bzw. ausgelegt, ob sowohl das DSG als auch das Spezialgesetz die Rechtsfrage regelt. Ist dies der Fall, dass beide anwendbar sind, muss geprüft werden, welche Norm vorgeht. Sieht etwa das Spezialgesetz einen höheren Schutz vor, ist dies anwendbar.

Normenkollision DSG – Spezialgesetz

Es kann nur eine Bestimmung unter Ausschluss der anderen zur Anwendung kommen. Enthält das Spezialgesetz eine Kollisionsnorm, so ist nach dieser vorzugehen. Besteht keine Kollisionsnorm, so ist das Verhältnis zwischen den beiden Normen mit den allgemeinen Auslegungsregeln zu klären (lex specialis, lex posterior). Jedoch sind diese beiden Grundsätze mit Vorsicht anzuwenden – sonst träte das DSG als allgemeine Regel gegenüber den besonderen Regeln stets in den Hintergrund (lex specialis). Lex posterior meint, dass ein jüngeres Gesetz dem älteren vorgeht bzw. müsste das DSG meistens den jüngeren Normen weichen.

Massgebend ist, dass das Spezialgesetz der von der BV vorgegebenen und im DSG konkretisierten Grundsätzen der Datenbearbeitung hinreichend Rechnung getragen hat. Ist dies der Fall, kann das Spezialgesetz dem DSG vorgezogen werden.

Normenkumulation DSG – Spezialgesetz

Ergibt die Auslegung zweier Normen, dass keine der beiden Normen der anderen vorgeht, so liegt eine Normenkumulation vor.

Ergänzt die Spezialnorm etwa das DSG, so kann sowohl das DSG als auch die Spezialnorm kumulativ angewendet werden.

Fall «Vertrauensärztliche Beurteilung» 6B_1199/2016 Bereichspezifisches Datenschutzrecht

Vertrauensarzt X verlangt mit Beschwerde in Strafsachen beim BGer, dass er freizusprechen sei.

BGer ist Ansicht, dass X dem Berufsgeheimnis von 321 StGB untersteht. Mithin ist - entgegen den Vorbringen des Beschwerdeführers - auch der von einem Arbeitgeber eingesetzte Vertrauensarzt dem Berufsgeheimnis nach Art. 321 StGB unterstellt. Ob und in welchem Umfang der Arzt dem Arbeitgeber berichten darf, hängt davon ab, ob er seitens des Arbeitnehmers vom Geheimnis entbunden worden ist.

X argumentierte, dass der C ihn als «Berechtigter» ihn dazu ermächtigt hat, dem Arbeitgeber ein ärztliches Zeugnis zuzustellen (straffrei nach 321 Ziff. 2 StGB)

BGer: Vorliegend habe C. den Beschwerdeführer **nicht umfassend vom Berufsgeheimnis befreit.** Er habe ihn nur ermächtigt, der Arbeitgeberin einen üblichen arbeitsrechtlichen Bericht zuzustellen, welcher ausschliesslich Angaben darüber enthalte, ob und in welchem Umfang eine Arbeitsunfähigkeit bestehe, wie lange diese dauern werde und inwiefern die allfällige gesundheitliche Einschränkung einen konkreten Einfluss auf die Arbeitsfähigkeit habe. Der Beschwerdeführer habe den Tatbestand von Art. 321 StGB objektiv erfüllt, indem er der Arbeitgeberin **weitergehende Informationen** zukommen gelassen habe (Urteil, S. 16 f.).

Die Vorinstanz erwägt in diesem Zusammenhang, **es folge aus Art. 328b OR, dass der Arbeitgeber vom Vertrauensarzt nur diejenigen Angaben erheben darf, welche die Eignung des Arbeitnehmers für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsverhältnisses erforderlich sind**. Dazu gehören Tatsache, Dauer und Grad der Arbeitsunfähigkeit sowie die Antwort auf die Frage, **ob es sich um eine Krankheit oder einen Unfall handelt.** Die Diagnose dürfe indes nicht erhoben werden. Der Praxisleitfaden SAMW/FMH halte ausdrücklich fest**, dass das Arbeitsunfähigkeitszeugnis an den Arbeitgeber keine Diagnose** zu enthalten habe und der Arbeitgeber keinen Anspruch habe, diese zu erfahren.

1) 328b OR und 321 StGB müssen nebeneinander betrachtet werden. StGB 321 regelt, wer unter das Gesetz fällt. OR 328b regelt, was bearbeitet werden darf und was nicht.

- Der Vertrauensarzt unterliegt dem Berufsgeheimnis nach 321 StGB bzw. kann sich danach strafbar machen. Der Arzt braucht eine Einwilligung, damit er sich nicht strafbar macht.

- OR 328b regelt, inwieweit Personendaten über den Arbeitnehmer bearbeitet werden dürfen. Ebenso sind die Praxisleitfäden in Erwägung bezogen worden, die klar regeln, dass keine Diagnose an den Arbeitgeber gesendet werden darf.

Der Arzt musste wissen, dass er im Rahmen von 328b dies nicht tun durfte bzw. somit nach 321 vorsätzlich gehandelt hat.

2) Besonders schützenswerte Daten.

3) Ja, wegen 35 Ziff. 1 DSG – Verletzung der beruflichen Schweigepflicht. Hier liegen besonders schützenswerte Personendaten vor im Sinne von 35 Ziff. 1 DSG.

Der Arzt könnte sowohl nach 321 StGB und 35 Ziff. 1 DSG vorgehen. 321 StGB würde aber 35 Ziff. 1 DSG konsumieren.

Anonymisierung

Z.B. Entscheide des BGer (Namen werden nicht genannt) oder Polizeimeldungen.

Personendaten können durch die Anonymisierung dem Geltungsbereich des DSG entzogen werden (bzw. DSG findet **nicht Anwendung** bzw. kein Schutz). Vorausgesetzt wird, dass jeder Personenbezug der Angaben entfernt wird oder dass die Daten so bearbeitet werden, dass eine Re-Identifikation nur noch mit unverhältnismässig grossem Aufwand möglich ist. Zu beachten ist, dass z.B. nur mit Augenbalken oder Verwischung der Gesichter auf einer Abbildung die Identifikation der Person nicht ausschliesst, da die Person je nachdem aufgrund anderer Merkmale wie Kleider/Hintergrund bestimmbar bleibt.

Problem: Anonymität kann heute nicht mehr voll gewährleistet werden. In Fällen von Gerichtsentscheiden konnte die Anonymisierung nicht mehr gewährleistet werden. Leerstellen in den Urteilen sollten die Personen schützen. Mit der Verknüpfung von anderen Daten vom Bund kann die Anonymisierung aufgehoben werden (De-Anonymisierung mit «Linkage»)

Datenschutz vs. Transparenz in der Öffentlichkeit

Datenschutzbeauftragter meint, dass Transparenz wichtig sei bei gewissen Firmen. Auf der einen Seite begrüsst man die Transparenz, auf der anderen Seite muss der Datenschutz gewährleistet werden.

Pseudonymisierung

Verfahren, bei denen Personenbezogene Merkmale nicht entfernt werden, sondern ersetzt werden mit Codes. Es liegen **immer noch Personendaten** vor. z.B. AHV-Nummer.

Art. 3 DSG (Begriffe)

- BAG-APP; Smartphones mit APP tauschen ID-Codes via Bluetooth aus. Über Bluetooth können ID-Codes deutlich mehr als 1.5 Meter ausgetauscht werden. Aber es gibt Mechanismen, die exakt arbeiten mit der 1.5 Meter Regel.

A wird positiv getestet und bekommt einen Code. Der private Schlüssel von A wird an den *Server des BAG geschickt*. Das BAG kann aber den Schlüssel nicht A persönlich zuordnen. Die

Swiss-Covid App macht regelmässig Abfragen beim *BAG-Server*. Anhand der Codes erkennen die Apps von B und C – welche regelmässig Abfragen machen beim BAG-Server (Personen mit nahem Kontakt zu A), dass eine relevante Distanz vorlag. Sie werden von der App gewarnt. Die Apps von B und C können A nicht identifizieren.

Streitpunkt: Es stellte sich die Frage, ob das zu schaffende System eine Personenbearbeitungsanlage darstellt oder nicht (Anwendung des DSG oder nicht)

- AHV-Nummer. Neu gibt es seit 2008 die 13-stellige AHV-Nummer. Aufbau der Nummer: Code für CH, anonyme Zufallszahl und Prüfziffer. Die AHV-Nummer gibt ja trotzdem eine Angabe an über eine Person – der normale Bürger könnte die Nummer zwar nicht einer Person zuordnen, jedoch könnten die Behörden die Nummer einer Person zuordnen. Somit handelt es sich bei der AHV-Nummer um ein Personendatum – das DSG findet Anwendung.

Datenschutz-Gesetzgebung Bund-Kantone

Grundsatz: Es gilt das Prinzip der begrenzten Einzelermächtigung des Bundes nach BV 3 und 42 + Subsidiäre Generalkompetenz der Kantone (BV 3; Kantone üben alle Aufgaben aus, die nicht dem Bund übertragen sind)

Wenn der Bund in der BV keine Ermächtigung hat, sind die Kantone zuständig.

Zuständigkeit des Bundes

Einleitung Datenschutzgesetz: *Die Bundesversammlung der Schweizerischen Eidgenossenschaft, gestützt auf die Artikel 95, 122 und 173 Absatz 2 der Bundesverfassung nach Einsicht in die Botschaft des Bundesrates vom 23. März 19883, beschliesst: …* Die einzelnen Artikel erwähnen die Zuständigkeiten im Bereich des Datenschutzes nicht ausdrücklich, aber es ist unbestritten, dass sie die Kompetenzen zum Erlass datenschutzrechtlicher Bestimmungen miteinschliessen.

In BV 164 Ziff. 1 lit. g könnte sich die Kompetenz finden für das Datenschutzrecht («Organisation und das Verfahren der Bundesbehörden»)

Datenschutz ist öffentliches Recht. Im öffentlichen Recht haben Bund und Kantone Kompetenzen.

Zuständigkeiten der Kantone

Das eidgenössische Datenschutzgesetz ist nur anwendbar, wenn die Datenbearbeitung durch private Personen oder Bundesorgane erfolgt (2 Ziff. 1 DSG). Das Datenschutzgesetz des Bundes ist nicht einschlägig, wenn im Rahmen der öffentlichen kantonalen oder kommunalen Tätigkeit Personendaten bearbeitet werden. Hier kommt das kantonale Datenschutzrecht zur Anwendung.

Wichtig: Die Kantone sind auch bei der Anwendung des kantonalen Datenschutzrechts im grundrechtlichen Bereich an die BV gebunden sowie an das Völkerrecht.

Soweit die kantonalen/kommunalen Behörden Bundesrecht vollziehen, ist die kantonale Datenschutzgesetzgebung anwendbar, wenn das Bundesrecht keine abschliessende Regelung enthält und das kantonale Recht einen angemessenen Schutz gewährleistet. Kantonale und kommunale Behörden gelten nicht als „Bundesorgane", auch wenn sie im Zusammenhang mit Bundesaufgaben tätig werden.

Vorbehalt (37 DSG): Obwohl der Bund grundsätzlich nicht zuständig ist, die Datenbearbeitung durch kantonale Behörden zu regeln, gelten nach 37 DSG für die kantonalen Organe beim Vollzug des Bundesrechts 1-11a, 16, 17, 18-22 und 25 Ziff. 1-3 DSG, soweit keine kantonalen Datenschutzvorschriften bestehen, die einen angemessenen Schutz gewährleisten.

Abgrenzung zwischen dem eidgenössischem und kantonalem Datenschutzrecht

- privatrechtlicher und öffentlich-rechtlicher Datenschutz

- öffentliche Organe des Bundes und öffentliche Organe der Kantone

Es muss entschieden werden, ob das Verhältnis dem privaten oder öffentlichen Bereich, den eidgenössischen oder den kantonalen Behörden zuzuordnen ist.

Kantonales Organ bleibt auch ein kantonales Organ im Sinne des Datenschutzes, wenn es Bundesrecht vollzieht.

Das Datenschutzgesetz ist neben Privaten Personen auf Bundesorgane anwendbar nach 2 Ziff. 1 lit. b DSG. Bundesorgane sind nach 3 lit. h Behörden und Dienststellen des Bundes sowie Personen, soweit sie mit öffentlichen Aufgaben des Bundes betraut sind.

Verhältnis zwischen dem eidgenössischem und kantonalem Datenschutzrecht

- Bundesrecht bricht kantonales Recht nach 49 Ziff. 1 BV; Bundesrecht geht entgegenstehendem kantonalem Recht vor (derogatorische Kraft des Bundesrechts). Verstösst z.B. kantonales/kommunales Recht gegen Grundrechte der BV/Völkerrecht, so braucht es gar keinen Rückgriff auf BV 49 bzw. gelten die Grundrechte in der ganzen Rechtsordnung.

- Problem wegen Kompetenzkonflikten: Ist ein Bundesgesetz kompetenzwidrig, ist es für das BGer massgeblich wegen 190 BV.

Subsidiäre Anwendung des DSG

DSG ist nur anwendbar im Rahmen der Datenbearbeitung durch Bundesorgane oder durch Private. Auf die Datenbearbeitung durch kantonale oder kommunale Behörden kommt die kantonale Datenschutzgesetzgebund zur Anwendung.

37 Ziff. 1 DSG durchbricht die Grundsätze der verfassungsmässigen Kompetenzverteilung im Bereich des Datenschutzes. Obwohl der Bund grundsätzlich nicht zuständig ist, die Datenbearbeitung durch kantonale Behörden zu regeln, geltend nach 37 Ziff. 1 DSG Bestimmungen des DSG für die kantonalen Organe beim Vollzug des Bundesrechts die

aufgeführten Normen, soweit keine kantonalen Datenschutzvorschriften bestehen, die einen angemessenen Schutz gewährleisten.

Europäischer Datenschutz

Datenschutzverordnung der EU findet keine direkte Anwendung auf die Schweiz, aber die Schweiz ist angewiesen, dass ihr Datenschutz als Europa-Konform betrachtet wird, damit der Datenfluss funktionieren kann.

Auf Stufe Bund wurde der Datenschutz im Bereich Schengen umgesetzt, gewisse Kantone müssen noch nachziehen.

Verfassungsrechtlicher/Grundrechtlicher Persönlichkeitsschutz

1963 anerkannte BGer die persönliche Freiheit als ungeschriebenes Grundrecht und entwickelte sie in seiner Rechtsprechung weiter.

Persönliche Freiheit 10 Ziff. 2 BV (weitere Freiheiten betroffen - Persönlichkeitsentfaltung) und Recht auf Schutz vor Datenmissbrauch nach 13 Ziff. 2 BV sind relevant für den grundrechtlichen Persönlichkeitsschutz im Datenbereich.

Für die Datenbearbeitung ist sowohl 10 Ziff. 2 BV und 13 Ziff. 2 BV zu überprüfen. Werden über eine Person Daten gesammelt/bearbeitet, ist nicht nur die persönliche Freiheit betroffen, sondern auch die Privatsphäre.

13 Ziff. 2 BV gilt als besondere Datenschutzbestimmung bzw. wenn es um den Schutz vor Missbräuchlicher Datenbearbeitung geht. Jedoch kann die Art und Weise, wie Daten erhoben oder verbreitet werden, auch die persönliche Freiheit nach 10 Ziff. 2 BV betreffen- z.B. wenn 13 Ziff. 2 BV betroffen ist, aber die Datenbearbeitung auch gleichzeitig die Willens- und Urteilsfähigkeit eines Menschen beeinträchtigt oder durch die Datenbearbeitung in die körperliche Integrität eingegriffen wird oder durch die Datenbearbeitung der betroffene Mensch in seiner Gesundheit psychisch geschädigt wird. Das Verhältnis zwischen BV 13 und BVB 10 Ziff. 2 ist dabei ungeklärt bzw. gibt es verschiedene Meinungen dazu.

In der Lehre wird davon ausgegangen, dass sich die Schutzbereiche von 10 Ziff. 2 BV, 13 Ziff. 1 und 13 Ziff. 2 BV überschneiden. Werden Daten bearbeitet, würde auch regelmässig eine Beeinträchtigung der persönlichen Freiheit nach BV 10 Ziff. 2 vorliegen.

z.B. D N A – Entnahme: Erstellung eines D N A-Profils und dessen Bearbeitung fällt unter den Schutzbereich von 13 Ziff. 2 BV, jedoch liegt mit der Entnahme bei der betroffenen Person ein Eingriff in die körperliche Integrität nach 10 Ziff. 2 BV vor.

35 Ziff. 3 BG: Indirekte Drittwirkung der Grundrechte gilt zwischen Privaten. Grundrechte sollen auch zwischen Privaten gelten. Indirekte Drittwirkung gibt es bzw. Aufforderung an den

Gesetzgeber, dass die Grundrechte auch zwischen Privaten gelten soll – deshalb gibt es das Datenschutzgesetz, welches auch die Datenbearbeitung durch Private regelt.

Persönliche Freiheit (10 Ziff. 2 BV)

„Jeder Mensch hat das das Recht auf persönliche Freiheit, insbesondere auf körperliche und geistige Unversehrtheit und auf Bewegungsfreiheit."

Vom Schutzbereich sind alle natürlichen Personen erfasst, nicht aber juristische. Diese können sich jedoch auf einzelne Gehalte von EMRK 8 berufen.

Der sachliche Schutzbereich erfasst die persönlichen Entfaltungsmöglichkeiten des Menschen und die ihm eigene Fähigkeit, eine Situation einzuschätzen und nach dieser Einschätzung zu handeln. Zur Persönlichkeitsentfaltung gehört insbesondere der Aspekt, über die wesentlichen Aspekte des eigenen Lebens selber zu entscheiden. Der Schutzbereich schützt somit jene Bereiche menschlicher Bestätigung vor staatlichen Eingriffen, die für ein selbstbestimmtes Leben in Würde und Freiheit unerlässlich sind.

- Schutz der körperlichen Integrität: Körperliche Unversehrtheit vor dem Staat.

-Schutz der geistigen Integrität: Freie Urteils- und Willensbildung. Das Recht verbietet es dem Staat, das Bewusstsein und die Willensbildung des Einzelnen zu manipulieren. Dazu gehört auch die psychische Integrität; sie ist tangiert, wenn staatliche Massnahmen zur Folge haben, dass ein Mensch eine psychische Krankheit erleidet oder in seinem psychischen Wohlbefinden schwerwiegend beeinträchtigt wird.

- Elementare Erscheinungen der Persönlichkeitsentfaltung: BV 10 Ziff. 2 schützt auch alle Freiheiten, die elementare Erscheinungen der Persönlichkeitsentfaltung des Menschen darstellen; Generalklausel.

BV 13 Allgemein

13 BV läuft parallel zu EMRK 8 bzw. Schutz von natürlichen und juristischen Personen.

Primär ist es ein Abwehrrecht gegen den Staat – es sieht aber auch ein Anspruch auf Schutz vor Eingriffen Dritter vor (BV 35 Ziff. 3 i.V.m. DSG/StGB Bestimmungen)»

Der Schutz der Privatsphäre betrifft in erster Linie den privaten Raum. Gleichzeitig schützt er aber auch private Tätigkeiten, die im öffentlichen Raum erfolgen (Spaziergang oder Einkauf). Auch wer sich in der Öffentlichkeit aufhält, hat ein Recht auf Achtung und Schutz der Privatsphäre.

Recht auf Privatsphäre 13 Ziff. 1 BV

- Privat- und Familienleben (Geheim- und Intimsphäre des Einzelnen sowie den Namen und seine Verwendung) Es fallen alle Lebenssachverhalte darunter, die der Einzelne als Privatsache abgeschirmt haben möchte. Der Schutz soll ermöglichen, dass natürliche Personen ihre Lebensweise frei wählen können, das private Leben nach den eigenen Wünschen zu gestalten,

sowie ohne Beeinträchtigungen durch den Staat Freizeitaktivitäten nachzugehen und Kontakte zu anderen zu pflegen.

- Unverletzlichkeit der Wohnung: Schutz vor physischem Eindringen oder Ausspähen von aussen durch staatliche Organe.

- Kommunikationsgeheimnis: Schutz bei Verwendung von Kommunikationsmitteln – Umfasst die Post, Telefon, Internet, Mailverkehr etc. andere Formen der elektrischen Kommunikation. Der Schutz verbietet es dem Staat, die mit den Mitteln der Kommunikation kommunizierten Inhalte auszuforschen oder abzuhören. Der Schutzbereich ist bereits berührt, wenn der Staat Kenntnis von einer privaten Kommunikation erhält.

Schutz vor Missbrauch persönlicher Daten (13 Ziff. 2 BV)

BV 13 Ziff. 2 ist das zentrale Grundrecht des Datenschutzes.

13 Ziff. 2 BV schützt sowohl natürliche als auch juristische Personen. Auch Personenvereinigungen, die keine juristischen Personen sind, können sich auf das Recht vor Datenmissbrauch berufen. Im Datenschutzgesetz werden ebenso juristische Personen geschützt nach 2 Ziff. 1 i.V.m. 3 lit. b DSG. Nach der Totalrevision werden dann in Zukunft die juristischen Personen nicht mehr vom Datenschutzrecht erfasst sein, werden aber weiterhin durch BV 13 Ziff. 2 etc. geschützt.

Nach dem herrschenden Verständnis ist der Schutzbereich von 13 Ziff. 2 BV bereits beeinträchtigt, wenn Daten einer Person ohne deren Einwilligung bearbeitet werden, nicht erst, wenn die Datenbearbeitung missbräuchlich erfolgt.

Sachlicher Schutzbereich **ist berührt**, sobald a) Personendaten (persönliche Daten) b) bearbeitet werden durch staatliche Organe.

a) Personendaten sind alle Angaben, die einen hinreichenden engen Bezug zu einer bestimmten oder bestimmbaren Person aufweisen (Orientierung an DSG 2 Ziff. 1 und ZGB 27)

b) Bearbeiten umfasst jeden Umgang mit personenbezogenen Angaben – z.B. Erheben, Sammeln, Verarbeiten, Aufbewahren oder Weitergeben. Auch die polizeiliche Videoüberwachung des öffentlichen Raums oder die Bearbeitung von DNA – Profilen fällt darunter (vgl. Bearbeiten nach 3 lit. e DSG)

Der Schutzbereich ist betroffen, wenn eine Person, die staatliche Aufgaben wahrnimmt, Daten erhebt, sammelt, speichert, aufbewahrt, bearbeitet, weiter- oder bekanntgibt.

Im Vergleich zum DSG gibt es bei 13 Ziff. 2 BV keine Unterscheidung zwischen besonders schützenswerten Personendaten sowie Persönlichkeitsprofilen und übrigen Personendaten, aber es gibt im Hinblick zu BV 36 unterschiedliche Anforderungen (je schwerer der Eingriff bzw. wenn besonders schützenswerte Daten betroffen sind) – vergleich Fall Zürich Verein.

Ansprüche aus 13 Ziff. 2 BV

- Anspruch auf Auskunft/Einsicht in die betreffenden Daten – Einschränkung ist nach BV 36 möglich.

- Anspruch auf Berichtigung unrichtiger Daten – ohne Einsicht wäre auch eine allfällige Berichtigung nicht möglich.

- Anspruch auf Vernichtung widerrechtlich gesammelten oder zu lange aufbewahrten Daten. Ein Anspruch auf Vernichtung besteht dann, wenn an der Aufbewahrung kein überwiegend öffentliches Interesse mehr besteht oder die Aufbewahrung als unverhältnismässig erscheint.

- Anspruch auf Aufsicht und wirksame Beschwerde: 15 DSG (ziviler Rechtsschutz) und 25 DSG (Rechtsschutz gegen Bundesorgane)

- Anspruch auf Schutz vor missbräuchlicher Datenbearbeitung durch Private. 13 Ziff. 2 BV verpflichtet auch den Staat, den Einzelnen wirksam vor missbräuchlicher Datenbearbeitung durch Private zu schützen – dies wurde getan mit der Schaffung des DSG, dem ZGB 28 und 328b OR etc.

Einschränkung durch BV 36

- Gesetzliche Grundlage

- Öffentliches Interesse; Schutz von Polizeigütern, Erfüllung von verfassungsrechtlich ausgewiesenen Staatsaufgaben

- Verhältnismässigkeit

- Kerngehalt; Massensammlung

Art. 8 EMRK vs. Bundesgesetze

Weitgehend deckungsgleich mit BV 13 Ziff. 2. Bei einem verfassungswidrigen Bundesgesetz (BV 190) kann man dies rügen beim BGer/BVGer, aber bei einer Verletzung muss das Bundesgesetz trotzdem angewendet werden. Gemäss BV 190 sind Bundesgesetzte und die Staatsverträge (EMRK) massgeblich für das BGer. Bei einem verfassungswidrigen Bundesgesetz kann das BGer nichts tun, wird aber eine Verletzung der EMRK gerügt und stellt das BGer dies fest, kann das BGer trotzdem die Erlasse aufheben – Staatsverträge (wie EMRK) gehen dem Verfassungsrecht der Schweiz vor.

Fall 107 Ia 52

Publikation der Namen der fruchtlos gepfändeten Schuldner im kantonalen Amtsblatt. Betroffener fechtet die Publikation bis vor BGer an.

BGer: Die Veröffentlichung der Namen fruchtlos gepfändeter Schuldner im kantonalen Amtsblatt verstösst **gegen die persönliche Freiheit**.

Die Veröffentlichung der Namen der Verlustscheinschuldner bezweckt die Information künftiger Gläubiger. Diese sollen wissen, wer nicht kreditwürdig ist.

Das Bundesgericht führte damals aus, die Auskündigung wolle den Schuldner in der Würdigung seiner ökonomischen Persönlichkeit durch seine Mitbürger herabsetzen und

bezwecke insofern eine Minderung seines öffentlichen Ansehens. Diese subjektive Zielsetzung ist durch die Entwicklung in der Zwischenzeit wohl in den Hintergrund getreten. Aber selbst wenn objektiv die gesetzliche Ordnung lediglich noch darauf gerichtet ist, die Gläubiger darüber zu informieren, wer nicht kreditwürdig sei, so wirkt die Massnahme auf den Schuldner nach wie vor wie eine öffentliche "Anprangerung". Die Auskündigung hat insofern strafähnlichen Charakter und ist jedenfalls geeignet, das öffentliche Ansehen des Betroffenen herabzumindern. Hinzu kommt, wie der Beschwerdeführer zutreffend geltend macht, dass sich diese Minderung des guten Rufs nicht nur auf die Person des Schuldners auswirkt, sondern auch auf diejenige seiner Angehörigen, namentlich seines Ehegatten und seiner Kinder.

Das Grundrecht darf aber nur eingeschränkt werden, wenn ein überwiegendes öffentliches Interesse den Eingriff rechtfertigt und soweit die Erfüllung der öffentlichen Aufgabe eine solche Einschränkung erfordert. Die angefochtene Massnahme kann deshalb vor der persönlichen Freiheit nur standhalten, wenn höhere Interessen der Öffentlichkeit oder bestimmter Privater den Eingriff gebieterisch erfordern.

Das einzige reale Interesse, das sich zugunsten der Veröffentlichung der Namen der Verlustscheinschuldner anführen lässt, ist der Schutz allfälliger künftiger Kreditoren. Allein diese werden bereits durch das gemäss Art. 8 Abs. 2 SchKG jedem Interessierten gewährleistete Recht auf Einsichtnahme in die Protokolle der Betreibungsämter geschützt.

Die Veröffentlichung des Namens der Verlustscheinschuldner stellt demnach einen **unzulässigen (unverhältnismässigen) Eingriff in die persönliche Freiheit** des Schuldners dar.

1) Interesse auf Information für die Gläubiger über die Schuldner, andererseits das Interesse auf Schutz der persönlichen Freiheit.

2) Abwägung zwischen den beiden Interessen im Rahmen der Verhältnismässigkeitsprüfung (BV 36)

Fall 113 Ia 1

X wurde bei einer polizeilichen Routinekontrolle angehalten worden und wurde auf den Polizeiposten mitgenommen. Nachdem X in Erfahrung gebracht hatte, dass der Vorfall sowie die Tatsache, dass kein Verdacht gegen ihn besteht, vermerkt worden war, verlangte er Akteneinsicht. Dies, um allfällige Fehler korrigieren zu können. Die Akteneinsicht wurde X verwehrt, er habe kein schützwürdiges Interesse.

BGer: Die Interessenabwägung im vorliegenden Fall ergibt, dass ein überwiegendes schutzwürdiges Interesse an der Einsicht in die Eintragungen betreffend die eigene Person in einem Polizeiregister besteht. **Über das allgemeine Interesse an der Kenntnisnahme hinaus sprechen hierfür der enge Bezug zur persönlichen Freiheit** und das Bedürfnis nach einer allfälligen Korrektur; der Akteneinsicht stehen weder der Verwaltungsaufwand noch generelle polizeiliche Geheimhaltungsinteressen entgegen

Anspruch auf Aktieneinsicht ist Teil des rechtlichen Gehörs. Dieser verfassungsmässige Anspruch gilt nicht nur in einem hängigen Verfahren, sondern darüber hinaus auch ausserhalb

eines formellen Verfahrens. Eine umfassende Wahrung der Rechte kann es gebieten, dass der Bürger etwa die Akten eines abgeschlossenen Verfahrens einsehe. Allerdings ist dieser verfassungsrechtliche Anspruch - im Gegensatz zu demjenigen eines Beteiligten auf Einsicht in die Akten eines hängigen Verfahrens - davon abhängig, **dass der Rechtssuchende ein schutzwürdiges Interesse glaubhaft machen** kann.

Der Beschwerdeführer begründet sein Begehren um Einsicht in den streitigen Registereintrag vorerst mit seinem Interesse an der Kenntnis der über ihn festgehaltenen Daten und dem Bedürfnis, prüfen zu können, ob diese korrekt registriert worden seien. Dieses allgemeine Interesse kann heute angesichts der technischen Möglichkeiten der Datenbearbeitung nicht mehr als unerheblich bezeichnet werden. Der einzelne Bürger kann es durchaus als Unbehagen und als Beeinträchtigung seiner Privatsphäre empfinden, wenn die Verwaltung personenbezogene Daten über längere Zeit hinweg aufbewahrt und allenfalls weitere Verwaltungsstellen zu diesen Daten auf unbestimmte Zeit hinaus Zugang haben.

Diese Überlegungen zeigen, dass das Aufbewahren von Daten, wie sie im vorliegenden Fall anlässlich der beim Beschwerdeführer vorgenommenen Personenkontrolle registriert worden sind, **einen engen Bezug insbesondere zum Grundrecht der persönlichen Freiheit** hat. Der Beschwerdeführer hat daher auch unter diesem Gesichtswinkel ein erhebliches Interesse daran, Einsicht in den umstrittenen Registereintrag zu nehmen und dessen Richtigkeit persönlich zu überprüfen. Schliesslich ist zu beachten, dass der Beschwerdeführer Einsicht in den Registereintrag gerade auch deshalb verlangt, um allfällige Unstimmigkeiten korrigieren lassen zu können; er erachtet das Einsichtsrecht als unerlässliche Voraussetzung für eine allfällige Korrektur. Er führt denn auch aus, die Angaben über die Geschehnisse vom 4. Mai 1984, wie sie sich aus dem angefochtenen Entscheid ergeben, stimmten nicht mit der Wirklichkeit überein.

Die Darstellung der Interessenlage zeigt, dass der Beschwerdeführer ein erhebliches schutzwürdiges Interesse an der Einsicht in den streitigen Registereintrag nachweisen kann. **Der Eintrag hat einen engen Bezug zum Grundrecht der persönlichen Freiheit.** Das Interesse an der Einsichtnahme ist um so gewichtiger, als der Beschwerdeführer nicht darüber informiert worden ist, in welche Art von Register der Eintrag erfolgt ist und welche Stellen für wie lange Zeit dazu Zugang haben.

1) Ja; Eintrag hat einen engen Bezug zum Grundrecht der persönlichen Freiheit.

2) Der Zusammenhang zwischen Einsicht und Richtigstellung ergibt sich, dass man ohne Einsicht gar keine Richtigstellung der Daten geltend machen kann. Erst nach einer Einsicht kann man feststellen, ob richtig gehandhabt wurde oder nicht.

Fall 113 Ia 257

P will Einsicht in die sie betreffende Polizeiakte. Rüge der Verletzung der persönlichen Freiheit.

Bei Ein- und Ausreisen habe sie erfahren, dass über sie eine Polizeiakte geführt werde mit falschen Angaben über angebliche Nähe zu terroristischen und anarchistischen Bewegungen.

Grundrecht der persönlichen Freiheit ist betroffen. Genfer Gesetz, das jedermann die Einsicht in ein ihm betreffendes Polizeidossier verwehrt.

Das Recht auf Kenntnisnahme der Daten über die eigene Person, deren Aufbewahrung zu einem Eingriff in die persönliche Freiheit führen kann, erscheint als notwendige Voraussetzung für den Anspruch auf allfällige Berichtigung. Die Einsicht sei notwendig für eine Kontrolle – es braucht hier gar kein schutzwürdiges Interesse.

1) Das schlichte Aufbewahren nicht.

2) Fehler von aufbewahrten Daten kann man nur erkennten, wenn man eine Einsicht hat.

Fall 102 Ia 516

X (Notar und Anwalt) wird beschuldigt, bei der Beurkundung von Grundstückkäufen falsche Kaufpreise angegeben zu haben.

STA ordnet Beschlagnahme aller in der Kanzlei aufbewahrten verfahrensrelevanten Dokumente an.

Argument von X ist ZGB 27/28.

BGer: Die Durchsuchung von Akten beim Träger eines Berufsgeheimnisses, der selbst Beschuldigter in einem Strafverfahren ist, setzt die Abwägung zwischen öffentlichen und privaten Interessen voraus. Zu einer unterschiedslosen Durchsuchung und Beschlagnahme aller in einer Notariatskanzlei verwahrten Dokumente kann die Strafverfolgungsbehörde selbst dann nicht schreiten, wenn dringender Verdacht dafür besteht, dass der Notar eine strafbare Handlung begangen hat.

1) hier ist das Verhältnis nicht zivilrechtlich, sondern öffentlich-rechtlich. Deshalb ist ZGB 27 und 28 nicht betroffen. Grundrechte sind hier betroffen (persönliche Freiheit)

2) Beschlagnahme – Eigentumsgarantie.

3) BV 36 – Abwägung zwischen den Interessen; Strafprozessordnung hat bei der Beschlagnahme Bestimmungen erlassen.

Fall 122 I 360

Zürcher Behörden sammeln Informationen über den Verein für Psychologische Menschenkenntnis und dessen Mitglieder.

Es wurden Namen von Mitgliedern, Unterorganisationen und Adressen auf elektronischen Datenträgern gespeichert.

Zürcher Lehrkräfte verlangten bei den Behörden **vollständige Einsicht** in die über sie erstellten Datenblätter und weitere Unterlagen betreffen ihre Beziehung zum Verein.

Im vorliegenden Fall **sammelten die Zürcher Behörden systematisch Daten über die Mitgliedschaft sowie die Funktion von Personen beim VPM.** Der VPM vertritt eine bestimmte psychologische Schule, und er ist in der Öffentlichkeit vor allem durch seine

Stellungnahmen zu schul- und gesundheitspolitischen Fragen bekannt geworden. Die Mitgliedschaft im VPM bringt somit eine bestimmte weltanschauliche sowie politische Haltung zum Ausdruck. Nach Einschätzung der Zürcher Behörden weist der VPM sektenähnliche Züge und eine totalitäre, vereinnahmende Tendenz auf; VPM-Lehrkräfte verursachten Schulkonflikte aufgrund ihres rechthaberischen, missionarischen Auftretens und unkollegialen Verhaltens, welches sich unter anderem in der Unfähigkeit zeige, andere Meinungen gelten zu lassen und sich Mehrheitsentscheidungen zu fügen; dabei würden sie offensichtlich vom Verein beraten und gesteuert.

BGer: Betroffen ist die **persönliche Freiheit bzw**. die Beschaffung und Aufbewahrung personenbezogener Daten. **Besonders schützenswerte Personendaten dürfen** nur gemäss **einer klaren gesetzlichen Grundlage bearbeitet werden**, es sei denn, die Datenbearbeitung sei für eine in einem formellen Gesetz klar umschriebene Aufgabe unentbehrlich. Im Kanton Zürich fehlt eine gesetzliche Grundlage dafür, die blosse Zugehörigkeit zu einem Verein systematisch ins Personaldossier von Lehrkräften aufzunehmen. **Für die Bearbeitung solcher Daten wäre vielmehr eine klare gesetzliche Grundlage erforderlich gewesen**, **die mit der nötigen Bestimmtheit regelt, unter welchen Voraussetzungen und zu welchem Zweck die Mitgliedschaft von Beamten bzw. Angestellten in politischen bzw. weltanschaulichen Vereinen registriert werden darf, welcher Personenkreis erfasst werden darf, wem derartige Informationen bekanntgegeben werden dürfen und wann bzw. unter welchen Voraussetzungen die Daten wieder gelöscht werden müssen.** Zum Schutz der persönlichen Freiheit der Betroffenen sowie aus Gründen der Rechtssicherheit darf die Erhebung solcher besonders schützenswerter Daten nicht in das Ermessen der Behörden gestellt werden.

Einschränkungen der persönlichen Freiheit sind zulässig, wenn sie auf einer gesetzlichen Grundlage (Normstufe und Normdichte) beruhen, im öffentlichen Interesse liegen, verhältnismässig sind und den Kerngehalt des Grundrechts nicht verletzen.

1) Ja – personenbezogene Daten fallen in den Schutzbereich der persönlichen Freiheit bzw. die Aufbewahrung der Daten.

2) Hier sind besonders schützenswerte Personendaten betroffen (3 lit. c Abs. 1 DSG) Da es um die weltanschaulichen Ansichten geht der Personen. Besonders schützenswerte Daten dürfen nach 17 Ziff. 2 DSG (**hier nicht anwendbar da kantonale Behörden**) nur bearbeitet werden, wenn ein Gesetz im formellen Sinn es ausdrücklich vorsieht …

In diesem Zeitpunkt des Falles war das DSG erst kürzlich in Kraft getreten. Das Bundesgericht nimmt das Bundesgesetz (Datenschutzgesetz), um das Grundrecht der persönlichen Freiheit näher zu konkretisieren. Das BGer hat sich in diesem Fall von 3 lit. c DSG inspirieren lassen («besonders schützenswerte Daten»)

Das Bundesgericht hat sich ebenso von DSG 17 (Rechtsgrundlagen) inspirieren lassen, wann ein «schwerer Eingriff» vorliegt bzw. für die Anforderungen an die gesetzliche Grundlage.

3) Da es hier um einen «schweren Eingriff» handelt bzw. besonders schützenswerte Personendaten betroffen waren, hätte es eine klare gesetzliche Grundlage gebraucht bzw. war die Normdichte nicht genügend.

Fall 124 I 85

Das BS-Polizeigesetz vom 13.11.1996 sah in § 33 vor, dass Uniformierte ein Namensschild tragen. Dem Regierungsrat wurde die Regelung von Ausnahmen von diesem Grundsatz delegiert. Gestützt darauf erliess der RR entsprechende VO-Bestimmungen, die die Namensnennung auf den Nachnamen beschränkten und Einschränkungen bzw. Ausnahmen für den unfriedlichen Ordnungsdienst und Einsätze von Sondereinheiten vorsahen.

BGer: Die im Polizeigesetz festgelegte Verpflichtung der Polizeibeamten, mit der Uniform ein Namensschild zu tragen, berührt die persönliche Freiheit. Sie erweist sich aber als verfassungsmässig.

Daraus geht hervor, dass eine allgemeine Verpflichtung zum Tragen eines Namensschildes und zur jederzeitigen Offenbarung seiner Identität in die persönliche Freiheit eingreift. Der Umstand, dass Polizeibeamte in einem besonderen Rechtsverhältnis zum Staat stehen, schränkt den Schutzbereich der persönlichen Freiheit nicht ein, sondern ist lediglich bei der Frage der Rechtfertigung unter dem Gesichtswinkel der gesetzlichen Grundlage, des öffentlichen Interesses und der Verhältnismässigkeit zu berücksichtigen.

1) Ja, es werden Daten offenbart (gemäss BGer) bzw. ist die persönliche Freiheit betroffen. Der Name und die Verwendung ist im Schutzbereich von BV 10 Ziff. 2 enthalten.

2) Politischer Wille zur Transparenz bzw. öffentliches Interesse.

3) Es musste abgewogen werden – die Polizisten befürchteten, dass dies negative Folgen haben könnte im privaten Bereich. Aber Polizisten müssen sich sowieso ausweisen bei einer Kontrolle etc. Eingriff ist verhältnismässig.

Vgl. Fall SBB-Namensschild für Mitarbeiter. Die Argumente des BGer waren deckungsgleich mit jenen in diesem Fall.

Fall 133 I 77 Videoüberwachung Stadt St. Gallen

Videoüberwachung – das aufgezeichnete Material wird nach 100 Tagen vernichtet – D wollte, dass bereits nach 2 Tagen das Material vernichtet werden muss.

Mit der Videoüberwachung ist das Bearbeiten von Daten betroffen bzw. werden diese festgehalten und aufbewahrt.

BV 13 Ziff. 2 gibt Anspruch auf Vernichtung zulange aufbewahrten Daten. Mit

Für die Datenbearbeitung ist sowohl 10 Ziff. 2 BV und 13 Ziff. 2 BV zu überprüfen. Werden über eine Person Daten gesammelt/bearbeitet, ist nicht nur die persönliche Freiheit betroffen, sondern auch die Privatsphäre.

BGer: Im vorliegenden Fall ist einzig die Verhältnismässigkeit der Dauer der Aufbewahrung von Videoaufzeichnungen gemäss Art. 3 Abs. 3 des Polizeireglements zu prüfen. Diese Aufzeichnungen müssen die Voraussetzungen von Art. 3 Abs. 2 des Polizeireglements erfüllen

und damit insbesondere für die Wahrung der öffentlichen Sicherheit und Ordnung geeignet und erforderlich sein.

Die Personenidentifikationen zulassende Aufzeichnung und Aufbewahrung von Überwachungsmaterial gemäss Art. 3 Abs. 2 des Polizeireglements weisen einen spezifischen Bezug zum Schutz vor Missbrauch persönlicher Daten auf. Der Beschwerdeführer macht denn auch geltend, dass gerade die - als zu lang beanstandete - Aufbewahrungsdauer ihn in seiner Persönlichkeit beeinträchtige. Die Beschwerde ist damit neben **Art. 8 Ziff. 1 EMRK** in erster Linie unter dem Gesichtswinkel des Schutzes vor Missbrauch persönlicher Daten nach **Art. 13 Abs. 2 BV** zu prüfen.

Dauer von 100 Tagen erscheint im Vergleich mit anderen Regelungen als lang. Umgekehrt ist unter dem Gesichtswinkel einer effektiven Strafverfolgung im Dienste der Wahrung der öffentlichen Ordnung und Sicherheit den persönlichen Verhältnissen der von Straftaten betroffenen Personen Rechnung zu tragen. Hierfür fällt ins Gewicht, dass das Anzeigeverhalten der Betroffenen weitgehend von persönlichen Umständen abhängt. Es ist nachvollziehbar, dass zum Beispiel bei Straftaten gegen die sexuelle Integrität oder gegen Jugendliche aus Furcht oder Scham oder mannigfaltigen anderen Gründen mit einer Anzeige oder einem Strafantrag eine gewisse Zeit zugewartet wird.

1) Verhältnis: BGer hat festgehalten, dass mit der Aufzeichnung vor allem die Gefahr des Missbrauchs betroffen wäre – deshalb wurde 13 Ziff. 2 BV überprüft.

2) Überwachung ist verhältnismässig – Abwägung zwischen den einzelnen Interessen. Die Überwachung ist lange, aber wichtig für die Strafverfolgung.

1C 273/2020 Funkwasserzähler in Auenstein

Personendaten: Vorliegend geht es um Daten **betreffend den Wasserverbrauch** sowie deren Bearbeitung. Die neu von der Gemeinde Auenstein eingesetzten elektronischen Wasserzähler messen den Wasserverbrauch und speichern die Stundenwerte auf dem internen Datenlogger während 252 Tagen. **Bei den Daten über den Wasserverbrauch handelt es sich um personenbezogene Daten** der Bewohnerinnen und Bewohner der Häuser, zumindest soweit ein Rückschluss auf diese möglich ist. Dies ist grundsätzlich der Fall bei Einfamilienhäusern oder Mehrfamilienhäusern, in denen je ein Wasserzähler pro Wohnung eingebaut ist. Soweit ersichtlich wohnt der Beschwerdeführer vorliegend in einem Einfamilienhaus; die aufgezeichneten Daten sind somit als Personendaten zu qualifizieren. Davon scheinen auch die Vorinstanzen auszugehen. Die Daten werden gemäss vorinstanzlich festgestelltem Sachverhalt zudem bearbeitet: der Wasserverbrauch wird aufgezeichnet und auf dem Funkwasserzähler werden Stundenwerte gespeichert. Einmal jährlich wird ein einziger Verbrauchswert auf das mobile Endgerät übertragen und anschliessend für die Rechnungsstellung verwendet. All diese Vorgänge stellen eine Datenbearbeitung dar.

Bearbeitung (staatliche): Ausserdem ist festzuhalten, **dass die Wasserzähler** gemäss § 36 des Wasserreglements **im Eigentum der Wasserversorgung der Gemeinde Auenstein stehen** und die durch die Wasserzähler beschafften Daten durch **diese bearbeitet werden**. Da es sich

bei der WV um eine öffentlich-rechtliche Anstalt der Gemeinde handelt, ist die Datenbearbeitung zudem staatlicher Natur.

Eingriff in 13 Ziff. 2 BV: Die Bearbeitung der Daten betreffend Wasserverbrauch - namentlich deren Aufzeichnung, Speicherung, Emission per Funk und Verwendung für die Rechnungsstellung - stellt somit einen Eingriff in das durch Art. 13 Abs. 2 BV geschützte Recht des Beschwerdeführers auf informationelle Selbstbestimmung dar.

Fragen

1) Gerügt wurde 13 Ziff. 2 BV bzw. Verletzung der Privatsphäre – Beschwerdeführer argumentiert, dass zu viele Daten bzw. ein Übermass an Daten gesammelt wurde. Einmal im Jahr wurde es abgezählt, aber das Gerät sendet die Daten im Minutentakt. Eigentlich bräuchte es nur den Jahresstand.

2) Es liegen Angaben vor über den Wasserverbrauch bzw. kann dies einer Person zugeordnet werden.

3) Angaben Wasserverbrauch – Rückschluss auf Personen

4) Ja ist relevant, welche Gesetzesbestimmungen zur Anwendung kommen. Die Wasserzähler stehen im Eigentum der Gemeinde bzw. werden die Daten durch die Gemeinde bearbeitet. Somit liegt eine staatliche Bearbeitung vor und es muss BV 36 geprüft werden.

Das Datenschutzgesetz (DSG des Bundes) kann **hier nicht angewendet werden**, da nicht Bundesorgane hier tätig sind, **sondern kommunale Organe der Gemeinde**. Man kann also nicht rügen, dass das DSG verletzt wurde.

Vor Bundesgericht kann man **nicht eine Verletzung des kantonalen Datenschutzgesetzes rügen**, da man vor BGer gemäss BGG **nur eine Verletzung von Bundesrecht** rügen kann – deshalb müsste man z.B. die Verletzung von BV 13 Ziff. 2 rügen.

Die Grundrechte nach der BV sind auch für die kantonalen Organe massgeblich.

5) Zweck der Erhebung der Daten über den Wasserverbrauch ist, dass man die Gebühr in Rechnung stellen kann. Für die Speicherung der Daten gab es aber keine gesetzliche Grundlage bzw. wurde hiermit Bundesrecht verletzt.

Randdaten nach BÜPF BGE 144 I 126

BÜPF ist Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs. Das BÜPF verpflichtet die **Fernmeldedienstanbieter** (Swisscom, Sunrise, etc.), die für die Teilnehmeridentifikation notwendigen Daten sowie die Verkehrs- und Rechnungsdaten zu speichern **für sechs Monate**. Vorratsdatensammlung für allfällige Strafverfahren)

Fragen

1) Anbieter sind private. Dennoch wurde der verwaltungsrechtliche Weg gewählt – die Privaten übernehmen öffentliche Aufgaben bzw. verpflichtet durch das BÜPF, die Daten zu sammeln. Deshalb handelt es sich um eine öffentlich-rechtliche Streitigkeit.

2) Überprüfung ist in beiden Hinsichten möglich – nur die EMRK kann aber durchgesetzt werden bzw. ein verfassungswidriges Bundesgesetz muss trotzdem angewendet werden. Deshalb immer EMRK rügen!

3) Sammeln der Randdaten der Kunden.

4) Ja

5) 13 Ziff. 1 und 2 BV überlappen sich.

6) Argumentieren: Speichern auf Vorrat – es werden alle Kommunikationsranddaten gespeichert für sechs Monate. Dies ist eine lange Zeit. Es kann herausgefunden werden, mit welchen Nummern und wie lange telefoniert wird. Jedoch argumentierte das BGer, dass bestimmte Schutzvoraussetzungen gelten bzw. für die Strafverfolgung schwere Delikte verfolgt werden müssen und nur dann die Daten bearbeitet werden. Das BVGer argumentierte als Vorinstanz, dass es ein schwerer Eingriff sei.

7) 13 Ziff. 1 und 2 gehen vor (sind spezieller)

8) Gesetzliche Grundlage – Öffentliches Interesse – Verhältnismässigkeit

Zivilrechtlicher Persönlichkeitsschutz

ZGB 27: Interner Schutz (Schutz Träger vor Persönlichkeitsverletzungen, die **im Einverständnis** mit dem Träger erfolgt sind) z.B. Schutz vor übermässigen Bindungen.

ZGB 28: Externer Schutz (Schutz Träger vor Persönlichkeitsverletzungen, die **gegen seinen Willen** erfolgen)

ZGB 28 ist identisch mit 13 DSG (Rechtfertigungsgründe beim Bearbeiten von Personendaten durch private Personen)

> Bearbeitung von Personendaten ist zulässig, solange die Bearbeitung im Einklang mit den Regeln von ZGB 28 ff. und des DSG stehen.

> Es müssen die Sonderbestimmungen in sensiblen Bereichen wie im Arbeitsverhältnis beachtet werden (OR 328)

Prüfschema von ZGB 28

1) *Schutzbereich der Persönlichkeit betroffen?*

= Alles, was zur Individualisierung einer Person dient und im Hinblick auf die Beziehung zu den einzelnen Individuen und im Rahmen der guten Sitten als schutzwürdig erscheint (BGer)

Der Schutzbereich umfasst natürliche und juristische Personen vor persönlichkeitsverletzenden faktischen Beeinträchtigungen durch Dritte

Datenschutz - Relevant:

a) > *Recht am eigenen Bild* (betroffen durch fotografische bzw. filmische Aufnahmen) Person **muss aber erkennbar sein** – Identifizierung **Vgl. mit der Bestimmbarkeit** des DSG (Begriff der Personendaten nach 3 lit. a DSG)

Eingriff in das Recht am eigenen Bild liegt vor bei einer Aufnahme, insbesondere wenn sich das Bild auf den «Privatbereich» einer Person bezieht.

Bei einer Veröffentlichung des Bildes (ohne Einwilligung) ist eine Verletzung immer gegeben – unabhängig davon, ob bereits die Aufnahme unrechtmässig war oder nicht! Das Bild darf nicht ausserhalb des Bereichs verbreitet werden, den der Betroffene ausdrücklich oder durch konkludentes Verhalten bestimmt hat.

b) > *Privatsphäre* (betroffen beim Einblick in das Privatleben durch Dritte) Private Lebensäusserung, die nicht für die Allgemeinheit bestimmt ist.

Eingriff in Privatsphäre liegt vor allem dann vor, wenn Aufnahmen der privaten Lebensäusserung gemacht werden, die nicht für die Allgemeinheit bestimmt ist. Ebenso wenn solche Informationen über das Privatleben verbreitet werden.

> Eine fotografische oder filmische Aufnahme zeigt neben dem Bild als solchem einen Geschehensablauf aus dem Leben des Betroffenen, weshalb bei einer Veröffentlichung regelmässig auch das Recht auf informationelle Privatheit berührt wird.

- Soziale Persönlichkeit

- Affektive Persönlichkeit

- Physische Persönlichkeit

2) *Liegt Verletzung vor? Ist es mehr als nur eine harmlose Beeinträchtigung?*

Gewisse Schwere der Beeinträchtigung ist vorausgesetzt. Nicht jede noch so harmlose Beeinträchtigung darf dazu führen, dass der Verletzer selbst in seiner eigenen Persönlichkeit beeinträchtigt wird.

3) *Liegt ein RF-Grund vor?*

- Gültige Einwilligung: Einwilligung muss freiwillig und aufgeklärt sein. Wenn man z.B. keine Kenntnis von dem Eingriff/Verletzung hat, ist eine Einwilligung nicht möglich. Vgl. 4 Ziff. 5 DSG (Einwilligung ist nur gültig, wenn sie nach angemessener Information erfolgt)

- Überwiegend privates oder öffentliches Interesse (Interessenabwägung) – Je intensiver und personenbezogener der Eingriff ist, desto höher müssen die Interessen sein, um die Verletzung der Persönlichkeit rechtfertigen zu können.

- Rechtfertigung durch Gesetz (Notstand bzw. Notwehr nach OR) es braucht eine spezialgesetzliche Grundlage

4) *Falls kein RF-Grund vorliegt – welche Rechtsbehelfe stehen zur Verfügung? DSG 15 Ziff. 1 verweist auf die Klagen zum Schutz der Persönlichkeit nach 28/28a und 28l des ZGB.*

Fall Drohnenaufnahme

Landwirt macht für eine Pflanzanalyse eine Drohnenaufnahme. Dabei wurde auch die Politikerin X, die mit ihrem Geliebten entlang des Feldes spazieren geht, gefilmt.

1) Schutzbereich: Recht am eigenen Bild (Person muss erkennbar sein). In diesem Fall ist die Politikerin erkennbar auf dem Bild der Drohne.

2) Verletzung? Ja; es werden Aufnahmen gemacht.

3) Rechtfertigungsgrund nach ZGB? Keine gesetzliche Grundlage vorhanden, keine Einwilligung vorhanden (Die Personen wissen nicht einmal, dass sie gefilmt werden), überwiegendes privates oder öffentliches Interesse? Hier liegt wohl kein überwiegendes Interesse vor.

4) Klagemöglichkeiten

Variante: Z, der sich im Pool auf einem nahe gelegenen Privatgrundstück sonnt, wird ebenfalls von den Drohnenaufnahmen miterfasst.

Fall «Privatdetetktivliche Observation BGE 136 III 410»

X. wurde als Mitfahrer in einem Fahrzeug Opfer eines Verkehrsunfalls und erlitt Körperverletzungen. X Erhobt Klage auf Ersatz des Haushaltschadens gegen die beiden Fahrzeuglenker und deren Haftpflichtversicherungen.

Kantonale Gerichte wiesen Klage ab- BGer ebenso.

Haftpflichtversicherung hatte zur Klärung des Haushaltschadens eine Detektei mit der Observation von X während einer bestimmten Dauer beauftragt und die Ergebnisse der Observation ins Recht gelegt.

X erhobt Klage gegen eine Mehrzahl von Personen – unter anderem gegen die Versicherungen und den Inhaber der Detektei sowie gegen Mitarbeitende. Klage auf Feststellung der Verletzung der Persönlichkeit.

Alle Instanzen haben aber die Klage abgewiesen.

BGer: Art. 28 Abs. 2 ZGB; Schutz der Persönlichkeit des Versicherten gegen privatdetektivliche Observation; Rechtfertigungsgrund des überwiegenden Interesses.

Die von der Haftpflichtversicherung veranlasste Observation der versicherten Person kann deren Privatsphäre wie auch deren Recht am eigenen Bild verletzen. Die Verletzung ist dann nicht widerrechtlich, wenn das Interesse an der Verhinderung eines Versicherungsbetrugs das Interesse des von der Observation Betroffenen auf Unversehrtheit seiner Persönlichkeit überwiegt.

Im Falle privatdetektivlicher Observation kann der Anspruch auf **Schutz der Geheim- und der Privatsphäre** betroffen sein (zit. Urteil 5C.187/1997 E. 2a), **aber auch - soweit das Ergebnis der Observation in Film oder Fotografie festgehalten wird - das Recht am eigenen Bild**. Nach der bundesgerichtlichen **Rechtsprechung ist die Verletzung des Rechts am eigenen**

Bild bereits zu bejahen, wenn jemand **ohne Zustimmung um seiner Person willen fotografiert** oder eine bestehende Aufnahme **ohne seine Einwilligung veröffentlicht** wird.

Eine Persönlichkeitsverletzung durch privatdetektivliche Observation der versicherten Person kann im überwiegenden privaten und öffentlichen Interesse liegen, d.h. dadurch gerechtfertigt sein, **dass weder die Versicherung noch die dahinter stehende Versichertengemeinschaft zu Unrecht Leistungen erbringen müssen.** Dieses Interesse an einer wirksamen Missbrauchsbekämpfung und der Aufdeckung bzw. Verhinderung von Versicherungsbetrug (vgl. **BGE 135 I 169** E. 5.5 S. 174) ist gegen das Interesse des von der Observation Betroffenen auf Unversehrtheit seiner Persönlichkeit abzuwägen. **Interessenabwägung** bei der Widerrechtlichkeit.

In tatsächlicher Hinsicht steht für das Bundesgericht verbindlich fest, **dass Alltagsverrichtungen des Beschwerdeführers** wie Einkaufen oder Autowaschen u.Ä. **aufgezeichnet wurden.** Gegenteiliges behauptet auch der Beschwerdeführer nicht. Es kann ergänzend auf die Feststellungen im Haftpflichtprozess verwiesen werden, wonach die Videoaufnahmen und der dazugehörige Überwachungsbericht belegten, wie der Beschwerdeführer ohne grössere Bewegungseinschränkungen Lasten tragen, einkaufen, Staub saugen sowie Auto waschen und polieren konnte.

Sämtliche gefilmten Tätigkeiten des Beschwerdeführers **haben an öffentlich zugänglichen Orten** stattgefunden. Nach der Rechtsprechung dürfen in den Gemein- oder Öffentlichkeitsbereich fallende Tatsachen von jedermann nicht nur ohne weiteres wahrgenommen, sondern grundsätzlich auch weiterverbreitet werden

Soweit sie den Persönlichkeitsschutz nach **Art. 28 ZGB** betreffen, erweisen sich die Begehren der Beschwerdeführerin als unbegründet.

1) Schutzbereich der Persönlichkeit betroffen?

2) Eingriff/Verletzung?

3) Widerrechtlich?

> Die Persönlichkeit darf nicht widerrechtlich verletzt werden beim Bearbeiten von Personendaten (12 Ziff. 1 DSG).

Fragen

1) Schutzbereiche definiert bzw. ob eine Persönlichkeitsverletzung vorliegt. In einem zweiten Schritt wurde geprüft, ob ein RF-Grund vorliegt.

2) Schutz der Privatsphäre und Recht am eigenen Bild

3) Privatsphäre = Lebensäusserung, die nicht für die Allgemeinheit bestimmt ist.

4) Privates Interesse des Beschwerdeführers gegen die Observation vs. Interesse der Versicherung, keine unrechtmässigen Leistungen zu entrichten.

Das BGer hat argumentiert, dass der Beschwerdeführer im öffentlichen Raum aufgenommen wurde bzw. man alles sehen kann bzw. Intensität des Eingriffs vs. Interesse der Versicherung.

Es lag eine Verletzung der Persönlichkeit vor, aber der Eingriff war im Verhältnis nicht schwerwiegend – der Beschwerdeführer wollte nicht mitwirken beim Verfahren etc.

5) Die Ehefrau des Beschwerdeführers wurde auch (unabsichtlich) aufgenommen – das BGer hat argumentiert, dass nur der Beschwerdeführer hätte aufgenommen werden müssen. Ihr Recht sei nicht verletzt – es war kein systematisches Sammeln von Daten der Ehefrau bzw. wurde sie nicht so intensiv aufgenommen wie ihr Ehemann.

Argument BGer: Auf Grund der massgebenden Tatsachenfeststellungen ist davon auszugehen, dass die Beschwerdeführerin nicht gezielt observiert wurde, sondern bloss zufällig und gleichsam nur als "Mitfang" in die Observation des Beschwerdeführers geraten ist (vgl. zum Problem: AEBI-MÜLLER/EICKER/VERDE, a.a.O., S. 29). Da sie nicht um ihrer Person willen fotografiert wurde, durfte eine Verletzung des Rechts der Beschwerdeführerin am eigenen Bild verneint werden.

Fall «Kündigung nach Handy-Kontrolle»

X AG kündigt Mitarbeitenden, nachdem sie von einem WhatsApp-Verkehr zwischen B (M gemeint?) und einer anderen Mitarbeitenden C Kenntnis erhielt.

Die X AG warf B vor, sich im WhatsApp-Verkehr gegenüber dem Geschäftsführer D ehrverletzend geäussert zu haben. [Für die weitere Beurteilung kann davon ausgegangen werden, dass die fraglichen «Verbalinjurien» die fristlose Entlassung rechtfertigen].

Umstritten war, ob die Chat-Protokolle von der X AG rechtswidrig beschafft worden bzw. ob sie prozessual verwertbar waren. Vgl. ZPO 156; Rechtswidrig beschaffte Beweismittel werden nur berücksichtigt, wenn das Interesse an der Wahrheitsfindung überwiegt.

Es handelte sich nicht um das private Smartphone, sondern um ein geschäftliches – Routinekontrolle.

Private Nutzung des Geschäftstelefons ist grundsätzlich nicht erlaubt.

X AG behält sich vor, im Falle des Verdachts einer Verletzung der Vorschriften ohne Vorwarnung eine Kontrolle vorzunehmen sowie die Inhalte zu überprüfen.

328b OR «*Der Arbeitgeber darf Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Im Übrigen gel-ten die Bestimmungen des Bundesgesetzes vom 19. Juni 1992122 über den Datenschutz.*»

Datenbearbeitungen im Arbeitsverhältnis sind grundsätzlich unzulässig, es sei denn, sie seien durch den Bezug zur Eignung des Arbeitnehmers oder zur Durchführung des Arbeitsvertrages gerechtfertigt. Jede Bearbeitung von Daten, die keinen genügenden Arbeitsplatzbezug haben, ist damit unzulässig.

Verhältnis OR 328b: Der Arbeitgeber darf nur für diese Zwecke die Daten über den Arbeitnehmer bearbeiten. Für andere Zwecke darf der Arbeitgeber Personendaten seiner Arbeitnehmer weder erheben noch sonst wie bearbeiten – auch wenn dadurch keine

Persönlichkeitsverletzung begangen wird. **Eine Datenbearbeitung ist selbst damit nicht erlaubt, wenn sie nach dem DSG erlaubt wäre;** Angesichts des zwingenden Charakters von Art. 328b OR vermag der Rechtfertigungsgrund der Einwilligung (Art. 13 Abs. 1 DSG) die Rechtswidrigkeit einer Datenbearbeitung nach Art. 328b OR nicht zu beseitigen. Anders als im Bereich des Datenschutzgesetzes vermag daher das Vorliegen eines Rechtfertigungsgrundes die Rechtswidrigkeit nicht zu beseitigen.

Durch das Chatten über die Person (Opfer) werden Angaben gemacht bzw. eine Äusserung über eine Person ist eine Angabe über eine Person, die bestimmbar ist (3 DSG). Beim Chatverkehr handelt es sich um Personendaten, die vom DSG erfasst sind – durch die Sichtung/Herstellung von Screenshots und Zitierung sind diese Daten von der Beklagten Partei bearbeitet worden im Sinne des DSG.

Es musste nun geprüft werden, ob diese Datenbearbeitung durch den Arbeitgeber B AG zur Durchführung des Arbeitsverhältnisses erforderlich war (328b OR).

> Das Gericht hat festgestellt, dass die Chats einen Grund für eine fristlose Kündigung dargestellt haben.

1) 328 OR ist **lex specialis zum DSG** bzw. dürfen nach OR 328 die Daten des Arbeitnehmers nur dann durch den Arbeitgeber bearbeitet werden, wenn sie für die Durchführung des Arbeitsverhältnisses erforderlich sind.

Hier gibt es eine Normenkollision zwischen DSG und dem OR 328. Die üblichen RF-Gründe nach DSG 13 fallen hier ausser Betracht bzw. regelt 328 OR speziell im Arbeitsverhältnis, was erlaubt ist und was nicht – bzw. ist eine RF durch 13 DSG bei Verletzung von OR 328 nicht möglich.

2) Ja – durch das Chatten werden Angaben gemacht bzw. werden diese Daten durch die X AG bearbeitet durch die Sichtung und Zitierung.

3) das Obergericht argumentiert, dass die inhaltliche Kontrolle das Problem sei. Der Arbeitgeber darf gemäss Gericht nach 328 nur geschäftliche Nachrichten, die das Arbeitsverhältnis betreffen, kontrollieren. Die Nutzung der Randdaten darf man kontrollieren, aber nicht den Inhalt – es handelte sich hier nicht um geschäftliche Kommunikation, sondern um privates.

Es liegt eine Verletzung von OR 328 vor.

4) OR 328 ist zwingendes Recht und kann nicht durch irgendwelche Anstellungsbedingungen abgeändert werden. 328b OR lässt gemäss Gericht gar keine Einwilligung als RF-Grund nach 13 DSG zu.

Das Gericht hat, sofern die Einwilligung gültig wäre, die Einwilligung als RF-Grund verneint, da die Arbeitnehmer gar nicht genau über allfällige Kontrollen informiert wurden bzw. somit nicht genug aufgeklärt worden (4 Ziff. 5 DSG).

5) wegen 328b OR kann auch keine Interessenabwägung vorgenommen werden, da 328b dem 13 DSG vorgeht (auch keine Einwilligung möglich). Das Gericht hat das überwiegende private Interesse sowieso verneint, da die Kontrolle ohne Verdacht durchgeführt wurde.

Fall «Google Streetview» 138 II 346

Betroffen ist der Persönlichkeitsschutz nach ZGB 28 bei der Publikation von Personendaten in Google Street View.

1) Einwand von Google, der EDÖB sei nicht zuständig, da die verwendeten Bilder in den USA veröffentlicht wurden.

Gericht > Das DSG enthält keine Regelung über den Regelungsbereich. Die Aufnahmen wurden in der Schweiz gemacht und sind in der Schweiz abrufbar. Hier liegt mehrheitlich ein Bezug zur Schweiz vor, womit das DSG zur Anwendung kommt. Der EDÖB wurde hier deshalb zu Recht tätig nach 29 DSG. Das Gericht hat argumentiert, dass die Datenbearbeitung überwiegend die Schweiz betrifft, weshalb das DSG anwendbar ist.

2) Hier werden Personen aufgenommen und Objekte, die zu Personen zuzuordnen sind bzw. Personen in Städten/wo sie sich aufhalten. Es liegt ein Personenbezug vor. Umstritten war, ob die Personen bestimmbar sind – das BGer argumentierte, dass gewisse Personen immer noch teilweise erkennbar waren und man im Zeitpunkt der Aufnahme einen Konnex zu einer bestimmten Person machen kann – eine andere Person könnte z.B. die Person auf der Aufnahme wegen dem Umriss gut erkennen.

Schon bei der Aufnahme waren die Personen für Google erkennbar – jeder Anonymisierungsvorgang ist eine Bearbeitung – die Personen von Google, die dann die frischen Aufnahmen bearbeitet haben, konnten die Personen schon vor der Anonymisierung erkennen bzw. waren die Personen schon bestimmbar vor der Veröffentlichung.

3) vgl. Observationsfall (Frau des Observierten war ebenso erkennbar – das BGer hat damals argumentiert, dass Recht auf eigene Bild sei nicht verletzt, weil die Ehefrau nicht Ziel der Observation war).

BGer: Das Recht am eigene Bild könne schon verletzt sein, wenn man eine Aufnahme macht. Aber eine Veröffentlichung ohne Einwilligung **ist immer** eine Verletzung. Im Vergleich zum Observationsfall ging es aber nicht um die Veröffentlichung.

Allgemeine datenschutzrechtliche Grundsätze 4 ff. DSG

„Basis des Datenschutzrechts" – ergänzt durch spezifische Grundsätze für Private (DSG 12 ff.) und Bundesorgane (DSG 16 ff.)

Die Grundsätze müssen bei der Bearbeitung von Personendaten kumulativ eingehalten werden. **Das Nichtbeachten stellt eine Verletzung der Persönlichkeitsrechte** der Betroffenen nach sich **(12 Ziff. 2 lit. a DSG)**

Fraglich ist, ob eine Verletzung der datenschutzrechtlichen Grundsätze per se die Widerrechtlichkeit der Datenbearbeitung nach sich zieht bzw. ob eine Verletzung der Grundsätze gerechtfertigt werden kann.

Die Grundsätze sind direkt anwendbar, jedoch haben die Bundesorgane oder Private noch selber spezifische Grundsätze zu beachten. Es gibt z.B. für Private in 14 DSG die Bestimmung

über die Informationspflicht beim Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen, welche den Transparenzgrundsatz von 4 Ziff. 4 DSG ergänzt.

Wichtig: **Verhältnis** zu den spezialgesetzlichen Regelungen - ein Zurücktreten der allgemeinen Datenschutzgesetzgebung kommt immer dann in Frage, wenn die Spezialgesetzgebung strengere bzw. über die Datenschutzgesetzgebung hinausgehende oder präzisierende Vorgaben enthält. Die allgemeinen datenschutzrechtlichen Bestimmungen sind subsidiär zu spezialgesetzlichen Grundsätzen.

Rechtmässigkeit (4 Ziff. 1 DSG)

Personendaten dürfen nur rechtmässig bearbeitet werden. Eine unrechtmässige Bearbeitung stellt eine widerrechtliche Verletzung der Persönlichkeit dar. Grundsatz der Rechtmässigkeit ist für Private und Bundesorgane unterschiedlich ausgestaltet, da die Voraussetzungen nicht die gleichen sind. Weiter müssen Private wie Bundesorgane die für sie geltenden spezifischen Grundsätze beachten (12 und 16 DSG).

Für Private ist sämtliches Bearbeiten von Personendaten erlaubt, sofern sie nicht gegen geltende Rechtsnormen verstossen. **Datenbearbeitungen dürfen nicht gegen das DSG oder gegen ausserhalb des DSG liegende Vorschriften verstossen.** Darunter können verschiedene Normen fallen wie z.B. 179 ff. StGB oder 328b OR. Werden solche Normen verletzt, liegt schon ein rechtswidriges Verhalten vor bzw. wenn 179 ff. StGB verletzt ist, ist somit 4 Ziff. 1 DSG verletzt.

Bundesorgane brauchen hingegen eine gesetzliche Grundlage für das Bearbeiten von Personendaten nach 17 DSG – dabei müssen noch 18 DSG etc. beachtet werden.

Dozent ist der Meinung, dass eine Verletzung des DSG somit den Grundsatz der Rechtmässigkeit verletzt. Hauptzweck der Norm ist sicherlich, dass Datenbearbeitungen grundsätzlich nicht unter Verstoss gegen ausserhalb des DSG liegende Vorschriften erfolgen dürfen. Gleichwohl steht im Falle eines Verstosses gegen die Vorgaben des Datenschutzgesetzes ausser Zweifel, dass die Datenbearbeitung in der Form rechtswidrig ist und insofern dem Grundsatz der Rechtmässigkeit nicht Genüge getan wurde.

<u>Prüfung</u>

1. Verstoss gegen eine Norm der Schweizer Rechtsordnung?

2. Bezweckt die Norm auch den Schutz der Persönlichkeit?

Werden beide Voraussetzungen bejaht, so liegt eine Verletzung des Grundsatzes der Rechtmässigkeit nach 4 Ziff. 1 DSG vor.

Urteil „Helsana Plus“ (BVGer)

„Datenbearbeitung ist erst unrechtmässig im Sinne des DSG, wenn dabei gegen eine Norm verstossen wird, die zumindest auch, direkt oder indirekt, den Schutz der Persönlichkeit einer Person bezweckt.

Einwilligung (4 Ziff. 5 DSG)

Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig erfolgt. Bei der Bearbeitung von besonders schützenswerten Daten oder Persönlichkeitsprofilen muss die Einwilligung zudem ausdrücklich erfolgen.

Angemessene Information liegt vor, wenn die betroffene Person über Art, Umfang, Zweck sowie über allfällige Risiken informiert wird.

Freiwillig ist die Einwilligung nur dann, wenn sie ohne Druck zustande gekommen ist. Druck liegt vor, wenn der mit der Verweigerung der Einwilligung zu der Datenbearbeitung verbundene Nachteil in keinem Zusammenhang mit der Datenbearbeitung und der mit ihr verfolgten Zielsetzung steht oder unverhältnismässig ist.

Z.B. ist die Zustimmung eines Arbeitnehmers zu einer Datenbearbeitung im Rahmen seines Arbeitnehmers, die nicht im Arbeitsvertrag vorgesehen ist, nicht freiwillig, wenn im Falle der Verweigerung die Entlassung droht, da hier der Nachteil unverhältnismässig wäre + steht der Nachteil (Entlassung) in keinem Zusammenhang zu der Datenbearbeitung.

z.B. Fall Steuerverwaltung Bern: Steuergesetz von Bern sieht vor, dass mit dem Einverständnis der steuerpflichtigen Peron die Eröffnung von Verfügungen und Entscheiden auf dem elektronischen Weg erfolgen kann. Die Aufsichtsstelle des Datenschutzes empfahl der Verwaltung, den Betroffenen zu ermöglichen, wählen zu können, dass nur die Rechnungen und nicht gleichzeitig auch die Verfügungen und Entscheide elektronisch zugestellt zu erhalten. Die Verwaltung folgte dem nicht und bot nur beides alles oder nichts an.

Fragen (Steuerfall)

1) Werden besonders schützenswerte Daten bearbeitet? Achtung! DSG nicht anwendbar, da es um kantonale Behörden geht. Argumentieren, dass hier schützenswerte Daten vorliegen – mit der Steuerveranlagung sieht man viel bzw. Partner, Mitglied Kirche, Spenden, etc.

Das kantonale Datenschutzgesetz sieht ebenso vor wie das nationale, dass es für die Bearbeitung von besonders schützenswerten Daten eine ausdrückliche Einwilligung braucht.

2) Verwaltungsgericht hat festgestellt, dass das kantonale Datenschutzrecht deckungsgleich ist wie beim Bund – hat deshalb die Einwilligung im Hinblick auf das DSG geprüft.

Geprüft wurde, ob hier eine „Freiwilligkeit“ vorliegt bzw. weil die Verwaltung Druck gemacht hat bzw. wenn man nicht einverstanden ist, dass beides zugestellt wird, man gar nichts mehr erhält. Somit liegt hier ein unverhältnismässiger Nachteil vor bzw. ist der Druck da – somit erfolgte die Einwilligung mit „Druck“ und damit nicht freiwillig.

Grundsatz von Treu und Glauben (4 Ziff. 2 DSG)

Bei der Bearbeitung von Personendaten ist dem Grundsatz von Treu und Glauben gerecht zu werden. Der Grundsatz besagt, dass ein loyales und vertrauenswürdiges Verhalten im Rechtsverkehr grundlegend ist bzw. einem widersprüchlichen Verhalten zuwider läuft.

Betrifft auch die Personendatenbearbeitung nach dem Beschaffen.

z.B. Wenn Datenschutzpannen vorliegen – müssen Dienste, welche Personendaten haben, die betroffenen Personen informieren.

Grundsatz der Verhältnismässigkeit (4 Ziff. 2 DSG)

Grundsatz verpflichtet sowohl Bundesorgane, als auch Private.

- Die Datenbearbeitung muss für die Erreichung des verfolgten Zwecks geeignet sein

- Die Datenbearbeitung muss für die Erreichung des verfolgten Zwecks das mildeste Mittel darstellen und damit erforderlich sein

- Die Datenbearbeitung muss für den Betroffenen in Anbetracht des Zwecks zumutbar sein bzw. muss zwischen der Datenbearbeitung und dem damit verbundenen Eingriff ein angemessenes Verhältnis bestehen.

Fall „GPS an Geschäftsfahrzeugen“ 130 II 425

▪ Aussendienst-Mitarbeitende der X AG verkauften und unterhielten Feuerlöschgeräte. Zu diesem Zweck durften sie Geschäftsfahrzeuge verwenden, die sie ständig am Wohnort behielten, aber grds. nicht für private Zwecke nutzen durften. 2002 installierte die X. AG an allen Fahrzeugen, nach Information der Mitarbeitenden, ein GPS-Ortungssystem.

▪ Aufgrund einer Meldung eines Mitarbeitenden verfügte das zuständige kantonale Inspektorat die Entfernung des Ortungssystems.

Fragen

1) 328b/Arbeitsgesetz

2) Unternehmung nimmt etwas vor. Jedoch hat die Behörde das Ortungssystem entfernt. Der materielle Kern war, ob der Arbeitgeber dies durfte bzw. die Arbeitnehmenden überwachen durfte.

3) Die beiden Regeln sind vereinbar miteinander. 328b sieht vor, dass zu Zwecken des Arbeitsverhältnisses Daten bearbeitet werden dürfen.

4) Gericht hat argumentiert, dass das Verhalten der Mitarbeiter nicht überwacht werden darf, aber für Optimierungen dies zulässig sein könnte – Bei gewissen Punkten hat es aber die Verhältnismässigkeit bejaht. Weil es keine permanente Überwachung war der Geschäftsfahrzeuge und sie jeweils nur 4h dauerte, sei die Ortung verhältnismässig gewesen.

Grundsatz der Zweckbindung (4 Ziff. 3 DSG)

Personendaten dürfen nur zu dem Zweck bearbeitet werden,

- der bei der Beschaffung angegeben wurde,

- aus den Umständen ersichtlich oder

- gesetzlich vorgesehen ist.

Der betroffene Person, deren Daten bearbeitet werden, muss deutlich sein, wofür ihre Daten verwendet werden und dass die Daten nicht zweckentfremdet werden.

Der Zweck der Datenbearbeitung muss bereits bei der Datenbeschaffung bekannt sein. Eine Datenbeschaffung ohne Zweckhintergrund verletzt den Grundsatz der Zweckbindung, z.B. ist die Datenbeschaffung auf Vorrat unzulässig, da eine solche meist ohne konkretes Ziel und damit auch ohne Zweckbindung erfolgt > Verbot der Zweckentfremdung.

Grundsatz der Transparenz (4 Ziff. 4 DSG)

Die Beschaffung von Personendaten muss für die betroffene Person erkennbar sein. Der Grundsatz betrifft **nur die Beschaffung von Daten**, nicht die Bearbeitung als solche.

Aus dem Grundsatz der Transparenz ergibt **sich nicht per se eine aktive Informationspflicht** gegenüber der betroffenen Person. Es darf eine gewisse Aufmerksamkeit und ein Interesse am Schicksal der eigenen Daten vorausgesetzt werden.

Weitergehende Informationspflichten betreffend Datenbeschaffung 14 DSG für Private und 18a DSG für Bundesorgane

Ausnahmsweise kann aber das Beschaffen auch ohne das Wissen der betroffenen Person stattfinden, wenn hierfür eine gesetzliche Grundlage vorliegt. Dies ist besonders im Bereich der Polizei und der Strafverfolgung der Fall. Eine nachträgliche Information ist jedoch zwingend, sobald der Zweck der Überwachungsmassnahmen nicht mehr gefährdet wird.

Fall „Informationen über öffentliche Personen“

Eine Vereinigung in der Rechtsform eines Vereins sammelt Informationen über öffentliche Personen wie PolitikerInnen. Etliche dieser Informationen sind im Internet auffindbar und werden von den Betroffenen selbst veröffentlicht. Die betroffenen wissen nicht, dass die Vereinigung Informationen über sie sammelt.

1) Das DSG ist anwendbar bzw. liegt kein Ausschluss vor nach 2 Ziff. 2 DSG. Die Vereinigung ist privat und bearbeitet hier Personendaten der Politiker.

2) Verletzung von 14 Ziff. 1 DSG (Informationspflicht). Verletzung des Transparenzgrundsatzes.

Verhältnis von 14 DSG und 12 Ziff. 3 DSG:

- Es werden ohne Information der Betroffenen besonders schützenswerte Personendaten gesammelt und Persönlichkeitsprofile erstellt. Damit ist zunächst einmal das Transparenzprinzip (DSG 4 IV – spielt keine Rolle, ob besonders schützenswert oder nicht) verletzt. **Eine Persönlichkeitsverletzung** (DSG 12 II a.) liegt, wie Sie richtig erwägen, insofern

dennoch **nicht vor**, wenn die Betroffenen die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt haben (DSG 12 III).

- Weiter ist aber auch **die Informationspflicht (DSG 14) verletzt**, **auf die DSG 12 III keine Auswirkung hat.** Da soweit ersichtlich keine der Ausnahmen gegeben ist (DSG 14 IV: Betroffene bereits informiert, Speicherung vom Gesetz vorgesehen, Information nur mit unverhältnismässigem Aufwand möglich), liegt ein DSG-widriges Bearbeiten vor. Die Verletzung der Informationspflicht ist im Übrigen auf Antrag strafbar (DSG 34 I b Ziff. 1).

Verletzung von: Transparenzprinzip (4 Ziff. 4 DSG) und Informationspflicht (14 DSG)

Keine Verletzung von: Persönlichkeit bzw. nach 12 Ziff. 3 DSG

Grundsatz der Datenrichtigkeit (5 Ziff. 1 DSG)

Wer Personendaten bearbeitet ist verpflichtet, dass die Richtigkeit der bearbeiteten Personendaten verifiziert werden und angemessene Massnahmen zu treffen, um unrichtige oder unvollständige Daten zu berichtigen oder zu löschen. Bearbeitete Personendaten müssen korrekt sein und dürfen nicht verfälscht werden können.

„Richtig" sind Daten, wenn eine Tatsache oder einen Umstand im Hinblick auf den Bearbeitungszweck sachgerecht wiedergegeben werden kann.

a) Vergewisserungspflicht

Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. Die Vergewisserungspflicht enthält kein Verbot, unrichtige Daten zu bearbeiten, sondern nur eine Pflicht, sich über deren Richtigkeit zu vergewissern.

b) Berichtigungs- bzw. – Löschungspflicht

Datenbearbeiter hat Massnahmen zu treffen, damit im Hinblick auf den Bearbeitungszweck unrichtige oder unvollständige Daten berichtigt oder vernichtet werden.

Aus diesem Grundsatz resultiert die Pflicht zur Nachführung von Daten oder zu ihrer periodischen Überprüfung. Unrichtige oder unvollständige Daten müssen berichtigt oder vernichtet werden. Eine Vernichtungspflicht besteht auch dann, wenn die Daten für den Bearbeitungszweck nicht mehr erforderlich sind.

Grundsatz der Datensicherheit (7 DSG) – Andreas Sidler

- *Datenschutz* = Massnahmen zur Verhinderung von einer unerwünschten Bearbeitung von Personendaten

- *Datensicherheit* = Massnahmen zur Sicherstellung der Integrität, Verfügbarkeit und Vertraulichkeit von Daten

Betroffen ist 7 DSG und 8 VDSG

Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.

8 VDSG konkretisiert das Ganze – Wer als Privatperson Personendaten bearbeitet, sorgt für die Vertraulichkeit, Verfügbarkeit und die Integrität der Daten, um einen angemessenen Datenschutz zu gewährleisten. 8 VDSG sieht Schutzziele voraus bzw. dass der Bearbeiter von Personendaten das System gegen verschiedene Risiken (8 Ziff. 1 lit. a-e VDSG) schützen muss.

- Vertraulichkeit: Nur diejenigen Personen dürfen Zugriff auf die vorhandenen Daten haben, die auch über eine entsprechende Berechtigung darüber verfügen

- Verfügbarkeit: Die gewünschte Information hat in der gewünschten Form zum gewünschten Zeitpunkt am gewünschten Ort zur Verfügung zu stehen

- Datenintegrität: Die Daten müssen richtig sein – es darf durch die Bearbeitungsvorgänge keine unzulässige Änderung der Daten vorgenommen werden

7 DSG verpflichtet nicht nur den Dateninhaber, sondern jeden Datenbearbeiter.

Aus 7 DSG leitet sich ab, dass die Datenbearbeiter verpflichtet werden, ein umfassendes Sicherheitskonzept zu erarbeiten, in dessen Rahmen alle Aspekte der Datensicherheit Berücksichtigung finden müssen.

Datenschutzaspekte bei Projekten frühzeitig evaluieren bzw. prüfen

Vorgehen bei Lancierung Projekte und Datenschutz

1) Projekt in der Konzeptphase nach Berührungspunkten mit dem Datenschutz prüfen

2) Zweck und Verhältnismässigkeit der Datenbearbeitung prüfen

3) Datenschutzaspekte adressieren und Umsetzungsverfahren ausarbeiten

4) Risikobeurteilung (Schutzniveau festlegen, Informationsschutz)

5) Risiken bewerten und Massnahmen definieren

z.B. Swiss Covid App. Es gab eine kurze Entwicklungsphase – es fehlten internationale Standarts, zwei Betriebssystemhersteller, fehlende gesetzliche Grundlage beim Start der Konzepte. Es musste dafür gesorgt werden, dass mit der APP nicht zu fest in die Persönlichkeitsrechte eingegriffen wird.

Der EDÖB musste bei der App die Ansätze prüfen. Es wurde zudem eine genügende Rechtsgrundlage nach 17 DSG verlangt – da dadurch Personendaten bearbeitet werden.

> Einbezug der datenschutzrechtlichen Aspekte beim Start des Projektes war essentiell für den Projektverlauf

Fall „Google Streetview“ 2. Teil

1) BGer ist der Ansicht, dass es nicht für alle Personen erkennbar ist, warum die Daten beschafft werden – Grundsatz der Zweckbindung sowie Transparenzgrundsatz verletzt.

2) Verhältnismässigkeit (4 Ziff. 2 DSG) – Verhältnismässigkeit und öffentliche/private Interessen sind eng miteinander verbunden.

Ist ein Grundsatz verletzt, gilt die Fiktion einer Persönlichkeitsverletzung! 12 Ziff. 2 lit. a DSG (dann liegt eine Verletzung vor, wenn entgegen der Grundsätze Daten bearbeitet werden). Möglichkeit zur Rechtfertigung? Das BGer verknüpft die Rechtfertigung durch öffentliche/private Interessen mit dem Grundsatz der Verhältnismässigkeit.

Das BGer hat die Interessen der Privatpersonen und von Google Street View abgewogen. Es hat erklärt, dass die Interessen der Privatpersonen überwiegen. Es gäbe bessere Möglichkeiten, die Aufnahmen zu machen mit sicheren Massnahmen bzw. damit die Anonymisierung besser gewährleistet werden kann (Grundsatz der Verhältnismässigkeit)

3) Ja: 15 Ziff. 1 DSG i.V.m. 28a ZGB (Klagen aus Persönlichkeitsverletzung)

BGE „Dashcam“- Rechtmässigkeit (4 Ziff. 1 DSG)

Die Beschwerdeführerin rügt, die ihr vorgeworfenen Verkehrsregelverletzungen seien von einem anderen Verkehrsteilnehmer mit einer Dashcam aufgezeichnet worden. Diese Videoaufnahmen seien rechtswidrig erstellt worden und damit im Strafverfahren unverwertbar.

Die Vorinstanz erwägt, **dass die Aufzeichnungen der Dashcam in Verletzung der Bestimmungen des Datenschutzgesetzes erfolgt und damit rechtswidrig erstellt** worden seien. Von Privaten rechtswidrig erlangte Beweise seien nach der bundesgerichtlichen Rechtsprechung verwertbar, wenn sie auch von den Strafverfolgungsbehörden rechtmässig hätten erlangt werden können und kumulativ dazu eine Interessenabwägung für deren Verwertung spreche. Diese Voraussetzungen seien vorliegend erfüllt.

Das Erstellen von Aufnahmen im öffentlichen Raum, auf welchen Personen oder Autokennzeichen **erkennbar** sind, stellt **ein Bearbeiten von Personendaten** im Sinne von Art. 3 lit. a und lit. e des Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1) dar.

Art. **4 Abs. 4 DSG** bestimmt, dass die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung **für die betroffene Person erkennbar** sein muss. Die Missachtung dieses Grundsatzes **stellt eine Persönlichkeitsverletzung dar (Art. 12 Abs. 2 lit. a DSG).** Die Erstellung von Videoaufnahmen aus einem Fahrzeug heraus ist für andere Verkehrsteilnehmer **nicht ohne Weiteres erkennbar**. Die Datenbearbeitung ist damit als heimlich im Sinne von Art. 4 Abs. 4 DSG zu qualifizieren.

Eine Persönlichkeitsverletzung im Sinne von Art. 12 DSG ist gemäss Art. 13 Abs. 1 DSG widerrechtlich, wenn **kein Rechtfertigungsgrund** - namentlich ein überwiegendes

öffentliches oder privates Interesse - vorliegt. **In der Doktrin wird teilweise** die Auffassung vertreten, dass solche materiellrechtlichen Rechtfertigungsgründe die Rechtswidrigkeit einer (privaten) Beweiserhebung im verfahrensrechtlichen Kontext nicht zu heilen vermögen.

Die Videoaufzeichnung erfolgte in Missachtung von Art. 4 Abs. 4 DSG und ist damit rechtswidrig.

1) Ja – das Aufnehmen von Personen stellt eine Bearbeitung von Personendaten dar. Angabe, Personenbezug, Bestimmbarkeit.

2) Grundsatz der Transparenz – es wurde heimlich aufgenommen bzw. wusste es die betroffene Person nicht.

3) Ja: Vermutung von 12 Ziff. 2 lit. a DSG –Fiktion – es braucht nun ein Rechtfertigungsgrund.

4) Nur, wenn auch die Behörden diese Aufnahme machen durften und das Interesse der Strafverfolgung überwiegt. Das BGer hat festgestellt, dass für die Aufklärung schwerer Straftaten rechtswidrig erlangte Beweise verwendet werden dürfen. In diesem Fall liegt aber keine schwere Straftat vor. **Die Rechtfertigung nach DSG spielt hier im Strafprozess keine Rolle!**

Der Bearbeiter muss nun wegen der Fiktion beweisen, dass ein RF-Grund vorliegt! Aber in Bezug zur St PO ist dies irrelevant.

Besondere Grundsätze

Kommen nicht allgemein bei jeder Datenbearbeitung zum Zug, sondern nur für bestimmte Arten von Datenbearbeitungen. Beide Grundsätze gelten sowohl für Private als auch für Bundesorgane.

Grenzüberschreitende Datenbekanntgabe (6 DSG)

Idee: Es soll sichergestellt werden, dass die Weitergabe von personenbezogenen Daten an einen Datenempfänger in einem Drittland nur unter der Bedingung erfolgen kann, wenn im Empfängerland ein angemessenes Datenschutzniveau vorliegt.

6 DSG gilt für eine bestimmte Art der Datenbearbeitung; die grenzüberschreitende Bekanntgabe von Personendaten. 6 DSG ist **kumulativ** zu den allgemeinen Grundsätzen anzuwenden (beides muss geprüft werden)

Der grenzüberschreitende Datenverkehr liegt dann vor, wenn Personendaten vom territorialen Anwendungsbereich eines Datenschutzgesetzes in denjenigen eines anderen übergehen und dort bearbeitet werden bzw. werden die Personendaten der schweizerischen Rechtsordnung entzogen.

- liegt vor wenn eine schweizerische Konzerngesellschaft Kundendaten an eine Schwestergesellschaft im Ausland zur zentralen Auswertung überträgt. Die Daten werden in den Anwendungsbereich eines Datenschutzgesetzes des Auslandes übertragen und die Daten werden dort bearbeitet durch die Auswertung der Schwestergesellschaft.

- Verein publiziert Mitgliederdaten auf seiner öffentlich zugänglichen Website im Internet. Siehe Art. 5 VDSG – solche Publikationen gelten nicht als Übermittlung in das Ausland. Sonst würde man ja bei jeder Publikation von einem grenzüberschreitenden Datenverkehr sprechen.

a) Sofern die ausländische Gesetzgebung keinen angemessenen Schutz für die Personendaten gewährleisten kann, ist von einer grenzüberschreitenden Bekanntgabe abzusehen bzw. weil dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde.

Ein angemessener Schutz liegt dann vor, wenn das ausländische Datenschutzgesetz in sachlicher, persönlicher und räumlicher Hinsicht mit dem Schweizerischen vergleichbar ist und der Datenschutz im Drittland auch praktisch effektiv gewährt wird. Verlangt wird auch oft, dass die Gesetzgebung im Empfängerstaat den Anforderungen der Datenschutzkonvention des Europarates entspricht.

Der EDÖB veröffentlicht nach 7 VDSG eine Liste der Staaten, deren Gesetzgebung einen angemessenen Schutz gewährleistet.

b) 6 Ziff. 2 DSG sieht aber eine Ausnahme vor bzw. dass auch dann eine Datenbekanntgabe erlaubt ist, wenn im Ausland eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet. Die Auflistung in 6 Ziff. 2 DSG ist abschliessend.

- hinreichende Garantien (lit.a): Der Schutz kann durch hinreichende Garantien insbesondere durch Vertrag gewährleistet werden bzw. einen angemessenen Schutz im Ausland. Z.B. Datenschutzvertrag oder Vertragsklausel. Der Inhalt der Garantie bestimmt sich nach den Kriterien des DSG. Unter anderem muss der Datenübermittler, der Datenempfänger, die Zwecke der Übermittlung, die Kategorien der betroffenen Daten und Personen und die Aufbewahrungsdauer bekannt sein. Ebenso die Rechte der betroffenen Person.

- Einwilligung im Einzelfall (lit. b): Die Einwilligung muss sich im Einzelfall auf einen bestimmten Zweck oder auf eine bestimmte Situation beziehen bzw. auf einen konkreten Einzelfall. Eine Einwilligung ist erst gültig, wenn sie nach angemessener Information freiwillig erfolgt.

- Zusammenhangmit einem Vertrag (lit. c): Wenn die Bekanntgabe von Personendaten ins Ausland für den Abschluss oder den Vollzug eines Vertrages unabdingbar ist. Die betroffenen Personen sind auf die Übermittlung ihrer Personendaten aufmerksam zu machen.

- Wahrung eines überwiegenden öffentlichen Interesses oder im Zusammenhangmit Rechtsansprüchen vor Gericht (lit. d): Bekanntgabe muss unerlässlich für die Wahrung des überwiegenden öffentlichen Interesses sein – in Frage kommt auch ein öffentliches Interesse eines anderen Staates. Ebenso können Personen ins Ausland übermittelt werden, wenn die Daten für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht (verschiedene Arten von Gerichten) unerlässlich sind.

- Schutz des Lebens oder der körperlichen Integrität des Betroffenen (lit. e): Datenübermittlung ins Ausland, wenn die Bekanntgabe zum Schutz des Lebens oder der körperlichen Integrität der betroffenen Person dient. Z.B. bei Personenunfall –wichtig ist dabei die hypothetische Einwilligung der betroffenen Person.

- Allgemeine Zugänglichmachung der Daten (lit. f): Bekanntgabe ist zulässig, wenn die betroffene Person die Daten allgemein zugänglich gemacht hat und eine Bearbeitung nicht ausdrücklich untersagt hat – vgl. 12 Ziff. 3 DSG. Jedoch muss dies im Einzelfall geprüft werden, ob Personendaten als allgemein zugänglich gelten, wenn sie im Internet veröffentlicht wurden – es muss der Zweck der Veröffentlichung angegeben werden.

- Übermittlung innerhalb von Unternehmen oder Konzernen (lit. g): Bekanntgabe von Personendaten innerhalb von Unternehmen oder Konzernen zulässig, wenn die Beteiligten Datenschutzregeln unterstehen, die im Empfängerland einen angemessenen Schutz gewährleisten.

Information des EDÖB (6 Ziff. 3 DSG)

Es handelt sich hier um eine Meldepflicht – nicht Genehmigungspflicht. Die Bestimmung bezweckt die Kontrolle von Schutzmassnahmen im Rahmen von grenzüberschreitenden Bekanntgaben und hat zum Ziel, einen einheitlichen und angemessenen Datenschutz sicherzustellen. Die Information des EDÖB hat in der Regel vor der Bekanntgabe ins Ausland zu erfolgen.

Die Bestimmung findet Anwendung bei 6 Ziff. 2 lit. a (Garantien oder Vertrag) und g (Unternehmen/Konzern) DSG.

Adressat der Bestimmung ist der private Inhaber von Datensammlungen und Bundesorgane.

Datenbearbeitung durch Dritte (10a ff. DSG)

Geregelt wird hier die Datenbearbeitung durch Dritte. **Auch die Datenbearbeitung durch Dritte im Ausland untersteht 10a DSG, jedoch ist gleichzeitig 6 DSG kumulativ anwendbar.**

Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz Dritten übertragen werden, a) wenn die Daten nur so bearbeitet werden, wie es der Auftraggeber selbst es tun dürfte und b) keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet (beachten, ob es spezialgesetzliche Normen gibt oder vertragliche Klauseln – dass man nicht ein „Out-Sorcing“ machen darf).

Fallbeispiel: Psychiater behandelt Patienten. Aber er hat den Bericht nicht selber geschrieben, sondern diktiert. Er hat dann das Material an ein externes Büro gesendet – das Büro hat dann den Bericht ausgefertigt. Man warf dem Psychologen vor, dass er nicht die Einwilligung des Betroffenen geholt hat. Jedoch sah es das Bezirksgericht nicht als Verletzung von 321 StGB. Der EDÖB hat aber darauf hingewiesen, dass es grundsätzlich nicht verboten ist, das Material zur Ausfertigung an ein anderes Büro zu senden. Die Psychologen müssen aber gewährleisten dass die Dritte die Personenarbeiten nur so bearbeiten, wie es sie selber dürften. Würden die Daten in falsche Hände gelangen, würden beide (Auftraggeber und Dritter/Bearbeiter) haften. Der Datenschutz darf nicht durch die Überragung relativiert werden.

10a DSG kommt zur Anwendung, wenn der Inhaber einer Datensammlung (Auftraggeber) eine andere natürliche oder juristische Person (Dritter) **damit beauftragt**, Personendaten zu

bearbeiten. Der Betroffene ist die Person, dessen Daten von dieser Bearbeitung betroffen sind. Als Dritter wird eine „andere Einheit“ verstanden, welche in gewissen Bereichen unabhängig vom Inhaber der Datensammlung agiert – ist anhand der Umstände im Einzelfall zu überprüfen.

Der Auftraggeber hat sich zu vergewissern, dass der Dritte die Datensicherheit gewährleistet (10a Ziff. 2 DSG). Der Auftraggeber bleibt verantwortlich für die Übertragung. Der Auftraggeber muss den Dritten sowie die Daten sorgfältig auswählen, instruieren und kontrollieren. Er kann sich nicht durch die Übertragung der Bearbeitung befreien. Der Auftraggeber kann sich aber im Voraus darüber informieren.

10a DSG kommt zur Anwendung, wenn eine „Übertragung“ an einen Dritten vorliegt. **Der Auftraggeber ist/wird/bleibt Inhaber der Datensammlung** und der Dritte bearbeitet die Daten **nur für die Zwecke des Auftraggebers**. Der Dritte handelt somit gemäss den Instruktionen des Auftraggebers – Abgrenzung zur Funktionsübertragung bzw. bei der Funktionsübertragung bearbeitet der Dritte die Daten autonom (10a DSG wäre dann nicht mehr anwendbar). Es genügt bereits eine kleine Datenbearbeitung, welche als „Übertragung“ gilt.

„Bearbeitung in gleicher Weise“ (10a Ziff. 1 lit. a DSG)

Die Daten müssen aber gleich wie durch den Auftraggeber selbst bearbeitet werden (Sorgfaltspflicht des Auftraggebers) Der Auftraggeber hat persönlich dafür zu sorgen, dass der Dritte die Daten in gleicher Weise bearbeitet, wie er selbst es auch tun würde bzw. müsste.

Die Befugnisse können sich aus dem Gesetz ergeben, oder aus einer schriftlichen Vereinbarung.

Der Auftraggeber muss analog der Geschäftsherrenhaftung OR 55 alle gebotene Sorgfalt aufwenden, um Verstösse des Dritten gegen das Datenschutzgesetz zu verhindern. Der Auftraggeber ist verpflichtet, den Dritten im konkreten Einzelfall sorgfältig auszuwählen und zu instruieren. Aber auch nachher wird der Auftraggeber nicht von seiner Sorgfaltspflicht befreit.

Wichtig: Neben den Grundsätzen von 10a müssen auch die allgemeinen Grundsätze bei der Datenbearbeitung beachtet werden. Der Dritte darf die Daten nur so bearbeiten, wie es auch der Arbeitgeber tun dürfte – darunter fallen auch die allgemeinen Grundsätze, weil auch die bei einer Datenbearbeitung beachtet werden müssen.

„Gesetzliche oder vertragliche Geheimhaltungspflicht“ (10a Ziff. 1 lit. b DSG)

Datenbearbeitung durch Dritte ist unzulässig, wenn ihr gesetzliche oder vertragliche Geheimhaltungspflichten entgegenstehen.

- Gesetzliche Geheimhaltungsvorschriften: Geheimhaltungspflicht kann sich aus dem Spezialgesetz ergeben. Wird die Pflicht verletzt, sieht die Norm unter anderem strafrechtliche oder haftpflichtrechtliche Konsequenzen vor.

- Vertragliche Geheimhaltungspflichten: Vertragsklauseln, die eine Datenbearbeitung durch Dritte teilweise oder ganz ausschliessen. Wird eine solche Pflicht verletzt, können allfällige Ansprüche aus vertraglicher und deliktischer Sicht ergeben.

- Bei zulässiger Überragung gilt das „Bekanntgabeprivileg“. Sind die Voraussetzungen für eine Datenbearbeitung durch Dritte nach 10a Ziff. 1 lit. a und b DSG erfüllt, so liegt ein Bekanntgabeprivileg vor. Der Auftraggeber darf besonders schützenswerte Personendaten oder Persönlichkeitsprofile dem Dritten weitergeben, ohne dass es sich dabei um eine Persönlichkeitsverletzung handelt nach 12 Ziff. 2 lit. c DSG.

- Bei Persönlichkeitsverletzung gilt das „Rechtfertigungsprivileg“ des Dritten. Der Dritte kann auch die Rechtfertigungsgründe des Dritten geltend machen (10a Ziff. 3 DSG).

Fehlt es an den Voraussetzungen von 10a Ziff. 1 lit. a und b DSG, stellt die Übermittlung der Daten zur Bearbeitung durch einen Dritten eine Persönlichkeitsverletzung dar und ist somit widerrechtlich! Die betroffene Person kann in diesem Fall ihre Ansprüche aufgrund von 15 DSG gegenüber dem Auftraggeber oder dem Dritten geltend machen. Der Auftraggeber sowie der Dritte können sich aber auf einen Rechtfertigungsgrund nach 13 DSG stützen (10a Ziff. 3 DSG).

- Bei grenzüberschreitender Datenbekanntgabe gilt zusätzlich DSG 6!

„Cloud-Dienstleistung“

Schweizer Unternehmen will Cloud-Dienstleistungen eines US-amerikanischen Unternehmens übernehmen.

Es braucht:

- Datenbearbeitungsvertrag (10a Ziff. 1 DSG)

- Datenschutzgarantien im Sinne von 6 Ziff. 2 lit. a DSG

Variante: Transfer erfolgt im Rahmen von „Privacy-Shield“. Privacy Shield ist (wie bereits abgeklärt) nicht genügend, um einen angemessenen Schutz zu gewährleisten.

Fall „Tessi“

Sowohl 6 DSG als auch 10a DSG anwendbar.

- Gestützt worauf das das BFS Personendaten bearbeiten? 22 DSG (Bearbeiten für Forschung, Planung und Statistik)

- es liegt eine Übertragung von Personendaten ins Ausland vor – die Daten werden im Ausland bearbeitet. Gemäss Bericht des EDÖB war es kein angemessener Schutz nach 6 Ziff. 1 DSG – deshalb musste 6 Ziff. 2 DSG herangezogen werden.

- die Datenbearbeitung wurde durch Dritte vorgenommen (10a DSG)

„Privacy Shield CH-USA“

Zweck ist ein angemessenes Datenschutzniveau in den USA zu gewährleisten. US-Amerikanische Unternehmen, die am Shield partizipieren wollen, müssen sich in den USA zertifizieren und kommen auf eine öffentlich zugängliche Liste. Betroffene haben ein Auskunfts- und Berichtigungsrecht und können Beschwerden erheben.

Seit Inkrafttreten haben sich über 3‘000 Unternehmen angeschlossen.

Nach vertiefter Analyse kommt der EDÖB in seiner Stellungnahme vom 8.9.2020 zum Schluss, dass das Privacy Shield Regime trotz der Gewährung von besonderen Schutzrechten für Betroffene in der Schweiz kein adäquates Schutzniveau für Datenbekanntgaben von der Schweiz an die USA gemäss Bundesgesetz über den Datenschutz (DSG) bietet. Aufgrund dieser auf das schweizerische Recht gestützten Einschätzung hat der EDÖB in der Staatenliste des EDÖB den Verweis auf einen «angemessenen Datenschutz unter bestimmten Bedingungen» für die USA gestrichen.

Der Privacy Shield reicht gemäss EDÖB nicht aus, um 6 DSG gerecht zu werden.

Fall „Gerichtshof der EU“ – Privacy Shield

> Privacy Shield CH-USA bietet nach Auffassung des EDÖB kein adäquates Datenschutzniveau.

Die Datenschutz-Grundverordnung (DSGVO) bestimmt, dass personenbezogene Daten grundsätzlich nur dann in ein Drittland übermittelt werden dürfen, wenn das betreffende Land für die Daten ein angemessenes Schutzniveau gewährleistet. Nach dieser Verordnung kann die Kommission feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder seiner internationalen Verpflichtungen ein angemessenes Schutzniveau gewährleistet2 . Liegt kein derartiger Angemessenheitsbeschluss vor, darf eine solche Übermittlung nur erfolgen, wenn der in der Union ansässige Exporteur der personenbezogenen Daten geeignete Garantien vorsieht, **die sich u. a. aus von der Kommission erarbeiteten Standarddatenschutzklauseln ergeben können**, und wenn die betroffenen Personen über durchsetzbare Rechte und wirksame Rechtsbehelfe verfügen

Herr Schrems, ein in Österreich wohnhafter österreichischer Staatsangehöriger, ist seit 2008 Nutzer von Facebook. Wie bei allen anderen im Unionsgebiet wohnhaften Nutzern werden seine personenbezogenen Daten ganz oder teilweise von Facebook Ireland an Server der Facebook Inc., die sich in den Vereinigten Staaten befinden, übermittelt und dort verarbeitet. Herr Schrems legte bei der irischen Aufsichtsbehörde eine Beschwerde ein, die im Wesentlichen darauf abzielte, diese Übermittlungen verbieten zu lassen. Er machte geltend, das Recht und die Praxis der Vereinigten Staaten böten keinen ausreichenden Schutz vor dem Zugriff der Behörden auf die dorthin übermittelten Daten.

In Bezug auf das im Rahmen einer solchen Übermittlung erforderliche Schutzniveau entscheidet der Gerichtshof, dass die insoweit in der DSGVO vorgesehenen Anforderungen, die sich auf geeignete Garantien, durchsetzbare Rechte und wirksame Rechtsbehelfe beziehen, dahin auszulegen sind, **dass die Personen**, deren personenbezogene Daten auf der Grundlage **von Standarddatenschutzklauseln** in **ein Drittland übermittelt** werden, **ein Schutzniveau**

genießen müssen, das dem in der Union durch die DSGVO im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist.

In Bezug auf das Erfordernis des gerichtlichen Rechtsschutzes befindet der Gerichtshof, dass **der im Privacy-Shield-Beschluss** 2016/1250 angeführte Ombudsmechanismus entgegen den darin von der Kommission getroffenen Feststellungen den betroffenen Personen **keinen Rechtsweg zu einem Organ eröffnet, das Garantien böte, die den nach dem Unionsrecht erforderlichen Garantien der Sache nach gleichwertig wären,** d. h. Garantien, die sowohl die Unabhängigkeit der durch diesen Mechanismus vorgesehenen Ombudsperson als auch das Bestehen von Normen gewährleisten, die die Ombudsperson dazu ermächtigen, gegenüber den amerikanischen Nachrichtendiensten verbindliche Entscheidungen zu erlassen. Aus all diesen Gründen erklärt der Gerichtshof den Beschluss 2016/1250 für ungültig.

Datenbearbeitung durch Private

ZGB: 28 ZGB

DSG: Private 12 ff. DSG, Bundesorgane (16 ff. DSG) und EDÖB (26 ff. DSG)

Grundzüge von 12 DSG

- Verletzung der Persönlichkeit als absolutes Rechtsgut ist grundsätzlich unzulässig

- Eine Bearbeitung von Personendaten **stellt nicht per se eine Persönlichkeitsverletzung** dar! Es braucht eine gewisse Intensität. Ob eine Verletzung vorliegt, beurteilt sich nach einem objektiven Massstab. Bundesgerichts-Entscheid – Weltwoche-Artikel – das BGer hat die Verletzung anhand von einem Massstab (ausgehend vom Durchschnittleser) überprüft.

- In den Fällen von DSG 12 Ziff. 2 liegt eine Fiktion der Persönlichkeitsverletzung vor. Wenn die Tatbestände erfüllt sind, dann liegt immer eine Persönlichkeitsverletzung vor.

Lit. a: Personendaten werden entgegen den Grundsätzen von 4, 5 Ziff. 1 und 7 Ziff. 1 DSG bearbeitet.

Trotz des Wortlauts („ohne RF-Grund“ steht nicht) ist eine Rechtfertigung möglich – eine Rechtfertigung ist aber nicht leichthin anzunehmen. Vgl. Fall „Logistep“

Lit. b: **Ohne RF-Grund** werden Daten einer Person gegen deren ausdrücklichen Willen bearbeitet.

Lit. c: **Ohne RF-Grund** werden **besonders schützenswerte Personendaten** oder **Persönlichkeitsprofile an Dritte bekanntgegeben**.

- Nicht jede Verletzung der Persönlichkeit ist widerrechtlich, sie kann nach 13 Ziff.1 DSG durch Einwilligung, überwiegendes Interesse oder Gesetz gerechtfertigt werden.

- Eine widerrechtliche Persönlichkeitsverletzung verlangt kein Verschulden oder Bösgläubigkeit.

Grundzüge von DSG 13

DSG 13 Ziff. 1 entspricht ZGB 28 Ziff. 2.

- *Einwilligung* erfordert eine gültige, vorgängige, nicht widerrufene Einwilligung (vgl. 4 DSG)

- *Überwiegendes privates Interesse*: In Praxis wichtig aber unsicher, da wertende Abwägung der Interessen im Einzelfall nötig sind. Wobei sowohl die Interessen des Datenbearbeiters als auch jene der betroffenen Person sowie weiterer Betroffener berücksichtigt werden können.

13 Ziff. 2 DSG zählt die Varianten auf, bei denen ein überwiegendes Interesse der bearbeitenden Person in Betracht fällt. Aber es muss trotzdem eine Abwägung im Einzelfall durchgenommen werden.

Methodisches Vorgehen (Überwiegende private Interessen)

1. Private Interessen an Datenbearbeitung zum verfolgen Zweck mit den eingesetzten Mitteln?

2. Sind tatsächliche Interessen berechtigte Interessen?

3. Berechtigte Interessen der betroffenen Person?

4. Berechtige Interessen an Datenbearbeitung und jene der betroffenen Person gegeneinander abwägen.

Fall: Stimmerkennung Postfinance

a) Opt-In oder Opt-Out? Opt-Out liegt vor, da man ausdrücklich widersprechen muss, damit die Stimme nicht aufgenommen und ein Stimmabdruck gemacht wird. Bei Opt-In gilt das Prinzip, dass wenn man nicht JA sagt, nichts gemacht wird.

b) DSG anwendbar, da es sich um eine Angabe über eine Person handelt, welche bestimmbar ist. Gerade durch die Stimme soll festgestellt werden, wer anruft bzw. um wessen Stimme es handelt. Durch den Stimmabdruck möchte man etwas überprüfen. Fraglich ist, ob es sich um besonders schützenswerte Daten handelt.

Persönlichkeit ist betroffen durch die Stimme. Man greift durch den Abdruck intensiv in die Persönlichkeit ein. Somit liegt eine Verletzung vor. Rechtfertigung muss geprüft werden – überwiegendes privates Interesse könnte in Frage kommen als RF-Grund. Eine Einwilligung würde ausser Betracht fallen, da man nicht über alles informiert wird (vgl.4 Ziff. 5 DSG). Da hier sowieso besonders schützenswerte Daten vorliegen, bräuchte es eine ausdrückliche Einwilligung.

Schema prüfen:

- Welches Interesse? Effizienz, Bewertung

- Berechtigte Interessen der betroffenen Person: Ja – Recht auf Stimme

- Abwägung: Hier überwiegen die Schutzinteressen des betroffenen Person. Keine Rechtfertigung möglich.

- *Überwiegendes öffentliches Interesse:* In der Praxis von untergeordneter Bedeutung.

- ***Gesetz*** gebietet, erlaubt oder setzt Datenbearbeitung voraus. Gestützt auf jede Norm des schweizerischen Privatrechts, auch kantonal oder kommunal. Frage der Rechtfertigung ist durch Auslegung zu beantworten.

Fall „Logistep" 136 II 508 („Datenbearbeitung durch Private")

Empfehlung des EDÖB an die Logistep AG. Es wurden Daten gespeichert und wurden an die Urheberrechtsinhaber weitergegeben. EDÖB ist der Ansicht, dass die Bearbeitungsmethoden der Logistep AG geeignet seien, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen.

Deshalb **Empfehlung des EDÖB** an die AG, die Datenbearbeitung unverzüglich einzustellen, solange keine ausreichende gesetzliche Grundlage für eine zivilrechtliche Nutzung der durch sie erhobenen Daten bestehe. AG lehnt Empfehlung ab – EDÖB kann an BVGer gehen. Bei einem Entscheid des BVGer kann der EDÖB an das BGer gehen.

Der EDÖB wirft dem Bundesverwaltungsgericht vor, Art. 12 Abs. 2 lit. a DSG falsch ausgelegt zu haben. Diese Bestimmung lässt seiner Ansicht nach in ihrer aktuellen Fassung keine Rechtfertigungsgründe mehr zu.

Zusammenfassend ist festzuhalten, dass das Bundesverwaltungsgericht die von der Beschwerdegegnerin bearbeiteten IP-Adressen zu Recht **als Personendaten im Sinne von Art. 3 lit. a DSG qualifiziert hat**

Während auf die Rechtfertigungsgründe von Art. 13 DSG in Art. 12 Abs. 2 lit. b und c DSG ausdrücklich verwiesen wird, fehlt ein entsprechender Vorbehalt in der aktuellen Fassung von lit. a der letztgenannten Bestimmung. Es fragt sich, ob das Streichen des Vorbehalts in Art. 12 Abs. 2 lit. a DSG im Zuge der Gesetzesrevision vom 24. März 2006 **ein qualifiziertes Schweigen zum Ausdruck bringt**. Die Rechtfertigung einer gegen die Grundsätze der Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG verstossenden Bearbeitung von Personendaten wäre diesfalls generell ausgeschlossen. In der Literatur gehen die Meinungen auseinander.

12 Ziff. 2 lit. b und c sehen vor, dass es Rechtfertigungsgründe geben kann, jedoch 12 Ziff. 2 lit. a DSG nicht.

Eine strikt systematische Auslegung, wonach lediglich bei lit. b und c, nicht aber bei lit. a von Art. 12 Abs. 2 DSG das Geltendmachen eines Rechtfertigungsgrunds zulässig sein soll, erweist sich als verfehlt, zumal in der aktuellen Fassung von lit. a Rechtfertigungsgründe zwar nicht mehr erwähnt, jedoch auch nicht ausdrücklich ausgeschlossen werden. Die Bestimmung ist daher so auszulegen, dass eine Rechtfertigung der Bearbeitung von Personendaten entgegen der Grundsätze von Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG zwar nicht generell ausgeschlossen ist, dass Rechtfertigungsgründe im konkreten Fall aber **nur mit grosser Zurückhaltung** bejaht werden können.

In Berücksichtigung des Bestrebens des Gesetzgebers, die Bedeutung der Grundsätze von Art. 4 DSG zu betonen, **schlägt das Bundesamt für Justiz in seiner Auslegungshilfe zur Änderung von Art. 12 Abs. 2 lit. a DSG vor, künftig rechtfertigende Umstände primär bei der Auslegung der allgemeinen Grundsätze zu berücksichtigen** (Bundesamt für Justiz, a.a.O., Ziff. 3.1). Ein derartiges Vorgehen **erscheint etwa dort praktikabel, wo sich die**

Abgrenzung zwischen den Grundsätzen von Art. 4 DSG und den Rechtfertigungsgründen von Art. 13 DSG ohnehin als schwierig erweist, so beispielsweise beim Grundsatz der Verhältnismässigkeit

Das Vorgehen der Beschwerdegegnerin stellt eine Persönlichkeitsverletzung dar. Es verstösst gegen die **Grundsätze der Zweckbindung und der Erkennbarkeit**, mithin gegen **Grundsätze, die für den Datenschutz** von grosser Wichtigkeit sind (Art. 4 Abs. 3 und 4 DSG). Im Folgenden ist zu prüfen, **ob die Persönlichkeitsverletzung gerechtfertigt werden kann**. Dabei kommt von vornherein nur ein überwiegendes privates oder öffentliches Interesse in Betracht; eine Einwilligung der Verletzten oder die Rechtfertigung durch Gesetz ist offensichtlich zu verneinen (Art. 13 Abs. 1 DSG). **Wie bereits erwähnt, dürfen zudem Rechtfertigungsgründe beim Verstoss gegen die Grundsätze von Art. 4 DSG nur mit grosser Zurückhaltung bejaht werden** (E. 5.2.4 hiervor)

Die Beschwerdegegnerin selbst verfolgt ein wirtschaftliches Interesse. Sie strebt eine Vergütung für ihre Tätigkeit an. Diese Tätigkeit besteht darin, mit Hilfe einer eigens dafür entwickelten Software in P2P-Netzwerken nach urheberrechtlich geschützten Werken zu suchen und von deren Anbietern Daten zu speichern. Eine solche Methode führt allgemein - über den konkreten Fall hinaus - wegen fehlender gesetzlicher Reglementierung in diesem Bereich zu einer Unsicherheit in Bezug auf die im Internet angewendeten Methoden wie auch in Bezug auf Art und Umfang der gesammelten Daten und deren Bearbeitung. Insbesondere sind die Speicherung und die mögliche Verwendung der Daten ausserhalb eines ordentlichen Gerichtsverfahrens nicht klar bestimmt.

Die Rüge des Beschwerdeführers erweist sich somit als begründet, was zur Gutheissung der Beschwerde führt.

Fragen

1) Eine Empfehlung nach 29 Ziff. 3 DSG ist eine Empfehlung an Private, das Bearbeiten von Personendaten zu ändern oder zu unterlassen – beim EDÖB handelt es sich um eine Aufsichtsbehörde. Die Empfehlung ist aber KEINE Verfügung.

Der EDÖB wird unter anderem tätig, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzten (Systemfehler)

2) Wird eine solche Empfehlung nicht befolgt oder abgelehnt, so kann der EDÖB die Angelegenheit dem Bundesverwaltungsgericht zum Entscheid vorlegen. Er ist berechtigt, gegen den Entscheid des BVGer Beschwerde zu führen beim Bundesgericht. Hier gelangte er an das BVGer und anschliessend an das BGer.

3) Angabe über Person, Personenbezug, Bestimmbarkeit. Die Bestimmbarkeit lässt sich bejahen, auch wenn die Logistep die Personen nicht bestimmen kann, aber sie geben die Daten an Personen weiter, welche die Personen erkennen können (können ohne grossen Aufwand die Personen identifizieren). Somit ist das DSG anwendbar –IP-Adressen sind Personendaten.

Würde aber eine Privatperson (Einzelperson) die Daten bearbeiten, muss im Einzelfall beurteilt werden, ob Bestimmbarkeit vorliegt als Kriterium. Per se spielt es keine Rolle. Wenn die Einzelperson im Einzelfall erfolgreich solche Daten bearbeiten kann bzw. die Transaktionen

verfolgen kann bzw. somit die Personen zu identifizieren, kann das Vorliegen der Bestimmbarkeit bejaht werden.

Bestimmbarkeit: Die Bestimmbarkeit einer Personenangabe lässt sich NICHT abstrakt festlegen, sondern muss aus der Sicht der Person, welche die Angaben bearbeitet, beurteilt werden. Im Einzelfall ist deshalb darauf abzustellen, ob der Datenbearbeiter **oder ein Dritter mit Hilfe der ihm zur Verfügung stehenden technischen Mittel in der Lage wäre, die Person** aufgrund der vorhandenen Angaben ohne übermässigen Aufwand zu identifizieren.

Ob IP-Adressen als Personendaten qualifiziert werden können, lässt sich nicht abstrakt beantworten. Vielmehr ist im Einzelfall zu prüfen, ob der Inhaber der Angaben über die Möglichkeit verfügt, die entsprechende Person zu identifizieren.

Im Fall Logistep konnte der Datenbeschaffer die Personen nicht identifizieren, jedoch hat er die Daten weitergegeben an einen Dritten, für den eine Identifizierung mit zumutbarem Aufwand möglich ist.

IP-Adressen sind somit NICHT immer per se Personendaten! Siehe Lehrbuch S. 424!

4) Grundsatz der Transparenz (die Betroffenen merken nichts von der Bearbeitung), Grundsatz der Zweckbindung.

Dies wurde gerügt bzw. da entgegen der Grundsätze von 4 DSG Personendaten bearbeitet wurden.

Werden solche Grundsätze verletzt, hat man die Fiktion nach 12 Ziff. 2 lit. a, dass eine Persönlichkeitsverletzung vorliegen würde. Es stellt sich die Frage, ob dies nun gerechtfertigt werden kann.

5) EDÖB ist der Ansicht, dass eine Verletzung der Grundsätze nicht gerechtfertigt werden kann. Das BGer ist der Auffassung, dass man so nicht argumentieren könnte. Eine Verletzung der Grundsätze kann mit Zurückhaltung gerechtfertigt werden.

Der EDÖB konnte hier mit seiner Auffassung nicht durchdringen.

6) Überwiegendes Interesse? Das BGer hat sich zunächst mit der Verhältnismässigkeit auseinandergesetzt. Interesse ist hier Zweck zum Schutz des Urheberrechts. Das BGer argumentiert, dass ein solches Vorgehen nötig ist zur Verfolgung von Urheberrechtsverletzungen. Es liegen private Interessen der Logistep, die Interessen der Betroffenen, die Intervention des EDÖB dient zur Verfolgung von Interessen. Hier liegen aber keine überwiegende Interessen für die Bearbeitung vor – es werden Unsicherheiten geschafft. Deshalb kann die Verletzung der Grundsätze nicht gerechtfertigt werden.

Die Datenbearbeitung ist somit widerrechtlich.

Datenbearbeitung durch öffentliche Organe (Bundesorgane) 15-25bis DSG

Aktueller Fall PMT

Intensive Personendatenbearbeitung. Betroffen sind auch besonders schützenswerte Personendaten (z.B. Religionszugehörigkeit) und Persönlichkeitsprofile. Der EDÖB hat sich kritisch geäussert – bereits liegen im Polizeirecht verschiedene Gesetze vor, die es schwierig machen, sich zu orientieren bzw. für welche Tatbestände welche Zugriffe erlaubt sind oder nicht.

Rechtsquellen

Sofern Spezialgesetz vorhanden, prüfen, ob anwendbar. Sonst allgemein DSG anwendbar. In der Regel gehen jüngere Spezialbestimmungen dem allgemeinen Datenschutz nach DSG vor. Wenn aber das ältere Spezialrecht strengere Datenschutznormen vorsieht, kann dies ausnahmsweise dem DSG vorgehen.

Geltungsbereich

- persönlich: Bundesorgane (DSG 3 lit. h), Ausnahme wenn Private mit der Ausführung von Bundesaufgaben betraut werden

Zentralverwaltung und dezentrale Verwaltung (öffentlich-rechtliche Körperschaften, Stiftungen und Anstalten)

Personen, die mit öffentlichen Aufgaben des Bundes betraut sind

In Frage kommen natürliche oder juristische Personen sowohl des Privatrechts als auch des öffentlichen Rechts.

Nicht als Bundesorgane gelten kantonale oder kommunale Behörden, selbst wenn sie im Zusammenhang mit Bundesaufgaben tätig werden. Die Wahrnehmung von Bundesaufgaben macht das handelnde kantonale Organ nicht zu einem solchen des Bundes – die kantonale Datenschutzgesetzgebung kommt zur Anwendung.

Es muss sich um eine öffentliche Aufgabe des Bundes handeln.

- sachlich: Bearbeitung von Daten in einem öffentlich-rechtlichen Verhältnis. DSG 23 lit. e contrario – wenn ein Bundesorgan privatrechtlich handelt, gelten die Bestimmungen für das Bearbeiten von Personendaten durch private Personen (z.B. SBB-Organe im Privatbereich)

1. Datenbearbeitung

3 DSG anwendbar. Jeder Umgang mit Personendaten.

2. in einem öffentlich-rechtlichen Verhältnis

Nicht nur dann, wenn Bundesorgane gegenüber der betroffenen Person hoheitlich gegenübertreten, sondern auch dann, wenn sie mit Privaten öffentlich-rechtliche Verträge abschliessen oder informelle Absprachen treffen.

- räumlich: Territorialitätsprinzip

- Allgemeine Ausnahmen von DSG 2 Ziff. 2

Zulässigkeit der Datenbearbeitung

1. Genügende Rechtsgrundlage

- Anforderungen des Legalitätsprinzips gemäss BV 5 Ziff. 1 und 36 Ziff. 1. Konkretisiert in DSG 17 und weiteren Bestimmungen des DSG sowie in Spezialgesetzen

a) Erfordernis des Rechtssatzes

b) Angemessene Bestimmtheit

c) Erfordernis der Normstufe, Formelles Gesetz bei schwerwiegenden Eingriffen in die verfassungsmässigen Persönlichkeitsrechte. Es muss aber nicht immer ein Gesetz im formellen Sinn vorliegen.

- Ausnahmen und Erleichterungen in DSG 17 Ziff. 2, 17a und 22

2. Öffentliches Interesse

Grundsätzlich keine Schranke. Alle öffentlichen Interessen können geeignet sein, die Datenbearbeitung zu rechtfertigen.

3. Verhältnismässigkeit

Fall „Revision Zollgesetz“

Totalrevision des Zollgesetzes und Schaffung eines Vollzugsaufgabengesetzes für das künftige Bundesamt für Zoll und Grenzsicherheit.

Kritik des EDÖB:

„…Bestimmungen zur Personendatenbearbeitung aus seiner Sicht gewichtige Mängel aufweisen. Diese lassen insbesondere die **vom Datenschutzgesetz verlangte Bestimmtheit vermissen**, welche es der Bevölkerung **ermöglichen würde**, die in deren Privatsphäre und Selbstbestimmung eingreifenden staatlichen Datenbearbeitungen sowie die ihr dagegen zur Verfügung stehenden Schutzrechte **einzuschätzen**. Der Beauftragte hat den Bundesrat dahingehend beraten, dass sich Regierung und Parlament als politische Organe des Bundes vorbehalten mögen, die wesentlichen Grundzüge der neu in einem einzigen System der Zollpolizei vorzunehmenden Datenbearbeitungen und die Schnittstellen zu diesem System zu regeln.“

„In ihrer gegenwärtigen Ausgestaltung überlässt es die Vorlage dem neuen Zollpolizeiamt, die auf einer **Vielzahl** von verwaltungs-, fiskal-, polizei- und kriminalrechtlichen Aufgaben beruhende Personendatenbearbeitung in ihrem System nach weitgehend autonomen Vorgaben vorzunehmen und die Informationen **nach Belieben** zu verknüpfen."

Fragen

1)

- „Mangelnde Bestimmtheit" Genügende gesetzliche Grundlage. Die Normen müssen genügend bestimmt sein. Wird hier kritisiert.

- Normstufe – vieles sei noch nicht im formellen Gesetz geregelt. Es liegt zwar ein formelles Gesetz vor, es ist aber noch nicht alles vorhanden, was drin stehen müsste.

2) In das formelle Gesetz gehört: Die Aufgaben der Behörde müssen im Gesetz möglichst klar umschrieben werden, auch die Grundzüge der Bearbeitung muss geregelt werden (Kategorien, Zwecke, Zugriffe Dritter)

Grundsätze der Datenbearbeitung

- Allgemeine Grundsätze; auch konkretisiert in DSG 17 Ziff. 2 lit. c (Treu und Glauben), DSG 18/18a (Zweckbindung, Transparenz), DSG 21 (Verhältnismässigkeit), DSG 25 Ziff. 3 (Richtigkeit)

- Insbesondere die **Datenbeschaffung** (18 ff. DSG)

Datenbeschaffung als „Datenbearbeitung". Datenbeschaffung braucht eine Rechtsgrundlage (Ausnahme 17 Ziff. 2 DSG), muss im öffentlichen Interesse stehen und verhältnismässig sein.

Aktive und passive Datenbeschaffung. Aktive Datenbeschaffung liegt vor, wenn das Bundesorgan von sich aus und durch gezieltes Vorgehen die erforderlichen Daten erhebt. Passive Datenbeschaffung ist umstritten, ob dies zur „Datenbeschaffung" gehört. Die Behörden gelangen ohne eigenes Tätigwerden zu den Daten. Dies kommt vor, wenn Bundesorgane, kantonale Behörden oder Privatpersonen von Gesetzes wegen zur Information an gewisse Bundesorgane verpflichtet sind.

Quellen der Datenerhebung

Aus der Rechtsgrundlage nach DSG 17 muss hervorgehen, aus welchen Quellen die Personendaten erhoben werden. Personendaten müssen primär bei den Betroffenen erhoben werden. Weiter möglich Datenbeschaffung bei privaten Dritten, bei anderen Bundesorganen oder bei kantonalen oder kommunalen Behörden.

Informationspflicht

Bundesorgane sind verpflichtet, die betroffene Person über die Beschaffung von Personendaten zu informieren (18a Ziff. 1 DSG). Diese Pflicht gilt auch dann, wenn die Daten bei Dritten beschafft werden.

Mittgeteilt werden muss nach 18a Ziff. 2 DSG.

Die Informationspflicht kann aber eingeschränkt werden (18b DSG) – Verweis auf Gründe von 9 Ziff. 1 und 2 DSG (Wenn Gesetz dies vorsieht, überwiegendes Interesse Dritter, Sicherheitsinteressen, etc.)

Bei systematischen Erhebungen gilt 18 DSG. Ziel solcher systematischen Erhebungen ist das Beschaffen von Personendaten im grossen Umfang. Die Informationspflicht wird aber hier weiter erstreckt. Die Einschränkungen der Informationspflicht können ebenso angewendet werden.

- Bekanntgabe (19 DSG) i.V.m. 3 lit. f DSG

Unter der Bekanntgabe versteht man jedes Zugänglichmachen von Personendaten wie das Einsicht gewähren, Weitergeben oder Veröffentlichen. In diesem Fall liegt eine Bekanntgabe von Personendaten vor, wenn Personendaten die Verfügungsgewalt des Bundesorgans, das die Daten erhoben hat, verlassen oder für andere durch Einsichtsgewährung, Weitergabe oder infolge einer Veröffentlichung zugänglich gemacht werden. Die Form der Bekanntgabe ist irrelevant. Massgebend ist, dass durch ein aktives oder passives Verhalten bewirkt wird, dass Private oder andere öffentliche Organe zu Informationen Zugang erhalten, die ihnen vorgängig nicht bekannt waren. Eine Datenbekanntgabe **liegt auch dann vor**, wenn Daten **innerhalb der Verwaltung** weitergegeben werden.

- Für die Bekanntgabe von Personendaten durch Bundesorgane braucht es eine eigenständige Rechtsgrundlage. Es gibt aber Ausnahmen (siehe 19 Ziff. 1 lit. a-d DSG). Betreffend Normstufe und Normdichte ist 17 Ziff. 1 und 2 DSG zu beachten.

- Überwiegendes öffentliches Interesse (19 Ziff. 4 DSG)

Jede Datenbearbeitung durch Bundesorgane muss durch ein öffentliches Interesse oder durch ein privates Drittinteresse, dass private Geheimhaltungsinteressen überwiegt, gerechtfertigt werden können.

Nach 19 Ziff. 4 lit. a und b hat das Bundesorgane die Bekanntgabe zu unterlassen, einzuschränken oder mit Auflagen zu verbinden, wenn wesentliche öffentliche Interessen (militärische Sicherheit, Staatsschutz oder Polizeiwesen) oder offensichtlich schutzwürdige Interessen einer betroffenen Person es verlangen (lit. a) oder gesetzliche Geheimhaltungspflichten oder besondere Datenschutzvorschriften es verlangen (lit. b).

Sonderfall Abrufverfahren (19 Ziff. 3 DSG)

Wenn Personendaten zugänglich gemacht werden, sodass das Bundesorgan die gewünschte Information selber beschaffen kann, ohne dass die bekanntgebende Behörde mitwirken muss. Z.B. Publikation von Urteilen oder von Telefonnummern im Internet.

Erforderlich ist grundsätzlich eine ausdrückliche gesetzliche Grundlage (es genügt ein Gesetz im materiellen Sinn). Für die Bekanntgabe von besonders schützenswerten Personendaten sowie Persönlichkeitsprofilen braucht es ein Gesetz im formellen Sinn.

Sonderfall Bekanntgabe im Rahmen der behördlichen Information der Öffentlichkeit (19 Ziff. 1bis)

Bundesorgane dürfen im Rahmen der behördlichen Information Personendaten bekannt geben, wenn die betreffenden Personendaten im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen und wenn an deren Bekanntgabe ein überwiegendes öffentliches Interesse besteht.

- Datenbekanntgabe ins Ausland (6 DSG)

Grundsätzlich nur zulässig, wenn dadurch die Persönlichkeit der betroffenen Person nicht schwerwiegend gefährdet wird. Ausnahmsweise (6 Ziff. 2 DSG).

Wenn Bundesorgane Daten bekanntgeben (ins Ausland), müssen sowohl die Voraussetzungen von 19 DSG und 6 DSG beachtet werden.

- Datenbearbeitung im Auftrag (10a DSG)

Auftraggeber ist jedes datenbearbeitende Bundesorgan. Als Dritter gilt jede vom Auftraggeber verschiedene natürliche oder juristische Rechtsperson oder Verwaltungseinheit.

- Bundesorgan muss selber berechtigt sein, die Daten zu bearbeiten (gesetzliche Grundlage nach 17/19 DSG)

- Dritte darf Daten nur soweit bearbeiten, als es das verantwortliche Bundesorgan selber dürfte

- Übertragung durch Gesetz oder Vereinbarung

- Kein Ausschluss durch gesetzliche oder vertragliche Geheimhaltungspflicht

- Überwachung mit optisch-elektronischen Anlagen

Videoüberwachung im öffentlichen oder öffentlich zugänglichen Raum

Werden Bilder aufgezeichnet, die Rückschlüsse auf bestimmte Personen zulassen bzw. wenn die Personen bestimmbar/identifizierbar sind, fällt dies unter den Begriff des Bearbeitens von Personendaten und damit unter das DSG.

Werden die Informationen nicht aufgezeichnet bzw. reine Wahrnehmung, ist das DSG nicht anwendbar.

Da es eine Bearbeitung von Personendaten durch ein Bundesorgan ist, braucht es dafür eine gesetzliche Grundlage nach 17 DSG, die Überwachung muss im öffentlichen Interesse liegen und verhältnismässig sein.

- Archivierung, Vernichtung und Anonymisierung (21 DSG)

Bestimmung regelt die Situation, was mit Personendaten gemacht werden muss, die nicht mehr benötigt werden. Besteht eine gesetzliche Aufbewahrungsfrist, kann die Vernichtung oder Archivierung erst nach deren Ablauf erfolgen.

Personendaten, die nicht mehr ständig benötigt werden, werden Bundesarchiv angeboten (21 Ziff. 1 DSG). Erachtet das Bundesarchiv die Daten als nicht archivwürdig, so werden sie vernichtet – ausser wenn sie anonymisiert sind oder zur Beweis- oder Sicherheitszwecken oder zur Wahrung der schutzwürdigen Interessen der betroffenen Person aufbewahrt werden müssen.

- Datenbearbeitung für nicht personenbezogene Zwecke (22 DSG)

Die Bestimmung lässt die Bearbeitung von Personendaten für nicht personenbezogene Zwecke unter erleichterten Voraussetzungen zu und entbindet sie von der Einhaltung gewisser Bearbeitungsgrundsätze (Zweckbindung 4 Ziff. 3, Formelle Grundlage 17 Ziff. 2 und 19 Ziff. 1 bezüglich Bekanntgabe von Personendaten)

Nicht personenbezogene Zwecke sind Forschung, Planung und Statistik.

Voraussetzungen:

- Daten müssen anonymisiert werden, sobald es der Zweck erlaubt

- Empfänger gibt die Daten nur mit Zustimmung des Bundesorgans weiter

- Wenn Ergebnisse veröffentlicht werden, ist die betroffene Person nicht bestimmbar

Verantwortlichkeit für die Einhaltung des Datenschutzes (16 DSG)

Grundsätzlich ist jenes Bundesorgan für den Datenschutz verantwortlich, das die Personendaten in Erfüllung seiner Aufgaben bearbeitet oder bearbeiten lässt. Entspricht im Allgemeinen dem Inhaber einer Datensammlung.

Wer Personendaten bearbeiten lässt (durch Dritte), hat zu vergewissern, dass der Dritte die Datensicherheit gewährleistet (10a Ziff. 2 DSG).

Die Verantwortlichkeit beinhaltet eine allgemeine und umfassende Verantwortung für das zuständige Bundesorgan. Die Persönlichkeitsrechte des Betroffenen dürfen in keiner Phase der Datenbearbeitung verletzt werden. Insbesondere muss das verantwortliche Organ die angemessenen technischen und organisatorischen Massnahmen für die Datensicherheit (7 DSG) treffen.

Sicherstellung der Verantwortlichkeit

- Spezifische Meldepflicht – Register der Datensammlung (11a)

Bundesorgane müssen sämtliche Datensammlungen beim EDÖB zur Registrierung anmelden.

- Berater für den Datenschutz (23 VDSG)

Bundeskanzlei und die Departemente haben jeweils mindestens einen Berater für den Datenschutz einzusetzen.

- Aufsicht über Bundesorgane (27 DSG)

Aufsicht durch den EDÖB. Der EDÖB kann den Bundesorganen Empfehlungen abgeben

- **Rechtsansprüche (8, 20 und 25 DSG)**

Rechte der Betroffenen gegen Bundesorgane (8, 20 und 25 DSG)

Umsetzung von 13 Ziff. 2 BV und 8 EMRK. Die betroffene Person hat gegenüber den datenbearbeitenden Bundesorganen verschiedene Ansprüche.

- Auskunftsrecht (8 DSG)

Siehe Auskunftsrecht unten

Die Auskunft erfolgt nur auf Gesuch hin. Es besteht grundsätzlich keine Auskunftspflicht – aber 18 und 18a DSG beachten (Informationspflichten)

- Anspruch auf Sperrung der Bekanntgabe (20 DSG)

Eine betroffene Person, die ein schutzwürdiges Interesse geltend macht, kann vom verantwortlichen Bundesorgan verlangen, dass es die Bekanntgabe von bestimmten Personendaten sperrt. Gegenstand ist hier nur die Bekanntgabe von bestimmten Daten.

Das schutzwürdige Interesse muss **lediglich glaubhaft gemacht** werden. Der Anspruch besteht nicht absolut – das Bundesorgan kann nach 20 Ziff. 2 DSG die Sperrung verweigern oder aufheben, wenn eine Rechtspflicht zur Bekanntgabe besteht oder die Erfüllung seiner Aufgabe sonst gefährdet wird.

Der behördliche Entscheid über die Sperrung stellt eine Verfügung im Sinne von VwVG 5 dar. Dementsprechend können negative Entscheide (Abweisung des Gesuches) beim BVGer mit Beschwerde angefochten werden.

Im Gegensatz zu 25 DSG wird bei 20 DSG nicht verlangt, dass die Bekanntgabe widerrechtlich sein muss. Dennoch muss aber ein schutzwürdiges Interesse geltend gemacht werden.

- Ansprüche aus 25 DSG

Problem: Bei der Datenbearbeitung (durch Bundesorgane) ist meist kein Verwaltungsverfahren vorgelagert, das mit einer Verfügung enden würde. Die Datenbearbeitung gehört vielmehr zu den Realakten. 25 DSG sorgt dafür, dass die betroffenen Personen ihre Rechte geltend machen können. Das Verfahren von 25 DSG endet stets in einer Verfügung, die dann bei den zuständigen Instanzen angefochten werden kann.

Betreffend der Frage zu den finanziellen Entschädigungen und Genugtuungsansprüche kommt das Verantwortlichkeitsgesetz des Bundes zur Anwendung – Staatshaftung.

Voraussetzungen (Formell)

- Ansprüche sind beim **zuständigen Bundesorgan** geltend zu machen (jenes Bundesorgan, das die Personendaten in Erfüllung seiner Aufgaben bearbeitet oder bearbeiten lässt)

- es muss beim zuständigen Bundesorgan **ein Gesuch** eingereicht werden

- mit dem Einreichen des Gesuchs wird ein Verwaltungsverfahren eingeleitet. Ein solches Verfahren verlangt **Partei- und Prozessfähigkeit** der gesuchsstellenden Partei (siehe VwVG)

- Berechtigung erforderlich – man muss ein **schutzwürdiges Interesse** haben. Der Gesuchssteller muss ein rechtliches oder tatsächliches Interesse am Ausgang des Verfahrens haben bzw. er muss stärker als die Allgemeinheit betroffen sein und in einer besonders beachtenswerten und nahen Beziehung zur Streitsache stehen. Das Rechtsschutzinteresse muss auch immer aktuell sein. Bezieht sich das Gesuch der Partei auf ihre eigenen Daten, ist die Voraussetzung des schutzwürdigen Interesses in der Regel ohne weiteres gegeben.

Voraussetzungen (Materiell)

Vorausgesetzt ist das Vorhandensein einer bereits erfolgten, einer andauernden oder einer noch drohenden **rechtswidrigen Datenbearbeitung** durch ein Bundesorgan. Rechtswidrigkeit liegt vor bei einem Verstoss gegen die materiellen Bestimmungen des DSG.

Verfahren und Rechtsschutz

Das Verfahren richtet sich nach den Vorschriften des VwVG. Es können zudem nach VwVG 56 vorsorgliche Massnahmen angeordnet werden – im DSG findet sich keine Regelung über vorsorgliche Massnahmen nach 25 DSG oder 20 DSG.

Die Verfügung kann mit Beschwerde beim BVGer angefochten werden. In zweiter Instanz entscheidet das BGEr – es besteht kein Ausschlussgrund nach 83 BGG.

Fall „Once Only“

„Der Bundesrat will die Datenbewirtschaftung der öffentlichen Hand durch die Mehrfachnutzung von Daten einfacher und effizienter machen: Personen und Unternehmen sollen den Behörden bestimmte Angaben nur noch einmal melden müssen.

Die Verantwortung für die Umsetzung liegt beim BFS (Bundesamt für Statistik).

Fragen

1) Wenn all diese Daten an einem Ort zusammenkommen, kann die Datensicherheit gefährdet werden. Mehrfachnutzung von Daten.

Gefahr für: Zweckbindung, Datensicherheit

2) 22 DSG

Fall „Erhebung kantonaler Steuerdaten“

Fragen

1) Darf BFS (Bundesamt für Statistik) Daten zu statistischen Zwecken erheben, wenn diese ohne Namen und Adresse, aber mit der AHV-Nummer geliefert werden?

AHV-Nummer ist Personendatum. 22 DSG anwendbar. Die Daten müssen nach 22 Ziff. 1 lit. a DSG aber anonymisiert sein, was hier aber nicht gemacht wird – da die AHV-Nummer ein Personendatum darstellt. Es sind keine ANONYME Daten, sondern PSEUDONYMISIERTE Daten. Somit ist die Voraussetzung nicht erfüllt nach 22 Ziff. 1 lit. a DSG.

2) JA – Bund hat verfassungsrechtliche Grundlage. Zusätzlich gibt es noch ein Spezialgesetz (BStatG).

Fall „Tonaufnahmen bei Gutachten“

▪ Die Vorlage «IVG. Änderung (Weiterentwicklung der IV)» (17.022) wurde am 19.6.2020 in der Schlussabstimmung von den Eidg. Räten angenommen.

▪ Sie enthält u.a. Art. 44 Abs. 6 ATSG, welcher für vom Versicherungsträger angeordnete Gutachten vorsieht: «Sofern die versicherte Person es nicht anders bestimmt, werden die Interviews in Form von Tonaufnahmen zwischen der versicherten Person und dem Sachverständigen erstellt und in die Akten des Versicherungsträgers aufgenommen».

Fragen

1) Tonaufnahmen ermöglichen die Identifizierung von Personen. Wenn Gesundheitsaspekte betroffen sind, liegen besonders schützenswerte Personendaten vor.

2) Grundsatz der Zweckbindung – es müsste genau angegeben werden, für das die Personendaten erhoben werden.

Fall „Namensschilder für SBB-Angestellte“

▪ A. ist Angestellter der SBB (nachfolgend „Arbeitgeberin“) und gemäss den internen Vorschriften über die Uniformen verpflichtet, bei der Arbeit in den Zügen ein Namensschild zu tragen, welches insbesondere den ersten Buchstaben seines Vornamens und den vollen Nachnamen trägt.

▪ Nachdem sich A. seit Dezember 2016 erfolglos bei seiner Arbeitgeberin um ein Namensschild ohne Erwähnung seines Nachnamens bemühte, focht er den letzten, förmlichen ablehnenden Entscheid der Arbeitgeberin vom 4.10.2018 mit Beschwerde vom 5.11.2018 beim BVGer an.

▪ Im Wesentlichen machte A. eine Verletzung des Verhältnismässigkeitsprinzips im Rahmen des Datenschutzrechts geltend. Er berief sich dabei insbesondere auch auf eine entsprechende Stellungnahme des EDÖB zur Problematik der Namensschilder, welche Alternativen zur Namensnennung erwog.

BVGer wies Beschwerde von A ab.

Fragen

Vgl. Fall Namensschilder bei der Polizei (BS)

1) DSG ist anwendbar. Die Schilder sind eine Angabe über eine Person, welche bestimmbar ist. Bearbeitung von Personendaten durch Bundesorgane – die SBB übernimmt eine öffentliche Aufgabe des Bundes. Erkennbar auch als Bundesorgan, weil die SBB verfügt hat und das ganze an das BVGer weitergezogen wurde.

Es liegt eine Bearbeitung vor, da hier eine „Offenbarung" vorliegt.

2) Verhältnismässigkeit bejaht. Interesse ist die Kundennähe. Es ist verhältnismässig, weil es zumutbar ist. Man könnte auch mit dem Namensschild unredliches Verhalten der SBB-Angestellten verfolgen. Es gibt keine Alternativen, um dem Interesse gerecht zu werden. Es ist zumutbar für die Angestellten – es gibt nur selten Probleme. Es gibt zudem Ausnahmeregelungen bei der SBB.

Rechte Einzelner

Zwei Stufen bei den Rechten:

1. Informationspflicht & Auskunftsrecht (Wissen)

2. Berichtigungsrecht & weitere Ansprüche (Mittel)

Es braucht das Wissen als Voraussetzung zur allfälligen Ergreifung von Mitteln, um eine unrechtmässige Datenbearbeitung zu verhindern bzw. zu beseitigen.

Rechte Privater (gegenüber Privaten)

- Auskunftsrecht (8)

- Berichtigung (5 Ziff. 2 und 15 Ziff. 1)

15 Ziff. 1: „Die klagende Partei kann insbesondere verlangen, dass die Datenbearbeitung gesperrt wird, keine Daten an Dritte bekannt gegeben oder die Personendaten berichtigt oder vernichtet werden."

- Sperrung der Datenbearbeitung, Verbot der Bekanntgabe und Berichtigung bzw. Klage nach 28, 28a und 28o ZGB (15 Ziff. 1)

- Bestreitungsvermerk (15 Ziff. 2)

- Mitteilung oder Veröffentlichung (15 Ziff. 3)

Rechte Privater (gegenüber Bundesbehörden)

- Auskunftsrecht (8)

- Berichtigung (5 Ziff. 2 und 25 Ziff. 3)

- Sperrung Bekanntgabe (20)

- Unterlassen widerrechtlicher Bearbeitung (25 Ziff. 1 lit. a)

- Beseitigen der Folgen widerrechtlichen Bearbeitens (25 Ziff. 1 lit. b)

- Feststellung der Widerrechtlichkeit des Bearbeitens (25 Ziff. 1 lit. c)

- Bestreitungsvermerk (25 Ziff. 2)

- Berichtigung, Vernichtung oder Sperrung der Bekanntgabe an Dritte (25 Ziff. 3)

- Mitteilung oder Veröffentlichung des Entscheids (25 Ziff. 3)

Informationspflicht

- Private: Inhaber von Datensammlungen: **Beschaffen** von besonders schützenswerten Personendaten und Persönlichkeitsprofilen (14). Im Gegensatz zu den Bundesorganen ist der Schutzbereich geringer bei den Privaten.

Es spielt keine Rolle, ob die Daten bei der betroffenen Person oder bei Dritten beschafft werden. Auch für die Beschaffung von Daten aus öffentlichen Quellen fällt unter 14 DSG (vgl. Fall mit den berühmten Personen auf der Website).

Die Information hat aktiv und ausdrücklich zu erfolgen. Die Information erfolgt grundsätzlich beim Beschaffen der Daten (Wortlaut der Norm stellt auch auf „die Beschaffung ab“). Sofern sich aber der mitgeteilte Zweck und die vorgesehenen Datenbekanntgabe ändern, besteht eine erneute Informationspflicht.

Jedoch hat man dennoch den Grundsatz von DSG 4 Ziff. 4 – jedoch verpflichtet diese im Gegensatz zu 14 DSG nicht direkt aktiv zu informieren – es muss für die Betroffenen eine Erkennbarkeit gewährleistet werden.

- Bundesorgane: Umfassende Informationspflicht beim Beschaffen von Personendaten (18a). Auch dort sind die betroffenen Personen aktiv zu informieren.

Auskunftsrecht

DSG 8 – Ist Teil der allgemeinen Datenschutzbestimmungen. Gilt für Private und Bundesorgane.

Um das Auskunftsrecht zu beantragen, bedarf es keines schutzwürdigen Interesses etc. Person muss aber nach 1 Ziff. 1 VDSG sich über ihre Identität ausweisen – sonst könnte die Auskunft an eine unberechtigte Person erfolgen.

Jede natürliche und juristische Person kann das Auskunftsrecht beantragen.

Auskunftsverpflichteter ist der Inhaber der Datensammlung. Ob die Bearbeitung durch den Inhaber selbst erfolgt oder eine Drittbearbeitung vorliegt, spielt keine Rolle – der Inhaber bleibt auskunftspflichtig. Der Dritte wird auskunftspflichtig, wenn er den Inhaber der Datensammlung nicht bekannt gibt oder dieser (Inhaber) keinen Wohnsitz in der Schweiz hat. In diesen Fällen besteht eine parallele Auskunftspflicht – sowohl der Inhaber und der Dritte sind auskunftspflichtig. Der Inhaber soll sich nicht durch die Datenbearbeitung Dritter der Auskunftspflicht entziehen können.

Der Inhaber muss die betroffene Person über alle in der Datensammlung vorhandenen Daten informieren. In einem ersten Schritt muss der Inhaber abklären, ob überhaupt Daten über die betroffene Person bearbeitet werden. Ist dies zu bejahen, muss der Inhaber der Datensammlung grundsätzlich über sämtliche vorhandenen Daten Auskunft geben. **Jedoch muss der Inhaber der Sammlung nur über sich in seiner eigenen Datensammlung befindende Daten Auskunft geben und das Auskunftsrecht besteht nur für Personendaten, die die Auskunftsberechtigten betreffen.** Ausgeschlossen sind Auskünfte über Daten Dritter und die Einschränkungen von DSG 9 sind zu beachten.

Das Auskunftsrecht ist in der VDSG konkretisiert (1, 2, 13 und 14 VDSG)

Mitteilungen an die betroffene Person erfolgt prinzipiell kostenlos. Jedoch gibt es Ausnahmen. Die Auskunft oder der begründete Entscheid der Beschränkung muss innerhalb von 30 Tagen nach dem Einreichen des Auskunftsgesuchs erfolgen (1 Ziff. 4 VDSG).

Das Auskunftsrecht geht mit dem Tod des Berechtigten unter. Jedoch ist es möglich, Auskunft über Daten von verstorbenen Personen zu erhalten, wenn der Gesuchssteller ein Interesse an der Auskunft nachweist und keine überwiegende Interessen von Angehörigen der verstorbenen Person oder von Dritten entgegenstehen (1 Ziff. 7 VDSG) – als Interesse gilt nach 1 Ziff. 7 VDSG die Verwandtschaft oder die Ehe mit der verstorbenen Person.

Bei einer falschen oder unvollständigen Auskunft werden Private auf Antrag mit Busse bestraft (34 Ziff. 1 lit. a DSG).

Einschränkung der Informationspflicht und des Auskunftsrechts

Informationspflicht

Private (14 Ziff. 4 i.V.m. 9) und Bundesorgane (18a Ziff. 4, 18b Ziff. 4 i.V.m. 9)

Betroffene bereits informiert, gesetzlich vorgesehen oder unmöglicher/unverhältnismässiger Aufwand.

Auskunftsrecht

- Grundsatz: Bundesorgane und Private können das Auskunftsrecht verweigern, einschränken oder aufschieben, wenn ein Gesetz im formellen Sinn die Einschränkung vorsieht oder es wegen überwiegender Interessen Dritter erforderlich ist (9 Ziff. 1 lit. a und b DSG).

- Bundesorgane können **zudem** die Auskunft verweigern, einschränken oder aufschieben, wenn es wegen überwiegender **öffentlicher** Interessen (insbesondere der inneren oder äusseren Sicherheit der Eidgenossenschaft) erforderlich ist oder die Information oder die Auskunft den Zweck einer Strafuntersuchung oder eines anderen Untersuchungsverfahrens in Frage stellt (9 Ziff. 2 lit. a und b DSG)

- Private können zudem (nur Private Inhaber) das Auskunftsrecht verweigern, einschränken oder aufschieben, wenn es **eigene** überwiegende Interessen es erfordern und die Personendaten nicht Dritten bekannt gegeben werden (9 Ziff. 4 DSG)

Indirektes Auskunftsrecht, wenn der Verpflichtete seiner Pflicht nicht nachkommen kann aufgrund von Geheimhaltungsinteressen oder Einschränkungen nach 9 DSG. Der Betroffene wird nicht durch den Inhaber selber informiert, sondern durch einen Dritten, der die Auskunftspflicht im Namen des Inhabers ausübt.

Recht auf Berichtigung und sonstige Ansprüche (5 Ziff. 2 DSG)

Personen, über welche unrichtige Daten bearbeitet werden, haben einen Anspruch auf Berichtigung. Dieses Recht gilt gegenüber Bundesorganen und Privaten. Der Inhaber der Datensammlung hat selber geringfügige Fehler zu berichtigen. Der Nachweis der Unrichtigkeit bzw. der Beweis dafür obliegt der betroffenen Person.

Liegt ein Anspruch auf Berichtigung vor, müssen die Daten in Übereinstimmung mit der Realität gebracht werden – dass kann auch zu einer Löschung oder auch Ergänzung führen.

Die weiteren Ansprüche werden noch hinzugefügt.

Fälle Vorlesung 4. Mai

„Grenzen des Auskunftsrechts“ 4A_277/2020“

B AG sucht Investoren (C, D, E und F)

Es entstanden Uneinigkeiten betreffend die Anteilsrechte von C, D, E und F an der B AG

B AG und deren Verwaltungsrat lehnen Begehren von C, etc. betreffend Auskunft und Herausgabe sämtlicher sie betreffender Daten ab. Daraufhin klagen C, etc. auf Auskunft und Datenherausgabe

Klage wurde abgewiesen, zweite Instanz heisst Berufung gut. A und B AG fochten Entscheid beim BGer mit Erfolg an.

- DSG sei ohnehin nicht anwendbar

- Auskunftsrecht ist zu verneinen bzw. verweigern

Fragen

1) Rechtsmittel vor BGer?

Hier liegt ein privates Verhältnis vor – somit Beschwerde in Zivilsachen (75 ff. BGG). Entscheid ist ein Endentscheid nach 90 BGG:

2) Anwendbarkeit des DSG?

BGer bejaht Anwendbarkeit des DSG. Es handelt sich um eine Bearbeitung von Personendaten. Fraglich war, ob eine Ausnahme von 2 Ziff. 2 lit. c – hängiger Zivilprozess vorliegt und deshalb das DSG nicht anwendbar wäre. Jedoch lag noch gar kein hängiger Zivilprozess vor bzw. noch keine Rechtshängigkeit (keine Einreichung eines Gesuchs/Klage). Somit greift die Ausnahme nicht und deshalb ist das DSG anwendbar.

3) Auskunftsrecht bejahen oder verneinen?

Beschwerdegegner verfolgen gemäss BGer mit ihrem Auskunftsbegehren nur die Abklärung **von Prozessaussichten.** Die Beschwerdegegner (C, etc.) nehmen das datenschutzrechtliche Auskunftsrecht in Anspruch. Auskunftsbegehren wird wegen Rechtsmissbrauch abgewiesen.

Beschwerde wird gutgeheissen –der angefochtene Entscheid wird aufgehoben und die Klage wird abgewiesen (Reformatorisch).

„Fahrschüler am Pranger“

X ist Fahrschüler beim Fahrlehrer Z

X vergisst, eine Rechnung zu zahlen

Z droht dem X mit einem Zahlungsbefehl

X zahlt die ausstehende Rechnung und sucht sich neuen Fahrlehrer

Kollege empfiehlt Fahrlehrer Y

Dieser weist X ab, weil er lieber Schüler möchte, die zahlen

Fahrlehrer Y verweist auf die Website der Fahrschule Z – X ist dort als schlechter Zahler aufgeführt

X verlangt von Z die Löschung des Eintrags auf der Website

Z weigert sich, den Eintrag zu löschen

Rechtliches Vorgehen von X gegen Z

1) Persönlichkeitsverletzung – Rechtfertigung möglich? Kein überwiegendes Interesse vorhanden. Für solche Sachen gibt es ja das Betreibungsregister.

Zudem hat er dem Bearbeiter ausdrücklich gesagt, dass er nicht möchte, dass die Daten bearbeitet werden – 12 Ziff. 2 lit. b DSG. Auch hier kein RF-Grund ersichtlich.

2) Rechtanspruch nach 15 Ziff. 1 – er kann als klagende Partei verlangen, dass die Datenbearbeitung gesperrt wird. Zuerst Schlichtungsverfahren, dann allenfalls Klagebewilligung.

X könnte auch eine vorsorgliche Massnahme anordnen lassen nach der ZPO.

3) Berufung nach der ZPO

4) Siehe ZPO – Gerichtsstände

5) das Schlichtungsverfahren ist kostenlos. Aber es gibt bei einer Klage Kosten.

Ergänzung

Wird der EDÖB tätig?

Nein, weil es sonst eine grössere Anzahl von Personen braucht, deren Persönlichkeit verletzt wird durch die Bearbeitungsmethode (29 Ziff. 1 lit. a DSG). In diesem Einzelfall würde der EDÖB nicht tätig werden.

Variante

Die Geldinformation AG gibt als Dienstleistung Bonitätsauskünfte an. Bzw. der Fahrlehrer leitet die Daten weiter. Da hier mehrere Personen betroffen sind, wird der EDÖB hier tätig.

Ergänzung Variante

Die Geldinformation AG verweigert die Auskunft. Man möchte aber wissen, wie die Prozesschancen stehen.

Wir haben ja einen ähnlichen Fall gehabt – das Auskunftsrecht darf nicht rechtsmissbräuchlich geltend gemacht werden. Aus taktischen Gründen müsste man versuchen, das Begehren so zu stellen, dass man einen datenschutzrechtlichen Zweck hat für die Auskunft und nicht (oder nicht nur) wegen den Prozessaussichten.

Ergänzung Variante

EDÖB leitet Verfahren ein. In einem solchen Fall hat die betroffene Person keine Parteistellung.

Einführungsfall – Contact-Tracing

Beizen weigern sich, die Gästedaten automatisch zu übermitteln. Die Beizen sind Private. Die Contact-Tracer könnten damit schneller die Betroffenen warnen. Dazu werden APPs benutzt von Anbietern – die Daten gehen an den Kantonen. Die kantonalen Datenschützer müssen das System im Kanton überprüfen, ob es Datenschutzkonform ist. Da aber auch Beizen die Daten aufnehmen als Private, muss der EDÖB das ganze überprüfen.

Fall 2 «Grenzen des Auskunftsrechts» BGer 4A_125/2020

- DD (Beschwerdegegner) wurde von US-Strafverfolgungsbehörden wegen Beihilfe zu Steuerdelikten angeklagt, was seinen Ausschluss aus der Anwaltskanzlei F AG zur Folge hatte

- Rechtsstreit – Überweisung von Geld der Anwaltskanzlei auf das Konto DD bei der Bank X (weil DD als Anwalt noch Ansprüche hatte)

- Bank XX (Beschwerdeführer 2) informierte DD, dass sein Konto gelöscht wird (wegen dem Delikt) der Beschwerdegegner DD wurde als «unerwünschter Kunde» erfasst in der Datenbank der Bank XX.

- Partner der Anwaltskanzlei hat die Bank informiert über das Verfahren gegen DD – erst dadurch wäre das Konto aufgelöst worden

- der DD will Auskunft über sämtliche Personendaten der Bank mit inhaltlichem Bezug auf ihn (in allen Formen) – er klagt dies ein

- Klage auf Durchsetzung des Auskunftsrechts (nachschauen). Das Auskunftsrecht wird gegenüber Privaten durch eine Klage vor dem zuständigen Zivilrichter durchgesetzt und in einem einfachen und raschen Verfahren entschieden (15 Ziff. 4 DSG).

- Bezirksgericht erlässt Beweisverfügung

- Bank soll aussagen als Zeuge

- Bank erhebt Beschwerde – Obergericht weisst die Beschwerde ab – Bank geht ans BGer

Frage ist die **Tragweite** des eingeklagten Anspruchs auf Auskunfterteilung nach 8 Ziff. 2 lit. a DSG – bzw. was man für Ansprüche hat. Zudem gibt es eine Einvernahme eines Zeugen (160 ff. ZPO). **Der Umfang des eingeklagten Anspruchs auf Auskunfterteilung beeinflusst den Umfang des Anspruchs auf Beweisabnahme im Prozess!** Das Beweisverfahren könnte ohne Prüfung der Anspruchsvoraussetzungen missbraucht werden und mit dem Beweisverfahren könnte faktisch über den eingeklagten Anspruch entschieden werden, ohne abzuklären, ob eine Pflicht zur Auskunft besteht. **Das Auskunftsrecht nach Art. 8 DSG besteht aber nicht in Bezug auf sämtliche Informationen,** die nach der Legaldefinition als Personendaten anzusehen sind. Mitgeteilt werden müssen nur Personendaten, **die sich in einer Datensammlung** befinden. Ist ein Gedächtnis eine Datensammlung? Das Auskunftsrecht richtet sich gegen den Inhaber der Datensammlung. Es bezieht sich nach dem Gesetzestext einerseits auf **die in der Datensammlung vorhandenen Daten** und schliesst andererseits die **verfügbaren Angaben** über die Herkunft der Daten ein. Entgegen der Auffassung der Vorinstanz werden Angaben über die **Herkunft von Daten, die allenfalls im Gehirn** unter den gewöhnlichen Erinnerungen einer Person gespeichert sein könnten (und nicht etwa auf Geheiss des Inhabers der Datensammlung auswendig gelernt wurden), **nicht vom Auskunftsrecht erfasst**. Denn über derartige Informationen kann der Inhaber der Datensammlung nicht verfügen.

Die Vorinstanz hielt fest, dass auch ausserhalb von der Datensammlung vorhandene Informationen unter die Auskunftspflicht fallen. Sie könnten namentlich in Form eines

Gesprächs bestehen, wobei als Informationsträger die Speicherung im Gedächtnis genüge. Das BGer argumentiert, dass die Vorinstanz mit dieser Auslegung das Auskunftsrecht überdehnt.

Die Beweisverfügung sieht Zeugenbefragungen und eine Parteibefragung zur Ermittlung der Herkunft von Personendaten vor (Zusammenhang Auskunftsrecht und Beweisverfahren).

1) Streit zwischen Privaten. Durchsetzung von 8 DSG. Beschwerde in Zivilsachen. Beweisverfügung anfechtbar, weil nicht wiedergutzumachender Nachteil drohen könnte.

2) Auskunftspflichtig ist jeder Inhaber der Datensammlung auskunftspflichtig. Es kommt nicht auf die Daten darauf an. Unerheblich ist die Art der Speicherung oder die Bezeichnung der Datensammlung durch den Inhaber.

3) Der Inhaber der Datensammlung muss beweisen, dass die zu erteilende Auskunft wahr und vollständig ist.

4) Informationen über die Herkunft der Daten – die Daten müssen bekannt gegeben werden, sofern sie bekannt sind (8 Ziff. 2 lit. a DSG). Es besteht aber keine Pflicht zur Speicherung von Informationen.

5) Personendaten können vorliegen in diesem Fall – bzw. aber das Recht auf Auskunft erstreckt sich nicht auf die Speicherung im Gedächtnis. Der Gesetzgeber geht davon aus, dass die Daten physisch fassbar sein müssten bzw. in einer Datensammlung vorhanden oder verfügbar. Es würde daran fehlen, wenn eine Erinnerung vorliegen würde. Das Auskunftsrecht kommt hier an die Grenzen.

Aufsicht und Verfahren

EDÖB

- Beauftragter entscheidet autonom und ohne Einwirkungen von aussen über die Art und Weise der gesetzlichen Aufgabenerfüllung.

- Aufsicht über Bundesorgane (27 DSG) und über Private (29 DSG). Der Bundesrat ist von dieser Aufsicht ausgenommen – er ist aber trotzdem an die Vorschriften gebunden.

Bundesorgane unterstehen auch der Aufsicht nach 27 DSG, wenn die privatrechtlich handeln (23 Ziff. 2 DSG)

- der Beauftragte wird vom Bundesrat für eine Amtsdauer von vier Jahren gewählt (die Wahl ist aber durch die Bundesversammlung zu genehmigen)

- Information (30 DSG)

- Mitwirkung im Gesetzgebungsverfahren (31 Ziff. 1 lit. b DSG) Bei Vorlagen über Erlasse und Massnahmen, die für den Datenschutz erheblich sind.

- der EDÖB wird von sich aus oder auf Meldung Dritter hin tätig (27 Ziff. 2 DSG)

- im Gegensatz bei Bunddesorganen wird der EDÖB nur tätig, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzten

(Systemfehler), wenn Datensammlungen registriert werden müssen (11a) oder wenn eine Informationspflicht nach 6 Ziff. 3 DSG besteht.

- Registerführung der Datensammlungen (zugänglich über Internet) – 11a DSG

Vgl. Strafandrohung EDÖB 34 DSG – würde eine betroffene Person bzw. beschuldigte Person eine Aussage machen, wäre es aber nicht verwertbar wegen Nemo tenetur. Auch Berufsgeheimnisse können dem EDÖB entgegengehalten werden. Der EDÖB hat ja ein Informationsbeschaffungsrecht, aber dies hat Grenzen.

Kontrolle über Bundesorgane

Beauftragte klärt den Sachverhalt von Datenbearbeitungen ab, die ihm problematisch erscheinen. Der EDÖB hat dazu nach 27 Ziff. 3 DSG verschiedene Rechte, um seine Kontrolle durchzusetzen. Ergibt die Abklärung, dass Datenschutzvorschriften verletzt werden, so empfiehlt der Beauftragte dem verantwortlichen Bundesorgan, das Bearbeiten zu ändern oder zu unterlassen (27 Ziff. 4 DSG). Die Empfehlung ist keine Verfügung. Wird sie aber nicht befolgt, kann der Beauftragte die Angelegenheit dem Departement oder der Bundeskanzlei zum Entscheid vorlegen – dieser Entscheid geht in der Form einer Verfügung nach VwVG 5. Der Beauftragte kann dagegen Beschwerde erheben.

Kontrolle über Private

EDÖB hat gegenüber Privaten die gleichen Informationsbeschaffungsrechte wie gegenüber Bundesorganen (29 Ziff. 2 DSG).

Ergibt die Abklärung, dass Datenschutzvorschriften verletzt werden (bzw. wenn der EDÖB tätig wird nach 29 Ziff. 1 lit. a-c DSG), so kann er dem für die Datenbearbeitung verantwortlichen Privaten empfehlen, das Bearbeiten zu ändern oder zu unterlassen (29 Ziff. 3 DSG). Wird eine solche Empfehlung nicht befolgt oder abgelehnt, so kann er die Angelegenheit unmittelbar dem BVGer auf dem Klageweg (35 lit. b VGG) zum Entscheid vorlegen. Er ist berechtigt, gegen den Entscheid BÖRA beim BGer einzulegen.

In den Kantonen

Kantone sind verpflichtet, öffentliche Kontrollorgane einzurichten. Sämtliche Kantone verfügen heute über ein kantonales Datenschutzorgan. Die kantonale Aufsichtsbehörde muss ihre Aufgaben unabhängig erfüllen können.

Das Datenschutzaufsichtsorgan ist für die Einhaltung des Datenschutzes bei der Bearbeitung von Personendaten durch kantonale öffentlich Organe zuständig. Insbesondere auch über Private, die kantonale öffentliche Aufgaben erfüllen – in diesem Bereich ist das DSG des Bundes nicht anwendbar – die kantonalen Datenschutzerlasse sind anwendbar.

Das Datenschutzaufsichtsorgan muss über entsprechende Kontrollinstrumente und Befugnisse verfügen. Das Organ übt seine Kontrolltätigkeit von Amtes wegen oder aufgrund von Meldungen Dritter aus. Sowie beim schweizerischen DSG haben die Organe Untersuchungsbefugnisse und Informationsbeschaffungsrechte. Die kantonalen

Datenschutzerlasse räumen dem Aufsichtsorgan die Befugnis ein, Empfehlungen abzugeben, wenn sie eine Verletzung datenschutzrechtlicher Vorschriften feststellen. Die Kantone sehen bei Nichteinhalten der Empfehlung unterschiedliche Vollstreckungsmöglichkeiten vor.

Datenregister (11a DSG)

Der EDÖB führt ein Register der Datensammlungen von Bundesorganen und privaten Personen, dass von jeder Person eingesehen werden kann (11a DSG).

Private, die vorsätzlich eine Meldung nach 11a DSG unterlassen oder falschen Angaben machen, werden mit Busse bis 10'000 Franken bestraft (34 Ziff. 2 lit. a DSG).

Bundesorgane, die Inhaber einer Datensammlung im Sinne von 3 lit. i DSG sind, unterliegen grundsätzlich immer einer Meldepflicht (10a Ziff. 2 DSG)

Privatpersonen müssen ihre Datensammlungen beim EDÖB **nur** anmelden, wenn regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet werden oder regelmässig Personendaten an Dritte bekannt gegeben werden. Die Mitteilungspflicht besteht aber hier nur, wenn Bearbeitungen oder Bekanntgaben regelmässig erfolgen – bzw. «sich periodisch wiederholend».

Es gibt aber Ausnahmen der Meldepflicht (11a Ziff. 5 lit. a-f DSG)

Auch in den Kantonen gibt es solche Register.

Internationaler Datenschutz

EMRK 8 – Recht auf Privatsphäre und Familienleben

Ist der nationale Instanzenzug ausgeschöpft, kann beim EGMR eine Beschwerde wegen Verletzung der Konvention (EMRK) und ihrer Protokolle eingereicht werden.

Betroffen ist das Recht auf Achtung des Privat- und Familienlebens in EMRK

Die Schweiz ist ein Vertragsstaat der EMRK – sie gilt deshalb auch für die Schweiz.

- *Schutzbereich*: Personendaten betreffen aufgrund ihrer Personenbezogenheit die Privatsphäre und fallen darunter. Der Schutzbereich ist weit gefasst.

- *Eingriffe*: Alle Formen der Bearbeitung der Personendaten, ebenso die Verweigerung der Einsichtnahme. Ein Eingriff in den Schutzbereich liegt dann vor, wenn dem Staat das entsprechende Verhalten zuzurechnen ist.

- *Rechtfertigung*: (**Staatlicher**) Eingriff muss auf einer genügenden gesetzlichen Grundlage beruhen, auf einem der in EMRK 8 Ziff. 2 abschliessend aufgezählten Gründen erfolgen und verhältnismässig sein.

8 Ziff. 2 EMRK: *Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.*

Fälle International

Urteil 1 Zakharov gegen Russland

- Chefredaktor eines Verlags, beschwerte sich beim EGMR, dass russische Telefonanbieter von Gesetzes wegen verpflichtet sind, eine Vorrichtung zu installieren, mit welcher Behörden operationelle Untersuchungsmassnahmen durchführen könnten.

- dieses System würde gemäss Beschwerdeführer eine flächendeckende Überwachung der Kommunikation ermöglichen, weil das russische Gesetz keine ausreichende Garantien vorsehe.

1) Beschwerde möglich allein vom Bestehen einer umstrittenen Gesetzgebung? EGMR sagt, dass es möglich sei – man muss nicht konkret individuell von der Massnahme betroffen sein in diesem Fall. Die Massnahmen waren geheim bzw. betrafen viele Personen – keine spezifischen Massnahmen – innerstaatlich gab es keinen ausreichenden Rechtsschutz, deshalb muss man hier nicht geltend machen, dass man direkt betroffen wäre.

Grundsätzlich muss man aber sonst ein schutzwürdiges Interesse nachweisen generell beim Verfahren an den EGMR. Hier war aber eine abstrakte Prüfung zulässig.

2) Der Kreis der betroffenen war nicht genau definiert im Gesetz – somit unbestimmt formuliert. Der Zweck der Überwachung war auch nicht klar geregelt. Die Dauer war nur teilweise genügend geregelt. Über die Vernichtung von Daten wurde nichts geregelt. Es gab zudem keine genügenden Kontrollmechanismen bzw. die Prüfpflichten der russischen Gerichte waren eingeschränkt. Die gesetzliche Grundlage war somit nicht genügend.

Urteil 2 (Urteil Bojic gegen die Schweiz)

Frau ist Opfer eines Verkehrsunfalles – beantragte deshalb IV. Unfallversicherer lässt Betroffene durch einen Privatdetektiv beschatten. Beweismittel wurden berücksichtigt was zu einer Rentenreduktion geführt hat.

Betroffene rügt Verletzung des Privatlebens bzw. die Beweise hätten nicht verwertet werden dürfen. Eingriff ins Privatleben nach EMRK 8.

Relevant für die Schweiz ist das ATSG. Die Betroffene rügt nach EMRK 8, dass die gesetzliche Grundlage nicht genüge.

Die Überwachung wurde von einer privaten Versicherungsgesellschaft angeordnet – jedoch sind solche Versicherungsgesellschaften nach der Rechtsprechung Behörden und sind deshalb verpflichtet, Grundrechte zu beachten.

1) Die Versicherungsgesellschaft wird nach der Rechtsprechung des EGMR als Behörde anerkannt. Es handelte sich um die obligatorische Versicherung – deshalb übernimmt sie staatliche Aufgaben.

2) Video- Überwachung im öffentlichen Raum. EGMR hat festgehalten, dass solche Videoüberwachungen, wenn sie erkennbar und zweckgebunden sind, wird nicht in das Privatleben eingegriffen. Wenn sie nicht erkennbar ist bzw. geheim, dann liegt ein Eingriff in das Privatleben vor – was in diesem Fall so war. Im öffentlichen Raum vs. Schutz Privatlebens. Das Privatleben kann sich auch im öffentlichen Raum abspielen. Wenn die Art der Überwachung bestimmte Merkmale aufweist (gezielt, verdeckt), dann liegt ein Eingriff in das Privatleben vor, auch wenn es im öffentlichen Raum stattfand – das war in diesem Fall so.

3) Es gab dazu keine genügende gesetzliche Grundlage – deshalb musste die Schweiz das ganze anpassen. Es lag eine Verletzung von EMRK 8 vor. Es gab zwar eine gesetzliche Grundlage, aber sie war ungenügend. Es fehlten bestimmte Regelungen über die Bearbeitung. Ob die Aufnahmen verwertet werden durften im Verfahren, unterlag die Beschwerdeführerin.

In der Folge des EGMR-Urteils schuf die Schweiz den neuen Observationsartikel. Der EDÖB brachte sich im Gesetzgebungsprozess ein. Die Observationen sind neben IV und UV nun neu auch möglich in den übrigen Sozialversicherungszweigen.

Urteil 3

Zeitschrift in Finnland publiziert Informationen über das steuerpflichtige Einkommen und Vermögen natürlicher Personen. Zudem wurde ein SMS-Dienst betrieben – wer eine SMS mit einem Namen schickte, bekam Steuerinformationen über diese Person, wenn sie in der Datenbank erfasst war. Die Datenschutzbehörde hat angewiesen, dass diese Datenbearbeitung zu stoppen sei. Die Zeitschrift haben sich vor dem EGMR gewehrt.

Es lag nach dem EuGH eine Verarbeitung von personenbezogenen Daten vor (Vorabentscheidungsverfahren).

Der oberste Verwaltungsgerichtshof wies die Datenschutzbehörde an, die Datenverarbeitung zu untersagen. **Dies tat die Behörde auch.** Die Beschwerdeführerinnen machen vor dem EGMR geltend, die Sammlung von Steuerdaten sei nicht rechtswidrig und es gehöre zum öffentlichen Bereich. Die Privatsphäre wird nicht verletzt.

1) 10 EMRK (Meinungsfreiheit und Pressefreiheit), 8 EMRK. Es waren zwei Schutzbereiche betroffen. Die Zeitschrift beruft sich auf EMRK 10 – weil die Datenschutzbehörde die Datenverarbeitung untersagt hat.

2) Datenschutzkonvention des Europarates – ja – der EGMR lässt sich auch darauf stützen in diesem Bereich.

3) JA – es ist eine Bearbeitung von Personendaten – die Privatsphäre ist davon betroffen.

4) Die Information ist ja bereits öffentlich. Ist damit der Schutzbedarf nicht entfallen? Der Eingriff geschah durch die Datenschutzbehörde. Meinungsfreiheit vs. Privatsphäre der Betroffenen. Die Problematik war, die die Daten dargestellt wurden. Die Daten waren in einer

Art Katalog abgebildet in der Zeitschrift. Die Datenschutzbehörde hatte aber eine gesetzliche Grundlage für das Eingreifen gegen die Zeitschrift.

Auch wenn die Informationen bereits öffentlich sind, heisst das nicht, dass die Daten nicht mehr geschützt sind.

In der Abwägung durch den EGMR sei der Schutz der Persönlichkeit der betroffenen Personen höher zu gewichten als das Interesse der Zeitschrift – betreffend der Meinungsfreiheit nach EMRK 10! Auch darum, weil die Publikationen nicht in einem öffentlichen Interesse stehen.

In diesem Fall wurden zwei Konventionsrechte gegeneinander abgewogen.

5) JA – der Eingriff lag vor in EMRK 10 (Aufsichtsbehörde gegen Zeitschrift)

6) JA – lag vor

7) Privatsphäre – die Aufsichtsbehörde stützte sich beim Eingriff in EMRK 10 gegen die Zeitschriften auf EMRK 8 – Schutz der Personendaten der Betroffenen.

8) Abwägung zwischen den beiden Konventionsrechten.

Europäischer Datenschutz (EU)

- Charta der Grundrechte der Europäischen Union (Art. 8 – Schutz personenbezogener Daten)

- DSGVO – Datenschutzgrundverordnung

- Richtlinie 2016/680 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Bearbeitung personenbezogene Daten durch die zuständigen Behörden

> Unterliegt die Schweiz diesen Bestimmungen? Das EU-Recht ist nicht anwendbar für die Schweiz. Jedoch haben wir völkerrechtliche Verträge – dort lässt sich daraus ableiten, dass die Richtlinie 2016/680 für die Schweiz anwendbar ist.

DSGVO

Als Verordnung ist sie direkt anwendbar. Vgl. Richtlinie – muss umgesetzt werden.

- *Persönlicher Anwendungsbereich:* Vorschriften zum Schutz **natürlicher Personen** bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten (1 Ziff. 1 DSGVO) im Vergleich schützt das schweizerische DSG natürliche und juristische Personen.

- *Sachlicher Anwendungsbereich:* Gilt ganz oder teilweise für die automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, **die in einem Dateisystem gespeichert sind oder gespeichert werden sollen** (2 Ziff. 1 DSGVO)

Ausnahmen beachten (2 Ziff. 2 DSGVO)

- *räumlicher Anwendungsbereich* (wurde ausgeweitet):

Verantwortlicher oder Auftragsverarbeiter **hat Niederlassung in EU** (unabhängig ob Bearbeitung in EU erfolgt oder nicht).

Die DSGVO gilt für das Bearbeiten von Daten natürlicher Personen ungeachtet der Staatsangehörigkeit oder des Wohnorts dieser Personen. Das bedeutet, dass wenn Personendaten einer natürlichen Person mit Wohnsitz in der Schweiz in einem Mitgliedstaat der Europäischen Union bearbeitet werden, fallen diese in den Anwendungsbereich der DSGVO.

Verantwortlicher oder Auftragsverarbeiter **hat keine Niederlassung in der EU**, aber die Bearbeitung betrifft Waren oder Dienstleistungen, die für Personen in der EU bestimmt sind oder betrifft die Beobachtung des Verhaltens einer Person in der EU.

Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund des Völkerrechts dem Recht eines Mitgliedsstaats unterliegt.

Die Verordnung wird in allen 28 Staaten der Europäischen Union direkt und gleichermaßen angewendet und betrifft alle privaten Unternehmen, staatliche Behörden und andere Organisationen, die personenbezogene Daten speichern und verarbeiten. Sie hatten über zwei Jahre – seit dem 27. April 2016 – Zeit, um die neuen gesetzlichen Bestimmungen zu erfüllen – egal wo sich ihr Sitz befindet

Denn die Verordnung gilt auch für Unternehmen und Organisationen außerhalb der EU: Sollte ein Unternehmen oder eine Organisation personenbezogene Daten von Personen, die in der EU leben, verarbeiten, dann muss es die DSGVO einhalten – egal, an welchem Standort das Unternehmen oder die Organisation angesiedelt ist.

Rechte betroffener (DSGVO)

- Verpflichtung des Verantwortlichen, Verfahren und Mechanismen vorzusehen, die es Betroffenen ermöglichen, ihre Rechte auszuüben (12)

- Recht auf Information bei der Erhebung von Personendaten (13 und 14)

- Recht auf Auskunft der Betroffenen auf Bestätigung der Nicht oder Bearbeitung personenbezogener Daten über sie (15)

- Recht auf Berichtigung bzw. Ergänzung (16)

- Recht auf Löschung bei Vorliegen bestimmter Gründe (17)

- Recht auf Einschränkung der Bearbeitung in bestimmten Fällen (18)

- Recht auf Mitteilung – Verantwortliche müssen der betroffenen Person jede Berichtigung, Löschung oder Einschränkung mitteilen (19)

- Recht auf Datenübertragbarkeit – bereitgestellte Daten müssen vom Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format herausgegeben werden (20)

- Widerspruchsrecht gegen Datenbearbeitung gestützt auf ein öffentliches oder berechtigtes Interesse (21)

- Recht auf Verzicht auf automatisierte Einzelfall-Entscheidung – Benachrichtigungspflicht, sofern voraussichtlich hohes Risiko für die persönlichen Rechte und Freiheiten vorliegt (22)

- Recht auf Benachrichtigung über Datenschutzverletzungen (34)

- Besondere Regelung zum Schutz von Kindern (8)

Pflichten der Verantwortlichen

- Neu wurde der Grundsatz der **Rechenschaftspflicht des Verantwortlichen** verankert. Dieser muss die **Einhaltung der allgemeinen Grundsätze** nachweisen können. Auf dieser Grundlage wurde das Prinzip der Beweislastumkehr eingeführt.

- DSGVO 24 verlangt im Sinne des risikobasierten Ansatzes, dass der Verantwortliche zu Beginn einer Bearbeitung die Wahrscheinlichkeit und den Grad der Gefährdung beurteilen und Kontollmechanismen und -systeme vorsehen muss.

- DSGVO 25 verlangt, dass die Grundsätze des Datenschutzes schon bei der technischen Ausgestaltung berücksichtigt werden (privacy by design – Datenschutz nach Mass) und dass datenschutzfreundliche Voreinstellungen vorgesehen werden (privacy by default – Datenschutz als Standard).

- DSGVO 30 verlangt, dass jeder Verantwortliche oder sein Vertreter **ein Register der Bearbeitungstätigkeiten führt**. Es gibt Ausnahmen für Unternehmen mit < 250 MA.

- DSGVO 35 verlangt **bei hohem Risiko** von Bearbeitungen für die Rechte und Freiheiten der Betroffenen eine **Datenschutz-Folgenabschätzung**. Je nach Ergebnis resultiert eine Pflicht zur Konsultation einer DSA, unter Vorbehalt von Massnahmen zur Eindämmung des Risikos.

- DSGVO 32 verpflichtet den Verantwortlichen, angemessene organisatorische und technische Massnahmen zu treffen, um ein dem Risiko **angemessenes Schutzniveau** zu gewährleisten.

- DSGVO 33 verpflichtet, **Verletzungen des Schutzes personenbezogener Daten (data breaches) der DSA zu melden** wenn sie Risiken für die Rechte und Freiheiten natürlicher Personen zur Folge haben könnte, DSGVO 34 regelt die Modalitäten der Mitteilung an Betroffene.

- DSGVO 37 verpflichtet in bestimmten Fallkonstellationen die Benennung eines **Datenschutzbeauftragten**.

Sanktionen

- Aufsichtsbehörden können nach DSGVO selbst Sanktionen sprechen

- darunter fallen Geldbussen oder weitere Massnahmen wie Mahnungen, Verwarnungen oder auch die vorübergehende oder dauerhafte Beschränkung der Bearbeitung

Anwendbarkeit auf Schweizer Unternehmen

- Niederlassung in der EU (3 Ziff. 1)

Bearbeitung personenbezogener Daten im Rahmen der Tätigkeit einer europäischen Zweigstelle oder einer Tochtergesellschaft eines schweizerischen Unternehmens in der EU

- Zielgruppe in der EU (3 Ziff. 2)

Bearbeitung personenbezogener Daten von Personen mit Aufenthalt in der EU durch ein Unternehmen mit Sitz in der Schweiz, soweit es diese Daten für seine Waren- und Dienstleistungsangebote in der EU bearbeitet

Bearbeitung personenbezogener Daten von Personen mit Wohnsitz in der EU durch ein in der Schweiz ansässiges Unternehmen, soweit diese Daten zum Zweck der Beobachtung des Verhaltens der betroffenen Personen innerhalb der Union bearbeitet werden

Aufgaben (Anwendbarkeit auf Schweizer Unternehmen)

1) Schweizerisches Unternehmen verkauft Uhren über einen Online-Shop an Personen mit sitz in der EU. DSGVO ist anwendbar, weil hier Waren angeboten werden an Personen in der EU.

2) Hotelier im Engadin erstellt von seinen Europäischen Gästen Profile, um ihnen Angebote für andere Aufenthalte machen zu können. Auch hier ist die DSGVO anwendbar.

Konvention 108 + (Europäische Datenschutzkonvention)

- Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten (**von der CH ratifiziert**)

- Zusatzprotokoll bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung (auch ratifiziert)

- Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener daten (konnte noch nicht ratifiziert werden). Wird erst gemacht, wenn das totalrevidierte DSG in der Schweiz in Kraft getreten ist.

- Einzige **rechtsverbindliche völkerrechtliche Regelung im Bereich des Datenschutzes** – was ist mit der EMRK? Entscheidend ist, dass es sich bei der Konvention um ein spezifisches Recht über den Datenschutz handelt – das ist bei der EMRK nicht nur der Fall, weil sie ja auch andere Rechte schützt und nicht nur 8 EMRK. Die Konvention 108+ ist nicht Teil der Rechtsprechung des EGMRs, aber der EGMR stützt sich zum Teil auch auf andere Konventionen wie die EMRK.

Anwendungsbereich

- **jegliche** automatisierte und nicht-automatisierte Personendatenbearbeitung. **Personendatenbearbeitung jeglicher Art**.

- unter Hoheitsgewalt **eines Vertragsstaates**

- betreffend natürliche Personen (wie bei DSGVO)

- in privaten und öffentlichen Sektoren (beides ist abgedeckt mit gewissen Ausnahmen)

- ausgenommen ist die Bearbeitung bei persönlichen oder familiären Tätigkeiten (vgl. Schweizerisches DSG)

Die Konvention verstärkt den Schutz der Schweizer Bürgerinnen und Bürger, wenn ihre Personendaten in einem der Vertragsstaaten bearbeitet werden.

Grundsätze

- Rechtmässigkeit der Datenverarbeitung und Gewährleitung der Qualität der Daten

- Vorschriften für besondere Daten

- Datensicherheit

- Transparenz

- Rechte von Betroffenen und Pflichten der Verantwortlichen und Auftragsverarbeiter

- Ausnahmen und Einschränkungen, Sanktionen und Rechtsmittel, Vorbehalt weitergehenden Schutz

- **Grenzüberschreitender Verkehr personenbezogener Daten**

Neuerungen des Änderungsprotokolls (wird noch ratifiziert)

- Ausweitung der Pflichten des **Verantwortlichen**

Pflicht zur Meldung bestimmter Datenschutzverletzungen, Informationspflicht von Betroffenen, Pflicht im Vorfeld bestimmter Datenverarbeitungen eine Datenschutz-Folgenabschätzung vorzunehmen, Pflicht zu Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen

- Ausbau der Rechte der **Betroffenen**

Auskunftsrecht, automatisierte Einzelentscheidungen

- Verpflichtungen **der Vertragsstaaten**

Sanktionensystem und Rechtsmittelsystem einrichten, Aufsichtsbehörden können verbindliche (anfechtbare) Entscheidungen erlassen.

Schengener Datenschutzgesetz (SDSG)

Datenschutz im Rahmen der Anwendungen des Schengen-Besitzstands in Strafsachen

Anpassungen der schweizerischen Gesetzgebung an das europäische Recht (Übergangsgesetz). Es handelt sich um eine Richtlinie, welche durch das «Bundesgesetz über die Umsetzung der Richtlinie» umgesetzt wurde. Mit diesem Bundesgesetz wird unter anderem das SDSG eingeführt sowie Änderungen in anderen Bundesgesetzen.

Geltungsbereich

Bearbeitung von Personendaten **durch Bundesorgane** – Zweck: Straftaten verhüten, aufklären und verfolgen, Strafen vollstrecken. Auf kantonale Behörden ist das SDSG nicht anwendbar.

- Bearbeitung von Personendaten

- durch Bundesorganen

- Zweck: Straftaten verhüten, aufklären und verfolgen, Strafen vollstrecken

- im Rahmen der Anwendung des Schengen-Besitzstands oder im Rahmen anderer internationaler Verträge mit Schengen-Staaten mit Verweis auf EU-RL 2016/680.

Ausnahme: bei hängigen Verfahren vor eidgenössischen Gerichten oder nach der St PO (wie beim DSG). Ebenso Subsidiarität des DSG – Fehlt es an einer Regelung in SDSG oder in einem Spezialgesetz, dann gilt subsidiär das DSG.

Neuerungen

- Erweiterung der besonders schützenswerten Personendaten (genetische und biometrische Daten)

- Datenschutz-Folgenabschätzung

- Privacy by Design and Default; Bundesorgane sind verpflichtet, die Datenbearbeitung ab der Planung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden – insbesondere die Grundsätze (vgl. Grundsätze DSG).

- Konsultation EDÖB

- Meldungen von Verletzungen der Datensicherheit

- Aufsicht

- Eröffnung einer Untersuchung

Das totalrevidierte Datenschutzgesetz

Ziel der Totalrevision ist die Anpassung an die veränderten technologischen und gesellschaftlichen Verhältnisse.

Weiterhin: Datenbearbeitung erlaubt, sofern Bearbeitungsgrundsätze eingehalten. Sind die Grundsätze nicht eingehalten, braucht es eine Rechtfertigung. Unterscheidung von der DSGVO: Grundsatz des Verbots der Datenbearbeitung, die nicht auf einer Rechtfertigung beruht.

Zum Teil Anlehnung an die DSGVO oder Konvention 108 +

- Geschützt sind nur noch Daten von natürlichen Personen. Daten von juristischen Personen werden nicht mehr vom DSG erfasst. Es gibt dafür andere Bestimmungen wie ZGB 28. Hier gibt es eine Angleichung an das europäische Recht.

- Besonders Schützenswerte Daten – werden ausgeweitet auf genetische und biometrische Daten (siehe SDSG)

- neue Grundsätze (Datenschutz durch Technik und Datenschutz durch datenschutzfreundliche Voreinstellungen). Sie verpflichten Behörden und Unternehmen, die Bearbeitungsgrundsätze des DSG bereits ab der Planung entsprechender Vorhaben umzusetzen, indem sie angemessene technische und organisatorische Schutzmassnahmen treffen. Der Datenschutz durch Technik verlangt, dass sie ihre Applikationen u.a. so ausgestalten, dass die Daten standardmässig anonymisiert oder gelöscht werden. Datenschutzfreundliche Voreinstellungen schützen die Nutzer von privaten Online-Angeboten, die sich weder mit Nutzungsbedingungen noch den daraus abzuleitenden Widerspruchsrechten auseinandergesetzt haben, indem nur die für den Verwendungszweck unbedingt nötigen Daten bearbeitet werden, solange sie nicht aktiv werden und weitergehende Bearbeitungen autorisieren. Um diesen Schutz des neuen Gesetzes zu gewährleisten, sollten Schweizer Unternehmen ihre Angebote rechtzeitig überprüfen und nötigenfalls durch Einsatz datenschutz- und kundenfreundlicher Programme Anpassungen vornehmen.

- Private Unternehmen können neu einen Datenschutzberater ernennen. Für Private ist dies aber fakultativ – Bundesorgane sind gesetzlich dazu verpflichtet.

- Datenschutz-Folgenabschätzung neu auch durch Private.

- Bekanntgabe von Personendaten ins Ausland – Daten dürfen ins Ausland bekanntgegeben werden, wenn neu der Bundesrat (vorher hat es der EDÖB gemacht) festgestellt hat, dass die Gesetzgebung des Drittstaates einen angemessenen Schutz gewährleistet. Ist der Staat nicht vom Bundesrat bezeichnet, so dürfen die Daten wie nach bisherigen Recht trotzdem dorthin geleitet werden, wenn ein geeigneter Datenschutz auf andere Weise gewährleistet wird.

- Ausgebaute Informationspflichten – im Sinne der Transparenz, dass ein Privater bei grundsätzlich jeder beabsichtigten Beschaffung von Personendaten die betroffene Person vorgängig angemessen informieren muss. Im aktuellen DSG ist diese Informationspflicht bisher nur bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen vorgeschrieben. Die Einschränkungen der Informationspflicht nach bisherigem Recht bleiben vorbehalten.

- Ausgebautes Auskunftsrecht – die Mindestinformationen, die vom Verantwortlichen herausgegeben werden müssen, wurden erweitert.

- Meldepflicht bei Verletzungen der Datensicherheit

- Ausweitung Sanktionen

- Untersuchung aller Verstösse gegen Datenschutzvorschriften. Der EDÖB eröffnet von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person, wenn genügend Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte. Er kann von der Eröffnung einer Untersuchung absehen, wenn die Verletzung der Datenschutzvorschriften von geringfügiger Bedeutung ist.

Quizz DSG – EDÖB

1) Schutzobjekt

Schutzobjekt sind nicht Daten, sondern Personendaten.

z.B. geheime Konstruktionspläne der Fima für erste Quantencomputer. Schutz nach DSG? Nein, weil kein Personenbezug. Es handelt sich hier um Sachdaten, welche durch den Schutz des Geschäftsgeheimnisses geschützt sind nach StGB.

z.B. Mobilitätsdaten – Bewegung von Smart Devices – die Daten könnten aufgezeichnet werden. Es handelt sich hier um Sachdaten. Aber hier ist ein Personenbezug möglich bzw. könnte hier eine Person identifiziert werden. Wenn Bestimmbarkeit bejaht, dann DSG anwendbar.

DSG bezweckt den Schutz der Persönlichkeit, nicht der Daten.

2) Personenbezug

Mobilitätsdaten bei der Bewegung von Smart Devices. Hier können Angaben von Personen vorhanden sein, weil es wird Auskunft gegeben, wo und wie sich eine Person fortbewegt.

Bestimmbarkeit ist zu bejahen. Hier liegt ein grosses Überwachungspotential vor.

Techniken zur Pseudonymisierung und Anonymisierung. Diese Techniken können bewirken, dass die Bestimmbarkeit verneint wird. Aber Pseudonymisierung ist bloss eine Ersetzung eines Namens mit einem Code.

Fall: Swisscom hat die Mobilitätsdaten anonymisiert. Am Anfang der Pandemie hat Swisscom nachgeschaut und Karten erstellt, wo im öffentlichen Raum viele Personen anzutreffen waren oder sind. Die Swisscom hat dem EDÖB gemeldet, dass alles in Ordnung wäre. Die Daten seien anonymisiert. Handlungsbedarf des EDÖB? JA – weil hier die Methoden geeignet wären, dass die Persönlichkeit einer grösseren Anzahl von Personen verletzt werden könnte. Die Anonymisierungsmethoden müssten hinreichend gewährleisten, damit es nicht zu einer ungewünschten Re-Identifikation kommen könnte.

Fall: Steckdose vor dem Fenster mit Blick auf einen menschenleeren Innenhof eines Stadthauses. Personenbezug? JA – es handelte sich um eine Fahndung durch Interpol. Die Fahnder hatten einen Abgleich gemacht mit dem Internet. Durch die Steckdose kann man ableiten, in welchem Land eine Straftat verübt wurde. Und wenn man zusätzlich noch einen

Blick in den Innenhof hat, kann man durch Google Earth etc. diesen Ort ausfindig machen und man hat dann den potenziellen Personenbezug.

Ist der Personenbezug hier datenschutzrechtlich relevant? Nein, bei Steckdosen lässt sich nicht direkt ein Personenbezug erstellen. Nach dem Bundesgericht ist für den Personenbezug die Absicht, Wahrscheinlichkeit und der Aufwand relevant.

3) Auslandbezug

Zuger Medizinalfirma MEDI sendet Patientendaten an Luzerner Auftragsdatenbearbeiterin EMMI. Nachher lässt die MEDI den Auftrag durch die rumänische Firma RUMA erledigen.

Hier ändert sich die datenschutzrechtliche Rechtslage nicht grundlegend, aber es gelten nun die Regeln nach 6 DSG (grenzüberschreitende Bekanntgabe). Rumänien hat zudem einen angemessenen Datenschutz. Die Daten dürfen übertragen werden auf die rumänische Firma.

Muss MEDI damit rechnen, dass die rumänische Justiz auf Patientendaten ihrer Kunden greift? JA – genauso wie die Luzerner Justiz auf Patientendaten zugreift. Der Datenschutz tritt immer hinter die Justiz zurück.

> In jedem (demokratischen) Rechtsstaat gibt es keine Daten, auf die eine Justiz nicht vorbehaltlos zugreifen könnte.

Muss MEDI besondere Vorkehren treffen mit Blick auf Bearbeitung in Rumänien? JA – weil die Daten in Rumänien bearbeitet werden. Man hat dann eine Informationspflicht gegenüber den Betroffenen. Es muss nachgewiesen werden, dass die Dritten in Rumänien instruiert wurden.

MEDI lässt den Auftrag nun durch die Firma SUN in Florida erledigen. Hier ändert sich was? JA – weil die USA hat keinen angemessenen Datenschutz (siehe Fall «Shrems»).

Sind die Risiken durch einen US-behördlichen Zugriff auf Patientendaten anders zu beurteilen, als sie noch durch die RUMA (rumänische Firma) bearbeitet wurde? JA – weil in Rumänien ein angemessener Datenschutz besteht, aber in den USA ist dieser mangelhaft. Mangelhafte Justizförmigkeit und Rechtsschutz.

Muss MEDI zusätzliche Vorkehren treffen mit Blick auf die Bearbeitung in den USA im Vergleich zur Bearbeitung in Rumänien? JA – weil der Privacy Shield nicht ausreicht.

MEDI lässt den Auftrag durch die Zuger Firma FUN erledigen. FUN ist eine Tochtergesellschaft von Microsoft. Aus der Sicht der Schweiz ändert sich nichts – weil die Firma sich an das Schweizer Recht halten muss (hat ja Sitz in Zug). Aus der USA gibt es aber Änderungen.

4) Sanktionen

- US Nachrichtendienst hat sich heimlich bei SUN umfangreiche Patientendaten aus Medikamententests beschafft und an die Firma Pfizer weitergegeben, die sich gegenüber MEDI so einen Wettbewerbsvorteil verschaffen konnte.

Könnte sich die Firma SUN nach dem neuen DSG strafbar gemacht haben?

Datensicherheit ist hier einschlägig. Hier könnte sie strafbar sein; subsidiäre Strafbarkeit des Unternehmens nach 64 nDSG. Aber nur dann, wenn es sich nicht lohnt, den Täter im Unternehmen zu ermitteln.

Management der Firma SUN, wenn Nachweis, dass die Mindestanforderungen an die Datensicherheit grobfahrlässig vernachlässigt wurden? NEIN – weil strafbar ist nur die vorsätzliche Begehung.

- US Nachrichtendienst hat bei SUN umfangreiche Patientendaten aus Medikamententests herausverlangt und an die Firma Pfizer weitergegeben, die sich gegenüber der SUN so einen Wettbewerbsvorteil verschaffen konnte.

Management der Firma SUN könnte strafbar gemacht werden, weil sie vorsätzlich Daten ins Ausland bekanntgegeben haben, ohne dass die gesetzlichen Voraussetzungen erfüllt sind.

- EDÖB kann selber keine Busse verhängen. Ebenso kann er nicht einen Strafantrag stellen. Er könnte aber als Privatkläger auftreten.